УДК 343.98
DOI 10.33244/2617-4154.3(16).2024.312-321

Н. С. Топчій,
канд. юрид. наук,
Національна академія внутрішніх справ
e-mail: tv1959@ukr.net
ORCID ID 0000-0002-1726-9028

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЕЛЕКТРОННОМУ КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ В УКРАЇНІ

У статті досліджується питання забезпечення інформаційної безпеки під час ведення електронного кримінального провадження в Україні. Наголошено, що Інтернет-простір став платформою для маніпулювання думкою населення та вчинення кримінальних правопорушень. Учасники кримінальної процесуальної діяльності, використовуючи інформаційні технології, зіштовхуються з труднощами у збиранні, вилученні, копіюванні, переміщенні та перевірці електронної інформації, що міститься в процесуальних документах. Особам, які проводять розслідування кримінальних проваджень, потрібно мати високий рівень компетентності в галузі використання інформаційних технологій і мати технічні засоби для збору доказів.

Визначено, що останні роки зазначалися внесенням ряду змін до національного законодавства з метою регулювання та запобігання зловживанням у сфері засекречення інформації. Закон України «Про основи національної безпеки України» зробив значний внесок у правову основу створення системи та органів захисту інформації, визначивши загрози національній безпеці в інформаційній сфері, а саме: обмеження свободи слова та доступу громадян до інформації; розповсюдження культу насильства, жорстокості та порнографії через засоби масової інформації; випадки комп'ютерної злочинності й комп'ютерного тероризму; розголошення інформації, що становить державну та іншу, визначену законом таємницю, а також конфіденційної інформації, що належить державі або спрямована на задоволення потреб і національних інтересів суспільства й держави; спроби маніпулювання суспільною свідомістю, включаючи поширення недостовірної, неповної або прихованої інформації.

Зроблено висновок, що електронне кримінальне провадження є формою кримінальної процесуальної діяльності, яка ґрунтується на складових алгоритмах автоматизованих кримінальних процедур, що включають Єдиний реєстр досудових розслідувань та інтегровані з ним електронні інформаційні системи.

Ключові слова: *електронне кримінальне провадження, інформаційна безпека, досудове розслідування, кримінальне провадження.*

Постановка проблеми. З моменту проголошення незалежності України 24 серпня 1991 року почалося створення системи захисту інформації держави. Цей процес включав розробку нормативно-правової бази для регулювання системи й органів захисту інформації з обмеженим доступом.

На сьогодні електронні програмні продукти стали невід'ємною частиною сучасного кримінального процесу, забезпечуючи системне управління кримінальним провадженням.

Як зазначають Н. Лугіна та В. Бойко у своїй науковій праці, «в епоху інформаційних технологій безпеці у віртуальному просторі варто приділяти велику увагу. Однак зі швидкими темпами науково-технічного розвитку людське суспільство переміщує багато сфер суспільного життя в кіберпростір, що надає широкі можливості злочинцям здійснювати свою протиправну діяльність. Ураховуючи курс України на входження у світовий інформаційний простір, ми переконані в необхідності створення національної моделі забезпечення кібербезпеки держави, громадян, а також підприємств, установ та організацій» [1, с. 43].

Впровадження електронних засобів у кримінальний процес, зокрема внесення до Кримінально-процесуального кодексу України 2001 року статті 87-1, яка регламентує процесуальний порядок застосування технічних засобів фіксації під час судового засідання, свідчить про поступовий перехід кримінальної процесуальної діяльності з паперового формату в електронний, що є типовим для багатьох країн світу.

У зв'язку зі швидкою інформатизацією суспільства в усіх сферах реформування кримінального процесу в Україні вимагає впровадження електронного кримінального провадження, що є об'єктивно необхідним. Сучасна практика кримінального провадження демонструє зростаючу тенденцію до активного використання інноваційних інструментів, як-от спеціалізоване програмне забезпечення для електронного здійснення кримінального процесу. Сьогодні це включає автоматизовану систему документообігу суду, Єдиний реєстр досудових розслідувань, Єдиний реєстр адвокатів України, Єдиний державний реєстр судових рішень та інші інструменти. Однак кожен з цих засобів повинен враховувати процесуальний статус і характер оброблюваної та збереженої інформації, а також підлягати аналізу й відповідати вимогам щодо її захисту, які не завжди є достатніми.

