УДК / UDC 343.98:004.7
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364419

Валерій Анатолійович Степанов
Український науково-дослідний інститут спеціальної техніки та судових експертиз СБ України
Київ, Україна
ORCID: https://orcid.org/0000-0002-5249-6883
Юрій Васильович Челпан
Український науково-дослідний інститут спеціальної техніки та судових експертиз СБ України
Київ, Україна
ORCID: https://orcid.org/0009-0007-3540-6421

РІЗНОВИДИ ПЕРЕХОПЛЕННЯ ІНФОРМАЦІЇ В ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖАХ УКРАЇНИ

Анотація. *Стаття присвячена систематизації інформації щодо різновидів перехоплення інформації в електронних комунікаційних мережах України та їх змісту. З цією метою проаналізовані діючі закони України та з врахуванням реалій сьогодення проєкт Закону України "Про перехоплення телекомунікацій" від 21.03.2005 № 4042-2. Визначено, що перехоплення інформації в електронних комунікаційних мережах України проводиться під час здійснення оперативно-розшукових, оперативно-технічних пошукових, розвідувальних заходів та негласних слідчих (розшукових) дій.*

Ключові слова: *електронна комунікаційна мережа, негласна слідча (розшукова) дія, оперативно-розшуковий захід, оперативно-технічний пошуковий захід, перехоплення інформації, розвідувальний захід.*

Valerii A. Stepanov
The Ukrainian scientific and research Institute of special equipment and forenscic expertise of the Security Service of Ukraine
Kyiv Ukraine
Yurii V. Chelpan
The Ukrainian scientific and research Institute of special equipment and forenscic expertise of the Security Service of Ukraine
Kyiv Ukraine
ORCID: https://orcid.org/0009-0007-3540-6421.

THE VARIOUS TYPES OF INFORMATION INTERCEPTION IN ELECTRONIC COMMUNICATION NETWORKS IN UKRAINE

Summary. *The article is devoted to the systematization of information on the types of information interception in electronic communication networks of Ukraine and their content. For this purpose, the current laws of Ukraine were analyzed, taking into account the realities of today, as well as the draft Law of Ukraine "On Interception of Telecommunications" dated March 21, 2005, No. 4042-2. It has been determined that interception of information in electronic communication networks*

in Ukraine is carried out during operative-search, operative-technical search, intelligence measures, and covert investigative (search) actions.

Keywords: *electronic communication network, covert investigative (search) action, operative-search measure, operative-technical search measure, interception of information, intelligence measure.*

Постановка проблеми. Аналіз досвіду країн Європи щодо перехоплення (зняття) інформації в електронних комунікаційних мережах, наведений в монографії [1], дозволяє зробити висновок, що уряди країн та суспільство розуміють необхідність застосування перехоплення інформації як адекватного механізму попередження та розслідування злочинів під час збереження оптимального балансу між необхідністю забезпечення як прав людини на інформацію, повагу до таємниці кореспонденції, приватного, сімейного життя та свободу вираження, так і забезпеченням безпеки суспільства та держави. Законодавство України передбачає можливість проведення підрозділами уповноважених органів перехоплення (зняття) інформації в електронних комунікаційних мережах з використанням єдиної системи технічних засобів.

На жаль, у законодавстві України та у працях науковців відсутня систематизована інформація щодо різновидів перехоплення інформації в електронних комунікаційних мережах України та їх змісту.

