УДК 343.3/.7
DOI https://doi.org/10.32840/1813-338X-2022.4.16

Є. С. Назимко
перший проректор
Донецького державного університету внутрішніх справ
доктор юридичних наук, професор

А. В. Щербіна
суддя Київського районного суду міста Одеси,
доктор філософії в галузі права

Т. І. Пономарьова
завідувач науково-дослідної лабораторії з проблем запобігання
кримінальним правопорушенням
Донецького державного університету внутрішніх справ
кандидат юридичних наук

ЗАРУБІЖНИЙ ДОСВІД КРИМІНАЛЬНО-ПРАВОВОГО ЗАХИСТУ АВТОМАТИЗОВАНИХ СИСТЕМ В ОРГАНАХ ТА УСТАНОВАХ СИСТЕМИ ПРАВОСУДДЯ

У статті розглядається зарубіжний досвід кримінально-правового захисту автоматизованих систем в органах та установах системи правосуддя. Зазначено, що аналіз державної статистики та судової практики дозволив підсумувати, що в останні роки все більш актуальними стають кримінальні правопорушення проти правосуддя, що зумовлено прагненням суб'єктів реалізувати протиправний умисел на порушення нормального процесу досудового розслідування та судового розгляду, що може мати наслідком ще більшу інтенсифікацію криміногенних загроз. Вказано, що підхід до судової системи в окремих країнах більш схожий на певний бізнес-проєкт, оскільки творці системи занадто орієнтовані на удосконалення зовнішньої взаємодії громадян та електронного суду. Ймовірно, саме у зв'язку із цим не приділено зосередженої уваги її нормативно-правовому, в особливості – кримінально-правовому захисту. Автори звертають увагу на те, що кримінальне законодавство Естонії не передбачає спеціальної норми, котра встановлювала би відповідальність за посягання на електронні судові системи. Не дивлячись на достатньо розгалужене програмне забезпечення, а також на наявні ризики, пов'язані із широким доступом до електронних даних, законодавець лише побічно захистив інформацію за рахунок інших норм.

Підсумовано, що законодавець не надає кримінальному правопорушенню, котре полягає у порушенні нормальної роботи автоматизованих систем в органах та установах системи правосуддя особливого значення. У жодному з розглянутих Кримінальних кодексів автори не знайшли хоча б схожої норми у розділі, присвяченому кримінальним правопорушенням проти правосуддя. Це дозволило констатувати, що Україна більш серйозно оцінює це суспільно небезпечне діяння, розуміючи, що останнє здатне дестабілізувати судову систему, а також негативно вплинути на загальну кримінологічну ситуацію України.

Ключові слова: *автоматизовані системи, органи та установи системи правосуддя, кримінальне правопорушення, несанкціоноване втручання, кримінальне законодавство, зарубіжні країни, позитивний досвід.*

Постановка проблеми. Сучасне суспільство характеризується перманентним зростанням кількісного показника кримінально протиправної діяльності, що свідчить про рудиментарність національного кримінального законодавства та його неспроможність повноцінно реалізовувати покладене на нього завдання, яке полягає у захисті суспільства та держави від протиправних посягань, а також запобігання кримінальним правопорушенням. Аналіз дер-

жавної статистики та судової практики дозволив підсумувати, що в останні роки все більш актуальними стають кримінальні правопорушення проти правосуддя, що зумовлено прагненням суб'єктів реалізувати протиправний умисел на порушення нормального процесу досудового розслідування та судового розгляду, що може мати наслідком ще більшу інтенсифікацію криміногенних загроз. Одним із способів протидії досудовому розслідуванню та судовому розгляду кримінальних проваджень є незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя, кримінальна відповідальність за вчинення якого передбачена ст. 376-1 КК України.