Інтернет-простір став середовищем для маніпуляції громадською думкою та вчинення кримінальних правопорушень. Учасники кримінального процесу, використовуючи інформаційні технології, стикаються з труднощами під час збирання, вилучення, копіювання, переміщення та перевірки електронної інформації в процесуальних документах. Органи розслідування повинні мати високий рівень знань у сфері інформаційних технологій і володіти технічними засобами для збору доказів.

Для досягнення основних цілей кримінального провадження в умовах переходу до електронної форми потрібно створити високоефективну систему електронної співпраці. Ця система має забезпечити швидке, якісне та всебічне розслідування злочинів. Електронне кримінальне провадження включає використання електронних інформаційних систем під час розслідування.

Аналіз останніх досліджень і публікацій. Тематика електронного кримінального провадження (далі – ЕКП) є відносно новою для наукових досліджень у галузі кримінального процесу. В останні роки українські науковці, наприклад А. Столітній, аналізують це питання. Проблема правового забезпечення інформаційної безпеки також вивчається в роботах спеціалістів з інформаційного права, як-от Б. А. Кормич, О. Г. Ярема, С. С. Єсімов, а також у контексті національної безпеки, наприклад, О. Д. Довгань, К. І. Беляков. Більшість наукових досліджень акцентують увагу на комплексному характері цієї проблеми. Також проводяться дослідження з питань доказування на основі електронних доказів, і теоретичні роботи з цього приводу створили науковці І. Бевзюк, О. Жученко, А. Калін, І. Каланча, О. Колотило, Т. Павлова, Д. Патрелюк, А. Столітній, Г. Чигирин та інші. Однак дослідження щодо електронного кримінального провадження та використання інформаційних систем у процесі розслідування вимагають подальшого детального вивчення.

Виклад основного матеріалу. З аналізу теоретичних положень випливає, що інформаційне середовище правореалізації ЕКП складатиметься з електронної системи, побудованої на базі ЄРДР. Крім основних функцій обробки електронної інформації, ця система надає телекомунікаційні засоби для учасників кримінального провадження. Електронне кримінальне провадження також включає взаємодію з електронними системами органів кримінальної юстиції, державними реєстрами та базами даних, а також зовнішніми інформаційними ресурсами для обміну даними, що вимагає інтероперабельності інструменту ЕКП. Створення ЕКП включає перетворення ЄРДР на інформаційно-телекомунікаційну систему та її інтеграцію з інформаційно-аналітичними системами органів кримінальної юстиції, формуючи інтегровану інформаційно-телекомунікаційну систему (далі – ІТС) як інструмент ЕКП. ІТС має потенціал стати стратегічним засобом зв'язку, реалізації прав і фіксації кримінального провадження, і її використання є обов'язковим для професійних учасників кримінального провадження. Вимоги до безпеки ІТС значно вищі через її критичний статус. Оскільки ЕКП має процесуальний статус, можливі незручності для органів кримінальної юстиції у разі непостійного функціонування апаратного забезпечення ІТС, тому важливо забезпечити надійний захист інформаційного ресурсу як об'єкта критичної інформаційної інфраструктури.

Відповідно до Закону України від 25 березня 1992 року № 2229-XII «Про Службу безпеки України» Служба безпеки України стала першим державним органом, що відповідає за захист інформації. Цей Закон надав Службі правовий статус державного правоохоронного органу спеціального призначення, який забезпечує державну безпеку України. Згідно зі статтею 24 цього Закону серед завдань Служби безпеки України є «участь у розробці та здійсненні заходів з охорони державної таємниці й конфіденційної інформації, яка є власністю держави згідно із Законом України «Про державну таємницю» та іншими актами законодавства, а також надання підтримки підприємствам, установам, організаціям та підприємцям у збереженні комерційної таємниці, розголошення якої може завдати шкоди життєво важливим інтересам України відповідно до законодавства» [2].

В останні роки було внесено ряд змін до національного законодавства, спрямованих на регулювання та запобігання зловживанням у сфері засекречення інформації. Закон України «Про основи національної безпеки України» відіграв ключову роль у створенні правової основи для системи та органів захисту інформації, визначивши загрози національній безпеці в інформаційній сфері [3], зокрема: обмеження свободи слова та доступу громадян до інформації; поширення культу насильства, жорстокості та порнографії через засоби масової інформації; випадки комп'ютерної злочинності та комп'ютерного тероризму; розголошення інформації, що становить державну та іншу, визначену законом таємницю, а також конфіденційної інформації, що належить державі або спрямована на задоволення потреб і національних інтересів суспільства та держави; спроби маніпулювання суспільною свідомістю, включаючи поширення недостовірної, неповної або прихованої інформації.