Результати аналізу наукових публікацій. В статті 16 проєкту Закону України "Про перехоплення телекомунікацій" від 21.03.2005 № 4042-2 [2] були визначені наступні види перехоплення телекомунікацій: оперативно-розшуковий захід оперативно-розшукової діяльності, а також оперативно-технічний пошуковий захід контррозвідувальної діяльності та боротьби з тероризмом. Автором цього проєкту Закону та ініціатором його подання до Верховної Ради України був народний депутат Ю. А. Кармазін. Активну допомогу в підготовці зазначеного проєкту Закону України [2] надавала Служба безпеки України. У розділах ІІ та ІІІ проєкту Закону України "Про перехоплення телекомунікацій" від 21.03.2005 № 4042-2 [2] було надано зміст перехоплення телекомунікацій в інтересах відповідно оперативно-розшукової діяльності, а також контррозвідувальної діяльності і боротьби з тероризмом. Після появи зазначеного проєкту Закону України [2] було прийнято в 2012 році нову редакцію Кримінального процесуального кодексу України [3], Закон України "Про розвідку" від 17.09.2020 № 912-IX [4], внесені зміни в закони України "Про оперативно-розшукову діяльність" від 18.02.1992 № 2135-XII [5], "Про контррозвідувальну діяльність" від 26.12.2002 № 374 [6] та "Про боротьбу з тероризмом" від 20.03.2003 № 638-IV [7]. Як наслідок, на даний час потребують коригування положення, визначені в проєкті Закону України [2], та необхідна систематизація інформації щодо різновидів перехоплення інформації в електронних комунікаційних мережах України та їх змісту.

Отже, **метою цієї статті** є проведення систематизації інформації щодо різновидів перехоплення інформації в електронних комунікаційних мережах України та їх змісту та надання результатів дослідження на розгляд читачам.

Виклад основного матеріалу. Поняття та особливості електронної комунікаційної мережі визначено у Законі України "Про електронні комунікації" від 16.12.2020 № 1089-IX [8]. Відповідно до зазначеного Закону України електронна комунікаційна мережа – це комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг. Поняття перехоплення електронних комунікацій наведено в нормативному документі [9], його вважають оперативно-технічним, контррозвідувальним, розвідувальним заходом або негласною слідчою

(розшуковою) дією, що здійснюється відповідно до законодавства України уповноваженими органами, який (яка) полягає у спостереженні, відборі за визначеними ознаками та фіксації сеансів зв'язку із застосуванням системи перехоплення електронних комунікацій.

Згідно зі статтею 5 Закону України "Про оперативно-розшукову діяльність" [5] однойменна діяльність здійснюється оперативними підрозділами уповноважених органів: Національної поліції, Державного бюро розслідувань, Служби безпеки України, Служби зовнішньої розвідки України, Державної прикордонної служби України, управління державної охорони, органів і установ виконання покарань та слідчих ізоляторів Державної кримінально-виконавчої служби України, розвідувального органу Міністерства оборони України, Національного антикорупційного бюро України та Бюро економічної безпеки України. Водночас з цим відповідно до пункту 9 статті 8 цього Закону України [5] зазначеним підрозділам надається право здійснювати ***оперативно-розшукові заходи*** зі зняття інформації з електронних комунікаційних мереж згідно з положенням статті 263 Кримінального процесуального кодексу України [3]. Зазначені заходи згідно з пунктом 21 статті 8 Закону України [5] проводяться на підставі ухвали слідчого судді, постановленої за клопотанням керівника відповідного оперативного підрозділу або його заступника, погодженого з прокурором. Ці заходи в рамках оперативно-розшукової справи застосовуються виключно з метою запобігання вчиненню тяжкого або особливо тяжкого злочину, запобігання і припинення терористичних актів та інших посягань спеціальних служб іноземних держав та організацій, якщо іншим способом одержати інформацію неможливо. Метою перехоплення (зняття) інформації в електронних комунікаційних мережах як оперативно-розшукового заходу оперативно-розшукової діяльності є пошук і фіксація фактичних даних: про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України [10], для запобігання та припинення правопорушень; про розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій для запобігання та припинення такої діяльності; в інтересах кримінального судочинства для з'ясування істини під час розслідування кримінальних справ, а також отримання інформації в інтересах безпеки громадян, суспільства і держави.