Аналіз останніх досліджень і публікацій. Особливості кримінально–правового та кримінологічного захисту системи правосуддя взагалі та незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя зокрема є предметом дослідження низки національних учених, серед яких необхідно виділити праці О. М. Бандурки, Є. О. Гладкової, О. О. Дудорова, М.В. Карчевського, О. О. Кваши, О. О. Книженко, Л.М. Палюх, М. І. Хавронюка, В. Б. Харченка та інших. Однак низка важливих для науки кримінального права питань залишається відкритими, що свідчить про доцільність звернення до позитивного досвіду та практики зарубіжних країн, а отже обумовлює актуальність обраної теми статті.

Метою статті є дослідження досвіду окремих зарубіжних країн в частині кримінально-правового захисту автоматизованих систем в органах та установах системи правосуддя, а також виокремлення позитивних рішень для імплементації у національну кримінально–правову та кримінологічну політику.

Викладення основного матеріалу. Відтак, відповідно до Закону про судову владу, Судова інформаційна система (CIC) Латвії є державною інформаційною системою, розробленою урядом Латвії (Міністерством юстиції). Завданням системи є забезпечення автоматизованого діловодства в рамках судового провадження з можливістю реєстрації справи, обробки та збереження даних, оперативного контролю за станом справи, ефективного обміну інформацією (даними) між судами та іншими установами, а також автоматичною підготовкою статистичних звітів. У Латвії існує єдина централізована CIC, яка була розроблена в 1998 році і запроваджена в 1999 році (у судах по всій країні в 2003 році). Система підтримується та розробляється Судовою адміністрацією Латвії і наразі перенесена на нову платформу в рамках проекту E-case (Електронна справа). Інформаційна система суду в Естонії (KIS) – це сучасна система управління інформацією в естонських судах 1-ї та 2-ї інстанцій та у Верховного Суду, яка є єдиною інформаційною системою для всіх видів судових проваджень. KIS дозволяє реєструвати судові справи, засідання та судові рішення, забезпечує автоматичний розподіл справ між суддями, створення повісток, публікацію судових рішень на офіційному сайті та збір метаданих. Інформаційна система також має інструмент пошуку для судових документів, судових рішень, засідань та справ. Конфіденційні дані та справи може бачити лише суддя у справі та співробітники суду, пов'язані зі справою» [1]. Таким чином, як ми бачимо, країни самі намагаються захистити свої судові інформаційні системи шляхом встановлення певних заборон для окремих працівників. Саме тому, ймовірно, кримінально-правовий захист відходить на другий план.

Вчені вірно вказують, що аналіз кримінальних правопорушень проти правосуддя, які встановлені законами про кримінальну відповідальність різних країн, указує на їх різну кількість та зміст. Необхідно зазначити, що встановлення злочинів проти правосуддя є типовим для законодавця різних країн. Це може вказати на суспільну небезпечність злочинів у сфері правосуддя та необхідність протидіяти їм кримінально-правовими засобами. Утім законодавець у різних країнах підійшов по-різному щодо формулювання злочинів проти правосуддя та назв розділів, які їх охоплюють. Відповідно до цього було названо дві основні групи підходів щодо формулювання назв та родових об'єктів кримінальних правопорушень проти правосуддя. Аналіз конкретних кримінальних правопорушень проти правосуддя дозволяє визначити типові діяння проти правосуддя: 1) неправдиве повідомлення про вчинення кримінального правопорушення, його симуляція, неповідомлення про вчинення (тяжкого) злочину та фальсифікація доказів; 2) неправдиве обвинувачення, лжесвідчення, лжеприсяга та інші неправдиві заяви; 3) діяння, пов'язані із прийняттям незаконних рішень (незаконне затримання або арешт, примушування давати показання, відмова від здійснення правосуддя, постановлення неправдивого судового рішення); 4) корупційні діяння осіб, що здійснюють правосуддя; 5) погроза або насильство проти учасників провадження,

а також посягання на їх власність; 6) перешкоджання відправленню правосуддя, неявка та наклеп; 7) втеча з місця позбавлення волі, звільнення особи, яка відбуває покарання, та приховування кримінального правопорушення; 8) інші діяння на стадії виконання судового рішення або вироку (невиконання судового рішення, ухилення від виконання судового рішення, бунт засуджених) [2, с. 165]. На жаль, формальні ознаки розглядуваного нами кримінального правопорушення містяться у принципово іншому розділі кримінальних законодавств, присвячених суспільно небезпечним діянням у сфері інформатики та зв'язку, а також інформаційній безпеці.