З розвитком телекомунікаційних мереж і збільшенням обсягу інформації, що циркулює в автоматизованих системах, постало питання про правове регулювання поширення та використання інформації через ці засоби. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» встановлює відповідні вимоги та правила. Цей Закон регулює відносини щодо захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, забезпечуючи дотримання прав власності громадян і юридичних осіб на інформацію, а також права власників на захист та обмеження доступу до неї, визначені чинним законодавством. Також Закон України «Про Національну програму інформатизації» розглядає концепцію інформаційного суверенітету держави, яка включає контроль і регулювання потоків інформації з-за меж держави для забезпечення дотримання законів, прав і свобод громадян та національної безпеки. Питання охорони державної таємниці розглядаються і в інших законах. Наприклад, Закон України «Про оперативно-розшукову діяльність» визначає підстави для проведення оперативно-розшукової діяльності, включаючи запити державних органів щодо перевірки осіб, які мають доступ до державної таємниці. Кримінальний кодекс України передбачає відповідальність за правопорушення, пов'язані з державною таємницею. Розділ I «Злочини проти основ національної безпеки України» містить статті 111 «Державна зрада» та 114 «Шпигунство», а розділ XIV «Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності кордонів, забезпечення призову та мобілізації» містить статті 328 «Розголошення державної таємниці» і 329 «Втрата документів, що містять державну таємницю». Кодекс України про адміністративні правопорушення також передбачає адміністративну відповідальність за порушення законодавства про державну таємницю (стаття 212-2) у певних випадках.

Аналізуючи цю тему, важливо звернути увагу на правовий статус електронних носіїв інформації, які містять результати негласних слідчих (розшукових) дій під час досудового розслідування. Наразі КПК України не містить визначення та регламенту щодо використання електронних доказів у кримінальному провадженні. Натомість КПК України надає певні ознаки процесуального статусу електронним носіям інформації, на яких зберігаються результати процесуальних дій, включаючи негласні слідчі (розшукові)

дії. Згідно зі статтею 84 КПК України доказами у кримінальному провадженні є фактичні дані, отримані відповідно до вимог Кодексу, на основі яких слідчий, прокурор, слідчий суддя та суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження й підлягають доказуванню. Серед цих доказів виділяються документи, які є одним із самостійних процесуальних джерел доказів, що використовують в кримінальному провадженні [4].

Відповідно до статті 99 КПК України під терміном «документ» розуміється фізичний носій інформації, створений спеціально для збереження різних видів даних, як-от письмові тексти, аудіозаписи, зображення тощо. Ці дані можуть бути використані як докази в кримінальному провадженні [4].

Серед матеріалів, які можуть бути розглянуті як документи за КПК України, виділяють фотографії, аудіо-, відеозаписи та інші форми інформації, зокрема електронні, якщо вони містять дані, які фігурують у цих документах. Це означає, що електронні носії інформації, які містять записи, зроблені під час процесуальних дій, охоплюючи таємні (розшукові) заходи, аудіо- та відеозаписи, тексти та зображення щодо фактичних даних, що є важливими для розкриття обставин кримінального правопорушення і є об'єктом доказів, також вважаються джерелами доказів згідно з чинним КПК України.

У зазначеній статті передбачено, що до документів, які можуть слугувати джерелами доказів, включаються процесуальні протоколи та їх додатки, які складені відповідно до Кодексу, а також носії інформації, на яких зафіксовані процесуальні дії за допомогою технічних засобів. Водночас сторона кримінального провадження, потерпілий або представник юридичної особи, стосовно якої ведеться провадження, мають зобов'язання надати суду оригінал документа. Під оригіналом документа розуміється сам документ, а оригінальним відображенням електронного документа вважається його представлення, яке має таку саму юридичну силу, як і сам документ. Копії інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах або їх компонентах, створені слідчим або прокурором за допомогою спеціаліста, розглядаються судом як оригінали документа.