Разом з цим, згідно зі статтею 5 Закону України "Про боротьбу з тероризмом" від 20.03.2003 № 638-IV [7] виключно з метою отримання упереджувальної інформації Служба безпеки України у разі загрози вчинення терористичного акту або під час проведення антитерористичної операції провадить ***оперативно-технічні пошукові заходи*** у системах і каналах електронних комунікацій. Зі свого боку в статті 22 проєкту Закону України "Про перехоплення телекомунікацій" від 21.03.2005 № 4042-2 [2] метою перехоплення телекомунікацій як оперативно-технічного пошукового заходу в інтересах контррозвідувальної діяльності та боротьби з тероризмом вважали своєчасне виявлення інформації про розвідувальну, терористичну та іншу протиправну діяльність спеціальних служб іноземних держав, організацій, груп та осіб на шкоду державній безпеці України, про загрози вчинення терористичного акту для запобігання і своєчасного припинення такої діяльності, ліквідації її наслідків. Додатково слід зазначити, що в статті 7 Закону України "Про контррозвідувальну діяльність" від 26.12.2002 № 374 [6] визначено право підрозділів та співробітників Служби безпеки України здійснювати ***контррозвідувальні заходи***, контррозвідувальний пошук, оперативно-розшукові заходи для виконання завдань та за наявності підстав,

передбачених статтею 6 цього Закону, з використанням оперативно-технічних сил і засобів.

Сутність оперативно-технічних пошукових заходів в електронних комунікаційних мережах полягає в тому, що виявлення осіб і фактів, які становлять оперативний інтерес, відбувається за невстановленими і заздалегідь індивідуально невизначеними ідентифікаційними ознаками, оскільки на початок проведення зазначених заходів відсутня певна, попередньо визначена інформація щодо суб'єктів та об'єктів перехоплення інформації в електронних комунікаційних мережах. На першому етапі цих заходів пошук відомостей здійснюють відгалуженням (відбором) частини потоку даних за встановленими на засадах загальних уявлень критеріями (сигнатурами) протоколів, сервісів і додатків, що властиві для комунікацій під час здійснення окремих видів злочинів, розвідувальної, терористичної та іншої протиправної діяльності. Під сигнатурою розуміють фіксовану послідовність символів, за якою визначається (ідентифікується) поміж інших додаток та/або протокол застосованого інформаційного ресурсу (сервісу) в електронних комунікаційних мережах. В подальшому на другому етапі в частині потоку даних відбувається пошук ідентифікаційних ознак об'єктів перехоплення інформації, поєднаних з суб'єктами перехоплення інформації. Потім на третьому етапі за отриманими ідентифікаційними ознаками здійснюється виділення об'єктів перехоплення інформації (наприклад, службові дані сеансів зв'язку суб'єктів перехоплення інформації). У результаті оперативно-технічних пошукових заходів надходить орієнтувальна інформація. Це дає змогу зробити певне припущення щодо відношення виявлених суб'єктів перехоплення інформації до якого-небудь злочину або протиправної діяльності, тобто встановити формальну тотожність отриманих відомостей з абстрактними моделями злочину або протиправної діяльності.

Зі свого боку в статті 263 глави 21 Кримінального процесуальному кодексу України [3] наведено про ***негласні слідчі (розшукові) дії*** зі зняття інформації з електронних комунікаційних мереж, пов'язані з втручанням у приватне спілкування. В статті 246 цього Кодексу визначено, що негласна слідча (розшукова) дія, як різновид слідчих (розшукових) дій, проводиться у випадках, якщо відомості про кримінальне правопорушення та особу, яка його вчинила, неможливо отримати в інший спосіб. Негласна слідча (розшукова) дія, передбачена статтею 263 зазначеного Кодексу, проводиться на підставі ухвали слідчого судді виключно у кримінальному провадженні щодо тяжкого або особливо тяжкого злочинів. Рішення про проведення цієї негласної слідчої (розшукової) дії приймає слідчий, прокурор, а у випадках, передбачених цим Кодексом, - слідчий суддя за клопотанням прокурора або за клопотанням слідчого, погодженого з прокурором. Слідчий зобов'язаний повідомити прокурора про прийняття рішення щодо проведення вказаної дії та отриманий результат. При цьому прокурор має право заборонити проведення або припинити подальше проведення зазначеної негласної слідчої (розшукової) дії.