У Литві вся інформація про кожну справу зберігається в централізованій інформаційній системі всіх судів, що називається LITEKO. Система була запущена в 2004 році і з тих пір підтримується та постійно оновлюється Національною судовою адміністрацією (НСА). У 2011 р. Уряд Литви затвердив програму розвитку інформаційного суспільства Литви (2011-2019 рр.), в якій вказав конкретні цілі державного сектору щодо розширення сфери допустимості та застосування державних електронних послуг. Для просування державної стратегічної мети НСА реалізувала проєкт розвитку електронних послуг у судах, а 1 липня 2013 року було запущено портал державних електронних послуг судів (EPP) як окремий модуль LITEKO. З зазначеної дати через EPP [3] сторони можуть формувати та передавати процесуальні документи до суду в електронній формі, ознайомлюватись із документами електронної справи, контролювати інформацію щодо судового збору, судових витрат та штрафів. Протягом 2015-2017 років було здійснено інтеграцію LITEKO з 14 інформаційними системами та реєстрами інших установ. Також було створено нове, вдосконалене технологічне рішення/платформу LITEKO як основу LITEKO2 [4]. Необхідно зауважити, що в Литві сформувався дуже цікавий підхід до будування автоматизованих систем в органах та установах системи правосуддя. Більше того, цікавим є те, що так званий електронний суд в країні дозволяє зацікавленим особам брати повноцінну участь у кримінальному провадженні.

«Так, наприклад, судова рада приймає стратегічні засади та «політичні» рішення щодо того, як слід будувати взаємодію LITEKO з іншими системами та реєстрами (наприклад, об'єднати чи просто інтегрувати з інформаційною системою досудового розслідування), також ініціює обговорення процесуальних змін, які можуть спростити процедуру та уможливити більш ефективне використання технологій (наприклад, зменшити кількість документів, що надаються сторонами, якщо завдяки інформаційній системі та інтеграціям суддя може отримувати інформацію безпосередньо з державних реєстрів; більше можливостей дистанційних слухань у кримінальних справах тощо). У січні 2017 року Судова рада прийняла Стратегічні засади розвитку литовської судової системи. Один із 7 напрямків присвячений розробці IT-інструментів, що сприяють ефективному здійсненню правосуддя. Модернізація LITEKO є найважливішою серед цих питань. Стратегія включає не лише основні напрямки діяльності та конкретні заходи; вона також охоплює показники, строки, відповідальних посадових осіб. НСА готує періодичний звіт про хід виконання стратегії, представляє його Судовій раді та обговорює можливі зміни, ризики, нові виклики тощо. Оскільки члени Судової ради – теж судді, вони знають багато практичних аспектів використання системи та нових рішень. Отже, ці дискусії дуже важливі і корисні для подальших розробок та для планування відповідних навчальних заходів, коригування системи комунікації та наставництва» [5]. В цьому контексті цікавим аспектом є нівелювання законодавцем повноцінного кримінально-правового захисту електронного суду. Як і у інших країнах, у кримінальному кодексі Литви відсутня аналогічна українській спеціальна норма, котра би передбачала такого роду протиправне діяння.