Фіксація прогресу та результатів негласних слідчих (розшукових) дій має відбуватися відповідно до чітко встановлених процедур, що передбачені законодавством про кримінальний процес України. Після проведення кожної такої дії складається протокол, до якого, за потреби, додаються відповідні додатки. Сам процес проведення негласних слідчих (розшукових) дій може бути задокументований за допомогою різних технічних та інших засобів.

Протоколи, що містять інформацію про проведення негласних слідчих (розшукових) дій, одночасно з усіма додатками повинні бути передані прокурору не пізніше ніж через двадцять чотири години після завершення цих дій. Прокурор, отримавши такі протоколи, приймає заходи для збереження отриманих предметів і документів, які можуть бути використані в кримінальному провадженні.

Під час розгляду питання про додатки до протоколів негласних слідчих (розшукових) дій важливо керуватися положеннями статті 105 КПК України, де зазначений перелік

таких додатків. Серед них вказані аудіо- та відеозаписи процесуальних дій, носії комп'ютерної інформації та інші матеріали, які пояснюють зміст протоколу.

Щодо легітимізації використання електронних носіїв інформації, на яких зберігаються результати негласних слідчих (розшукових) дій, існують проблеми, пов'язані з процесуальним оформленням процесу та результатів заходів, що включають у себе підготовку до проведення негласних слідчих (розшукових) дій, де використовуються спеціальні технічні засоби для негласного отримання інформації. Досі недостатньо регламентується процедура дослідження відомостей, отриманих у результаті раніше припинених негласних слідчих (розшукових) дій, які зберігаються на електронних носіях інформації.

Чинне кримінальне процесуальне законодавство не надає повних вказівок щодо процедур та оформлення дій слідчих або оперативних працівників, пов'язаних із використанням спеціальних технічних засобів для негласного отримання інформації під час проведення негласних слідчих (розшукових) дій. Навіть у випадках широкого застосування таких засобів, коли проводяться негласні дії, які тимчасово обмежують конституційні права особи, законодавство не конкретизує процедурні вимоги для таких ситуацій. Це важливо розуміти, оскільки ці дії мають процесуальний характер і здійснюються лише в контексті підготовки до проведення негласних слідчих (розшукових) дій. Вони не є «проміжним етапом» таких дій, оскільки відбуваються до їх початку, тобто до безпосереднього отримання та фіксації інформації про кримінальне правопорушення й особу, яка його вчинила за допомогою негласних методів.

З урахуванням цього подібні дії проводяться після прийняття рішення про проведення негласних слідчих (розшукових) дій і тісно пов'язані з ними, тому мають дотримуватись вимог щодо збереження конфіденційності без розголошення відповідного факту. Це природно обмежує проведення та фіксацію таких дій. Наприклад, на відміну від «відкритої» слідчої (розшукової) дії, яка передбачає огляд речей і документів згідно зі статтею 237 КПК України, під час огляду спеціальних технічних засобів негласного отримання інформації не можуть бути присутні поняті, потерпілі, підозрювані або інші учасники кримінального провадження. Замість цього огляд цих засобів, а також їх виготовлення (утворення) зазвичай здійснюють за участю спеціалістів.

Ураховуючи вищезазначене, доцільно використовувати загальні правила фіксації процесуальних дій у кримінальному провадженні, які передбачені КПК України, для документування ходу та результатів виконаних дій. Це означає, що після виконання таких дій може бути складений протокол згідно з вимогами статей 252 та 273 КПК України, до якого можуть бути додані відповідні додатки, якщо необхідно. Важливо зауважити, що, згідно з положеннями статей 103, 104 та 106 КПК України, процесуальні дії під час кримінального провадження фіксуються у відповідних протоколах або на носіях інформації, на яких зафіксовані ці дії за допомогою технічних засобів, що також відображається у протоколах. Ці протоколи складають слідчий або працівники уповноважених оперативних підрозділів за дорученням слідчого.

З іншого боку, Кримінальний процесуальний кодекс України передбачає, що фіксація ходу та результатів процесуальних дій у протоколі здійснюється лише у

виняткових випадках, визначених самим Кодексом. Тому під час інтерпретації норм кримінального процесуального законодавства в таких ситуаціях основним принципом є дотримання принципу верховенства права та інших основних вимог до кримінального провадження, визначених у статтях 7 і 8 Кримінального процесуального кодексу України. Згідно з цими принципами кримінальне провадження повинно здійснюватися з повагою до прав людини, визнанням їх як найвищої цінності та визначенням напряму діяльності держави.