Розглянемо особливості проведення негласної слідчої (розшукової) дії зі зняття інформації з електронних комунікаційних мереж. По-перше, вказане зняття інформації проводиться без відома осіб, які використовують засоби електронних комунікацій для передавання інформації. По-друге, в ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження (споживача послуг), електронну комунікаційну мережу, кінцеве (термінальне) обладнання, на якому може здійснюватися втручання у приватне спілкування. По-третє, зняття інформації з електронних комунікаційних мереж полягає у проведенні з

застосуванням відповідної єдиної системи технічних засобів спостереження, відбору та фіксації змісту інформації, яка передається особою та має значення для досудового розслідування, а також одержанні, перетворенні і фіксації різних видів сигналів, що передаються каналами зв'язку. По-четверте, зняття інформації з електронних комунікаційних мереж покладається на уповноважені підрозділи органів Національної поліції, Бюро економічної безпеки України, Національного антикорупційного бюро України, Державного бюро розслідувань та органів безпеки. По-п'яте, керівники та працівники постачальників послуг або мереж електронних комунікацій зобов'язані сприяти виконанню дій зі зняття інформації з електронних комунікаційних мереж, вживати необхідних заходів щодо нерозголошення факту проведення таких дій та отриманої інформації, зберігати її в незмінному вигляді.

У науково-практичному коментарі до Кримінального процесуальному кодексу України за редакцією С.В. Ківалова та С.І. Кравченко [11] вказується можливість здійснення зняття інформації з електронних комунікаційних (транспортних телекомунікаційних) мереж в інтересах національної безпеки та запобігання злочинів під час стратегічного моніторингу населення, що визнається Європейським судом з прав людини (European court of human rights) [12] як необхідність в демократичному суспільстві. В цьому науково-практичному коментарі зазначено, що отримавши ухвалу слідчого судді про дозвіл на зняття інформації з електронних комунікаційних (транспортних телекомунікаційних) мереж, слідчий, в порядку пункту 2 частi 2 статті 40, статті 41, частi 6 статті 246, частi 4 статті 263 Кримінального процесуальному кодексу України [3], письмово доручає відповідному оперативно-технічному підрозділу проведення зняття інформації з електронних комунікаційних (транспортних телекомунікаційних) мереж. За результатами проведення зняття інформації з цих мереж уповноважений оперативно-технічного підрозділу, який здійснював зазначену негласну слідчу (розшукову) дію, складає протокол згідно з вимогами статей 104–107, 252 та 265 вказаного Кодексу та протягом двадцяти чотирьох годин з моменту припинення негласної слідчої (розшукової) дії повинен направити його прокурору[11].

В статті О.В. Грибовського [13] наведено, що оперативно-розшукові заходи та негласні слідчі (розшукові) дії різняться за змістом проваджуваних заходів (дій). Оперативно-розшукові заходи проводяться з метою виявлення, попередження та розкриття злочину, що готується, а негласні слідчі (розшукові) дії направлені на виявлення та перевірку інформації, необхідної для розслідування вже вчиненого злочину.

Крім зазначеного вище відповідно до статті 15 Закону України "Про розвідку" від 17.09.2020 № 912-IX [4] розвідувальні органи стосовно особи, яка перебуває на території України, можуть на підставі рішення суду проводити окремі ***розвідувальні заходи***, що полягають у знятті інформації з електронних комунікаційних (транспортних телекомунікаційних) мереж шляхом відбору та фіксації змісту відповідних відомостей або даних, що передаються або отримуються особою. На підставі також виключно рішення суду такі розвідувальні заходи проводяться за умов, якщо вони безпосередньо пов'язані із здійсненням розвідувальної діяльності за межами України або спрямовані на здобування розвідувальної інформації, що має джерело походження за межами України. В цьому Законі під поняттям розвідувальний захід розуміють комплекс дій та рішень розвідувального органу та/або іншого суб'єкта розвідувального співтовариства із застосуванням методів, сил і засобів розвідки.