«НСА відповідає за реалізацію стратегічних цілей у розробці інформаційних систем та рішень у судовій системі. Цей орган виступає менеджером інвестиційних проєктів, здійснює щоденне обслуговування та адміністрування LITEKO, віддає на зовнішній підряд відповідні послуги та контролює якість цих послуг, підтримує діяльність робочих груп, координує мережу наставників з інформаційних технологій в судах, готує відповідні навчальні програми для користувачів LITEKO тощо. Для цих функцій в НСА є відділ інформаційних технологій, до складу якого входять менеджери IT-проєктів, програмісти, IT-адміністратори (загалом 8-9 працівників). Наприклад, відділ тісно співпрацює з іншими відповідними підрозділами НСА: відділом стратегічного планування – щодо підготовки інвестиційних проєктів та бюджетних запитів; юридичним відділом – з аналізу бізнес-процесів

та процедур, очікувань суддів та працівників апарату суду тощо; відділом державних закупівель – щодо розробки ТЗ та організації процедур закупівель (це досить складно – є різні надавачі різних послуг, бо встановлено законодавчі вимоги щодо заборони концентрації закупівель для забезпечення ринкової конкуренції; таким чином, НСА працює з 3-5 різними надавачами послуг LITEKO одночасно)» [5]. Хоча, варто також зауважити, що підхід до судової системи в даній країні більш схожий на певний бізнес-проєкт, оскільки творці системи занадто орієнтовані на удосконалення зовнішньої взаємодії громадян та електронного суду. Ймовірно, саме у зв'язку із цим не приділено зосередженої уваги її нормативно-правовому, в особливості – кримінально-правовому захисту.

«Інформаційна система суду в Естонії (KIS) – це сучасна система управління інформацією в естонських судах 1-ї та 2-ї інстанцій та у Верховного Суду, яка є єдиною інформаційною системою для всіх видів судових проваджень. KIS дозволяє реєструвати судові справи, засідання та судові рішення, забезпечує автоматичний розподіл справ між суддями, створення повісток, публікацію судових рішень на офіційному сайті та збір метаданих. Інформаційна система також має інструмент пошуку для судових документів, судових рішень, засідань та справ. Конфіденційні дані та справи може бачити лише суддя у справі та співробітники суду, пов'язані зі справою» [5]. Отже, можна сказати, що дана інформаційна система суду дещо схожа із національним Єдиним реєстром судових рішень. При цьому, естонський підхід також дещо відрізняється від українського.

«Так, наприклад, в країні існує електронна справа (e-File), котра забезпечує доступ до різних етапів кримінальних, цивільних та адміністративних проваджень, до судових рішень та процесуальних актів всім сторонам, у тому числі громадянам. Розвиток Електронної справи було викликано необхідністю розділити сховища даних, які функціонували незалежно одне від одного. Будучи інтегрованою системою, Електронна справа забезпечує одночасний обмін інформацією між інформаційними системами різних сторін: поліції, прокуратури, судів, установ виконання покарань, органів пробації, виконавців, системи БПД, податкових органів та митниці, центру державної служби підтримки, адвокатів і громадян. Електронна справа економить час і кошти, оскільки дані вводяться лише один раз, а комунікація між сторонами відбувається в електронному вигляді. Естонський проєкт Електронна справа отримав особливу відзнаку Європейської премії «Кришталеві ваги правосуддя 2014», яка присуджується за інноваційну практику, що сприяє ефективності та якості правосуддя» [5]. Таким чином, дана система дозволяє обмінюватись інформацією не тільки в межах судової системи, що формує певні ризики та загрози.