Отже, правильне документування зазначених процесуальних дій, включаючи фіксацію ходу та результатів їх проведення у відповідному протоколі з використанням відеозапису, є ефективним додатковим інструментом, який гарантує захист конституційних прав особи під час проведення негласних слідчих (розшукових) дій. Наявність таких протоколів дозволяє суду перевіряти дотримання засад законності та пріоритету права в процесі підготовки та здійснення негласних слідчих (розшукових) дій. Це має вирішальне значення для оцінки отриманих у результаті цих дій даних як достовірних та прийнятних доказів, а також для визначення законності їх використання в кримінальному провадженні.

Вважаємо, що важливо підкреслити потребу у внесенні системних змін до чинного кримінального процесуального законодавства з метою впровадження електронних носіїв інформації, на яких будуть фіксуватись результати негласних слідчих (розшукових) дій як законні докази в кримінальний процес в Україні. Це сприятиме дотриманню принципів верховенства права під час проведення таких дій і запобіжить непідтвердженим заявам щодо порушення прав особи без підстав.

Розпочати кримінальне провадження можна через внесення відомостей до Єдиного реєстру досудових розслідувань і створення витягу з цього реєстру, а також повідомлення прокурору про початок розслідування. Сьогодні в кримінальному провадженні переважають паперові документи, проте з розвитком електронного документообігу ситуація зміниться, і паперові документи будуть вважатися вторинними, тоді як електронні документи стануть основними.

Питання про ймовірність заміни паперових документів електронними в кримінальному провадженні наразі є предметом дослідження. Впровадження електронного формату може сприяти швидкому збору та фіксації доказів, а також їх передачі іншим учасникам справи, які мають відповідний доступ. Розвиток інформаційних технологій сприяє зростанню кіберзлочинності, що підкреслює важливість забезпечення інформаційної безпеки.

На офіційний Єдиний вебпортал органів виконавчої влади Міністерства юстиції України надійшла інформація щодо електронного провадження у кримінальному процесі. Міністр юстиції висловив позицію, що необхідно перейти від паперової форми документообігу до електронної. Це запровадження кримінальних проваджень у електронному форматі має на меті виправлення недоліків, пов’язаних із провадженням у паперовій формі, як-от зловживання між окремими судами й органами досудового розслідування щодо передачі матеріалів проваджень, надання або отримання матеріалів провадження для ознайомлення й витрату часу працівників прокуратури, слідчих та

органів дізнання на передачу справ. Керівництво Міністерства юстиції України підкреслює потребу в зменшенні зловживань з боку судів та органів досудового розслідування, а перехід від паперового до електронного провадження допоможе виконанню основних завдань Міністерства юстиції України.

Варто зауважити, що розвиток інформаційних технологій сприяв виникненню електронного кримінального розслідування. Проте проведення такого розслідування потребує застосування заходів для збереження інформації. Інформаційна безпека в кримінальному провадженні передбачає захист інформаційного середовища електронного кримінального розслідування за допомогою засобів і методів збереження інформації, які забезпечують ефективне функціонування кримінального провадження та сприяють досягненню його цілей.

Єдиний реєстр досудових розслідувань є центральною базою даних, яка може бути уразливою під час розслідування. У цьому реєстрі зберігається інформація про різні події, як-от повідомлення особи про підозру, зміна підозри, нові підозри, затримання особи, дані щодо розшуку, інформація про об'єднання та виділення матеріалів провадження, завдані збитки, застосування, зміна або скасування запобіжного заходу та інші значущі дані. Важливо забезпечити надійний захист цієї інформації від сторонніх втручань і маніпулювання даними, щоб забезпечити інформаційну безпеку. Існує ризик видалення, спотворення або знищення даних, що може надати злочинцям можливість уникнути відповідальності.

Висновок. Отже, підсумовуючи, варто наголосити, що електронне кримінальне провадження є формою кримінальної процесуальної діяльності, яка базується на алгоритмах автоматизованих кримінальних процедур, що включають Єдиний реєстр досудових розслідувань та інтегровані з ним електронні інформаційні системи.