Розвідувальний орган може розпочати проведення розвідувальних заходів стосовно особи, яка перебуває на території України на законних підставах і яку ідентифіковано

під час проведення розвідувального заходу за пошуковими критеріями, виключно на підставі рішення суду. У такому випадку за рішенням керівника розвідувального органу проведення розвідувального заходу за пошуковими критеріями може бути продовжено на строк до отримання рішення суду, але не більше ніж на 72 години з моменту ідентифікації особи. Зняття інформації з електронних комунікаційних (транспортних телекомунікаційних) мереж постачальників послуг, які надають послуги мобільного та/або фіксованого зв'язку, забезпечується системою технічних засобів, що використовується всіма розвідувальними органами на умовах автономного доступу до інформації у порядку, визначеному законодавством.

Під час проведення розвідувальних заходів зі зняття інформації з електронних комунікаційних мереж можуть бути застосовані крім зазначеної системи технічних засобів, також технічні засоби розвідки - технічні засоби, устаткування, апаратура, прилади, пристрої, препарати та інші вироби, спеціально розроблені, створені, запрограмовані, придбані, модернізовані, пристосовані і призначені для здійснення та забезпечення розвідувальної діяльності.

Розвідувальні заходи з перехоплення (зі зняття) інформації в електронних комунікаційних мережах України відповідно до цього Закону мають право проводити Служба зовнішньої розвідки України, розвідувальний орган Міністерства оборони України, розвідувальний орган центрального органу виконавчої влади, що реалізує державну політику у сфері охорони державного кордону, та Служба безпеки України (з метою отримання інформації в інтересах контррозвідки).

У статті [14] зазначено, що через недоліки законодавчої техніки назва вищезгаданого розвідувального заходу не зазнала змін у частині приведення її у відповідність до термінології Закону України "Про електронні комунікації" [8]. Саме в статті [14] виділено основні правові аспекти розмежування негласної слідчої (розшукової) дії зі зняття інформації з електронних комунікаційних мереж з аналогічним за назвою розвідувальним заходом щодо переліку органів, уповноважених на проведення перехоплення (зняття) інформації, умов проведення та процесу надання дозволу на його проведення. Особливо слід звернути увагу, що розвідувальний захід на відміну від аналогічної негласної слідчої (розшукової) дії або оперативно-розшукового заходу не потребує погодження прокурором клопотання. Це зумовлено відсутністю прокурорського нагляду за розвідувальною діяльністю.

Висновки.

Перехоплення інформації в електронних комунікаційних мережах України проводиться під час здійснення оперативно-розшукових, оперативно-технічних пошукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій. Слід зазначити, що оперативно-технічні пошукові заходи проводяться в інтересах контррозвідувальної діяльності та боротьби з тероризмом.

На даний час, поряд з декларованою владою імплементацією європейських стандартів до вітчизняного законодавства, так і не прийнято Закон України "Про перехоплення інформації в електронних комунікаційних мережах", який би визначив механізми отримання дозволів, мету, підстави та порядок проведення перехоплення інформації в електронних комунікаційних мережах України під час здійснення зазначених заходів та дії.

Відповідно до реалій сьогодення під час розробки проєкту Закону України "Про перехоплення інформації в електронних комунікаційних мережах" пропонуємо за основу саме проєкт Закону України "Про перехоплення телекомунікацій" від 21.03.2005 р. № 4042-2 з урахуванням змін в законодавстві України та концептуальних вимог до

перехоплення інформації, встановлених технічним комітетом законного перехоплення TC LI (Technical committee lawful interception) Європейського інституту телекомунікаційних стандартів ETSI (European telecommunications standards institute).

ПОДЯКИ: Немає

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Використана література

1. Степанов В.А., Войтенко М.В., Говоруха В.І., Прокопченко С.В., Сивобородько А.В., Челпан Ю.В. Регулювання у сфері законного перехоплення інформації в електронних комунікаційних мережах в Європі та Україні: монографія. Київ: ІСТЕ СБУ. 2025. 205 с.

2. Про перехоплення телекомунікацій: проєкт Закону України від 21.03.2005 № 4042-2. URL: w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?id=&pf3516=4042-2&skl=5 (дата звернення 04.03.2026).

3. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. *Відомості Верховної Ради України*. 2013. № 9-10, № 11-12, № 13. Ст. 88. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 04.03.2026).