«Публічний портал Електронної справи надає громадянам можливість ініціювати відкриття цивільного, адміністративного чи виконавчого провадження, а також провадження у справі про кримінальний проступок, і стежити за перебігом цього провадження, подавати документи та брати участь у провадженнях. Публічний портал Електронної справи – це частина Електронної справи, яку бачать усі. Електронна справа – це інформаційна онлайн-система, яка збирає документи, що стосуються цивільних, адміністративних, кримінальних проваджень та проваджень у справах про кримінальні проступки, а також дозволяє вчиняти відповідні дії, вносити дані та обробляти їх. Електронна справа дає можливість сторонам у справі та їхнім представникам подавати документи до суду в електронному вигляді та контролювати перебіг відповідних судових процесів. Громадяни можуть також оскаржувати позови та рішення, здійснювати платежі, пов'язані з провадженням у справах, а також робити запити в Базі даних судимостей щодо себе та інших осіб. У системі особи можуть бачити лише ті провадження, в яких самі беруть участь. Загальнодоступна частина Електронної справи є захищеною, оскільки для входу потрібно посвідчення особи або мобільний ідентифікатор. Це також економить час, оскільки дані можна переглянути та розпочинати провадження без необхідності особистого звернення до установи. І останнє, але не менш важливе: це зменшує час очікування на рішення, оскільки єдина система даних пришвидшує роботу чиновників» [5]. Що стосується нашої країни, на жаль, ми не можемо наразі продемонструвати такий досконалий підхід до діджиталізації кримінального процесу. Тим не менш, наша країна, як здається, є однією з небагатьох, котрі захистили саме автоматизовані системи в органах та установах системи правосуддя від протиправних посягань.

Цифрові судові справи були останньою та фінальною розробкою в ІТ-системі електронного правосуддя в Естонії з метою запровадження повністю безпаперових проваджень

у судах. Звичайна (судова) система ведення справ, така як KIS, сама по собі недостатньо зручний інструмент для суддів та сторін, які ведуть юридичну роботу над матеріалами справ. Цифрова судова справа забезпечила додатковий функціонал для суддів та інших юристів, забезпечуючи просунуті можливості систематизації та фільтрування документів, групової роботи з документами справи, у т.ч. доступні для пошуку коментарі та виділення, які може бачити лише відповідний користувач або групи користувачів, цифрові посилання між різними документами або частинами документів, а також функція копіювання та вставлення тексту всіх цифрових документів, що додаються до справи тощо [5]. Підхід естонців до комп'ютеризації кримінального процесу, безспірно, вражає. Однак, необхідно відмітити, що вивчення кримінального (пенітенціарного) законодавства дозволило підсумувати відсутність спеціальної норми та лише частковий захист нормами з розділу, присвяченого комп'ютерним кримінальним правопорушенням.

«Так, наприклад, в статті 269 КК Естонії вказано, що незаконне знищення, пошкодження, порушення або блокування комп'ютерної інформації або комп'ютерних програм карається штрафом або арештом. Ті самі дії: 1) спричинили великий майновий збиток, або 2) спрямовані проти ведуться державою основних або державних регістрів, або 3) вчинені за попередньою змовою групою осіб, караються арештом або позбавленням волі на строк до двох років. Стаття 270 встановлює кримінальну відповідальність за комп'ютерний саботаж – введення інформації або програм, їх модифікація, знищення або блокування з метою створення перешкод в роботі комп'ютерної або телекомунікаційної системи, що карається штрафом, або арештом, або позбавленням волі на строк до двох років. Ті самі дії: 1) спричинили істотну шкоду, або 2) спрямовані на створення перешкод в роботі основних державних або державних реєстрів, караються позбавленням волі на строк до чотирьох років. В статті 271 вказано, що незаконне використання комп'ютерів, комп'ютерних систем або комп'ютерних мереж шляхом усунення їх засобів захисту (кодів, паролів і т.д.) карається штрафом або арештом. Те саме діяння, вчинене: 1) повторно, або 2) із заподіянням істотної шкоди, або 3) з використанням комп'ютерів, комп'ютерних систем або комп'ютерних мереж, містять інформацію, що становить державну таємницю або призначену тільки для службового користування, карається штрафом, або арештом, або позбавленням волі на строк до двох років» [6]. Таким чином, можна підсумувати, що кримінальне законодавство Естонії не передбачає спеціальної норми, котра встановлювала би відповідальність за посягання на електронні судові системи. Не дивлячись на достатньо розгалужене програмне забезпечення, а також на наявні ризики, пов'язані із широким доступом до електронних даних, законодавець лише побічно захистив інформацію за рахунок інших норм.