Впровадження концепції електронного кримінального провадження має такі характеристики: оптимізація процедур досудового розслідування для більш ефективного проведення його стадій; удосконалення контролю й нагляду над процесом розслідування для забезпечення більшої прозорості та відповідності правових стандартів; зменшення витрат з бюджету за допомогою оптимізації процесів і використання електронних ресурсів; зменшення кількості співробітників завдяки можливості автоматизації деяких завдань; усунення бюрократичних процедур і скорочення часу, потрібного для завершення розслідування; підвищення довіри громадськості до правоохоронних органів через більш прозорий та ефективний процес розслідування; спрощення кримінальної процесуальної діяльності через використання автоматизованих алгоритмів та електронних систем; мінімізація ризику корупції через забезпечення прозорості й електронного контролю; використання ефективних методів електронної комунікації для швидкого та безпечного обміну інформацією; автоматизація процесів для зниження ручної праці та підвищення точності й ефективності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лугіна Н. А., Бойко В. В. Європейський досвід подолання кіберзлочинності в Україні в умовах сьогодення. *Нове українське право.* 2022. Випуск 6, том 2. С. 42–46.

2. Про службу безпеки України : Закон України від 25 березня 1992 р. № 2229-XII // База даних «Законодавство України» / ВР України. URL : https://zakon.rada.gov.ua/laws/show/2229-12 (дата звернення: 01.06.2024).

3. Про основи національної безпеки України : Закон України від 19.06.2003 № 964-IV // База даних «Законодавство України» / ВР України. URL : https://zakon.rada.gov.ua/laws/show/964-15 (дата звернення: 01.06.2024).

4. Кримінальний процесуальний кодекс України від 13.04.2012. *Голос України.* 2012. № 90–91.

REFERENCES

1. Luhina N. A., Boiko V. V. Yevropeiskyi dosvid podolannia kiberzlochynnosti v Ukraini v umovakh sohodennia. *Nove ukrainske pravo.* 2022. Vypusk 6, tom 2. S. 42–46.

2. Pro sluzhbu bezpeky Ukrainy : Zakon Ukrainy vid 25 bereznia 1992 r. № 2229-XII // Baza danykh «Zakonodavstvo Ukrainy» / VR Ukrainy. URL : https://zakon.rada.gov.ua/laws/show/2229-12 (data zvernennia: 01.06.2024).

3. Pro osnovy natsionalnoi bezpeky Ukrainy : Zakon Ukrainy vid 19.06.2003 № 964-IV // Baza danykh «Zakonodavstvo Ukrainy» / VR Ukrainy. URL : https://zakon.rada.gov.ua/laws/show/964-15 (data zvernennia: 01.06.2024).

4. Kryminalnyi protsesualnyi kodeks Ukrainy vid 13.04.2012. *Holos Ukrainy.* 2012. № 90–91.

N. S. Topchiy. ENSURING INFORMATION SECURITY IN ELECTRONIC CRIMINAL PROCEEDINGS IN UKRAINE

The article examines the issue of ensuring information security when conducting electronic criminal proceedings in Ukraine. It was emphasized that the Internet has become a platform for manipulating public opinion and committing criminal offenses. Participants in criminal procedural activities, using information technologies, face difficulties in collecting, extracting, copying, moving and checking electronic information contained in procedural documents. Persons who conduct investigations of criminal proceedings must have a high level of competence in the field of information technology use and have technical means for gathering evidence.

It was determined that recent years have been marked by the introduction of a number of changes to national legislation aimed at regulating and preventing abuses in the field of classified information. The Law of Ukraine "On the Basics of National Security of Ukraine" made a significant contribution to the legal basis of the creation of the information protection system and bodies by identifying threats to national security in the information sphere, namely: restrictions on freedom of speech and citizens' access to information; spread of the cult of violence, cruelty and pornography through mass media; cases of computer crime and

computer terrorism; disclosure of information constituting a state and other, legally defined secret, as well as confidential information belonging to the state or aimed at meeting the needs and national interests of society and the state; attempts to manipulate public consciousness, including the dissemination of inaccurate, incomplete or hidden information.

It was concluded that electronic criminal proceedings are a form of criminal procedural activity, which is based on the component algorithms of automated criminal procedures, which include the Unified Register of Pretrial Investigations and electronic information systems integrated with it.

Keywords: *electronic criminal proceedings, information security, pretrial investigation, criminal proceedings.*

Стаття надійшла до редколегії 22 липня 2024 року