«Що стосується Німеччини, варто відмітити, що країна достатньо серйозно відноситься до захисту державної таємниці, а також інформації, котра має ключове значення для державних справ. Так, наприклад, Кримінальний кодекс Німеччини, містить положення про те, що державною таємницею є факти, об'єкти й інформація, доступні лише обмеженому колу осіб, які повинні зберігатися в секреті від іноземних держав з метою недопущення спричинення шкоди зовнішній безпеці Федеративної республіки. Удосконалення захисту державних секретів здійснюється за трьома напрямами: вдосконалення законодавства у сфері захисту державних секретів і секретів фірм; посилення органів контррозвідки та надання їм великих повноважень, у тому числі й у сфері захисту державних секретів; створення організацій «самодопомоги» в промисловості та розгортання їх діяльності. Важливим у вдосконаленні захисту секретів під час проведення науково-дослідних робіт військового призначення в Німеччині є посилення повноважень органів контррозвідки, і, зокрема, тих її підрозділів, які здійснюють боротьбу зі шпигунством і опікуються захистом державних секретів, у тому числі й у промисловості. У системі забезпечення захисту державних секретів у питаннях боротьби з «промисловим шпигунством» іноземних держав важлива роль відводиться об'єднанням промисловців, так званим організаціям «самодопомоги»» [7, с. 114]. «До таких організацій відноситься, наприклад, «Координаційний центр по забезпеченню безпеки в промисловості», створений у Кельні в 1969 році, який вирішує проблеми забезпечення режиму секретності в промисловості держави» [8]. Цікавим фактом також є те, що в кримінальному законодавстві країни кримінальні правопорушення проти правосуддя диференційовані по різним розділам в залежності від мети, обумовлюючої протиправне посягання. Також німецьке законодавство не має спеціаль-

ного розділу, присвяченого комп'ютерним суспільно небезпечним діянням.

«У ФРН інформація з обмеженим доступом може мати три ступені секретності: «цілком таємно» (Streng Geheim); «таємно» (Geheim); «конфіденційно» (VS-Vertraulich). Слід зазначити, що у ФРН до державної таємниці відносяться лише відомості, які необхідно зберігати в секреті від іноземних держав з метою недопущення завдання шкоди зовнішній безпеці Федеративної республіки. В той же час відомості, які містять інформацію про проведення оперативно-розшукових заходів, належать до службової таємниці та охороняються відповідним законодавством. Відповідальність за порушення службової таємниці встановлена у 28 розділі Кримінального кодексу ФРН. Відповідні документи, що містять службову таємницю, позначають грифом «Для службового користування» (VS nur fur den dienstgebrauch)» [9, с. 114]. «Якщо документи для службового користування обробляються в автоматизованих системах, то мають бути дотримані певні вимоги безпеки. А саме автоматизовану систему має бути обладнано фаєрволом, у випадку підключення до мережі Інтернет, має бути затверджений перелік осіб, які мають доступ до автоматизованої системи, використовуватися механізми автентифікації та ідентифікації (ім'я користувача та пароль), обов'язковою є наявність Інструкції з ІТ-безпеки тощо» [9, Section II (1)]. Отже, не дивлячись на прагнення будь-яким способом захистити інформацію, особливо – державного значення, німецький законодавець проігнорував автоматизовані системи в органах та установах системи правосуддя та майже в повній мірі зневелював інтересами правосуддя, «розкидавши» кримінальні правопорушення по іншим розділам Кодексу, що майже в повній мірі «розмило» безпосередній та родовий об'єкти посягання.

Висновки. Таким чином, можна підсумувати, що в розглянутих країнах законодавець не надає кримінальному правопорушенню, котре полягає у порушенні нормальної роботи автоматизованих систем в органах та установах системи правосуддя особливого значення. У жодному з розглянутих Кримінальних кодексів ми не знайшли хоча б схожої норми у розділі, присвяченому кримінальним правопорушенням проти правосуддя. Це дозволяє констатувати, що наша країна більш серйозно оцінює це суспільно небезпечне діяння, розуміючи, що останнє здатне дестабілізувати судову систему, а також негативно вплинути на загальну кримінологічну ситуацію України.

Список використаних джерел:

1. Estonian Court Information System. URL: https://www.rik.ee/en/international/ court-information-system
2. Шепітько М.В. Поняття та види злочинів проти правосуддя за законодавством зарубіжних країн. *Вісник Національної академії правових наук України*. 2017. № 2. С. 157-165
3. E-service portal of Lithuanian courts. URL: https://e.teismas.lt/lt/public/home/
4. Казакевич П.В. Проблемні питання створення судових електронних систем у Європі та Україні. URL: https://law.chnu.edu.ua/wp-content/uploads/2020/12/Zbirnyk-16.10.20.pdf
5. Управління судовими інформаційними системами: міжнародний досвід. URL: https://www.pravojustice.eu/storage/app/uploads/public/5fa/a5e/c73/5faa5ec73c202992255267.pdf
6. Пенітенціарний кодекс Естонської Республіки від 6 червня 2001 р. зі змінами станом на 01.11.2017. URL: http://www.legislationline.org/download/action/download/ id/4707/file/Estonia_Penal Code_am2013_en.pdf
7. Ковальов К.Є., Леонов Б.Д. Забезпечення охорони державної та службової таємниці у сфері оперативно-розшукової діяльності за законодавством окремих держав: порівняльний аналіз. *Інформація і право*. № 1(20). 2017. С.112-122.
8. Executive Order 13526 Classified National Security Information, December 29, 2009. URL: http://edocket.access.gpo.gov/2010/pdf/E931418.pdf
9. Instruction sheet on the Handling of Protectively Marked Information Classified VSNUR FÜR DEN DIENSTGEBRAUCH (RESTRICTED). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/VSMerkblattEnglisch_pdf.pdf?__blob=publicationFile

Nazymko Ye. S., Shcherbina A. V., Ponomarova T. I. Foreign experience of criminal legal protection of automated systems in bodies and institutions of the justice system

The article examines the foreign experience of criminal legal protection of automated systems in bodies and institutions of the justice system. It is noted that the analysis of state statistics and judicial practice allowed us to conclude that in recent years criminal offenses against justice have become more and more relevant, which is due to the desire of subjects to realize the illegal intention to violate the normal process of pre-trial investigation and trial, which can have an even greater consequence

intensification of criminogenic threats. It is indicated that the approach to the judicial system in some countries is more similar to a certain business project, since the creators of the system are too focused on improving the external interaction of citizens and the electronic court. Probably, precisely in connection with this, focused attention was not paid to its regulatory and legal protection, in particular, to its criminal legal protection. The authors draw attention to the fact that the criminal legislation of Estonia does not provide for a special norm that would establish liability for encroachment on electronic judicial systems. Despite the sufficiently extensive software, as well as the existing risks associated with wide access to electronic data, the legislator only indirectly protected information at the expense of other norms. It is concluded that the legislator does not attach special importance to the criminal offense of disrupting the normal operation of automated systems in the bodies and institutions of the justice system. In none of the considered Criminal Codes, the authors did not find at least a similar norm in the section devoted to criminal offenses against justice. This made it possible to state that Ukraine assesses this socially dangerous act more seriously, realizing that the latter can destabilize the judicial system, as well as negatively affect the general criminological situation of Ukraine.

Key words: *automated systems, bodies and institutions of the justice system, criminal offense, unauthorized intervention, criminal legislation, foreign countries, positive experience.*