4. Про розвідку: Закон України від 17.09.2020 № 912-IX. Голос України від 23.10.2020 № 195. URL: zakon.rada.gov.ua/laws/show/912-20#Text (дата звернення 04.03.2026).

5. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-XII. *Відомості Верховної Ради України*. 1992. № 22. Ст. 303. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 04.03.2026).

6. Про контррозвідувальну діяльність: Закон України від 26.12.2002 № 374. *Відомості Верховної Ради України*. 2003. № 13. Ст. 89. URL: https://zakon.rada.gov.ua/laws/show/374-15#Text (дата звернення: 05.03.2026).

7. Про боротьбу з тероризмом: Закон України від 20.03.2003 № 638-IV. *Відомості Верховної Ради України*. 2003. № 25. Ст. 180. URL: https://zakon.rada.gov.ua/laws/show/638-15#Text (дата звернення: 05.03.2026).

8. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. *Голос України* від 16.01.2021 №7. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення 04.03.2026).

9. Технічні засоби для здійснення уповноваженими органами оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій в електронних комунікаційних мережах загального користування України. Загальні технічні вимоги: наказ Служби безпеки України і Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 31.12.2021 року № 460/781. URL: ssu.gov.ua/ uploads/ documents/ 2022/01/24/ztv-31122021.pdf (дата звернення 04.03.2026).

10. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України*. 2001. № 25-26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/ 2341-14#Text (дата звернення: 04.03.2026).

11. Науково-практичний коментар Кримінального процесуального кодексу України/за ред. С.В. Ківалова, С.І. Кравченко. Одеса: Фенікс. 2020. 924 с. URL: dspace.onua.edu.ua/items/ 6f995a96-7f0d-4217-83fe-801547652080 (дата звернення 04.03.2026).

12. Європейський суд з прав людини. URL: https://www.echr.coe.int/documents/ d/echr/ questions_answers_ukr (дата звернення 12.12.2025).

13. Грибовський О.В. Оперативно-розшукові заходи та негласні слідчі (розшукові) дії під час виявлення й фіксації одержання неправомірної вигоди. *Юридичний часопис Національної академії внутрішніх справ*. № 1. 2015. С. 180-190. URL: http://nbuv.gov.ua/ UJRN/aymvs_2015_1_18 (дата звернення 10.03.2026).

14. Луцик В.В. Зняття інформації з електронних комунікаційних мереж: фокус новел. *Юридичний науковий електронний журнал.* № 8. 2022. С. 500-504. URL: Isej.org.ua/8_2022/113.pdf (дата звернення 10.03.2026).

Валерій Анатолійович Степанов
кандидат технічних наук
науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
03113, вул. Миколи Василенка,3, Київ, Україна
email: valerii_stepanov@ukr.net
Юрій Васильович Челпан
провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
03113, вул. Миколи Василенка,3, Київ, Україна
email: yuriychelpan@gmail.com

Valerii A. Stepanov
Candidate of technical sciences
Researcher, The Ukrainian scientific and research Institute of special equipment and forenscic expertise of the Security Service of Ukraine
email: valerii_stepanov@ukr.net
03113 Kyiv Ukraine M. Vasylenka Str.
Yurii V. Chelpan
Leading researcher, The Ukrainian scientific and research Institute of special equipment and forenscic expertise of the Security Service of Ukraine
03113 Kyiv Ukraine M. Vasylenka Str.
email: yuriychelpan@gmail.com

Рекомендоване цитування: Степанов В.А., Челпан Ю.В. Різновиди перехоплення інформації в електронних комунікаційних мережах України. *Інформація і право*. № 2(57)/2026. 2026. С. 184-191. https://doi.org/10.37750/2616-6798.2026.2(57).364419

Suggested Citation: Stepanov V., Chelpan Yu. (2026) The Various Types of Information Interception in Electronic Communication Networks in Ukraine. *Information and Law*. 2(57)/2026. 184-191. https://doi.org/10.37750/2616-6798.2026.2(57).364419

Дата надходження статті до редакції: 04.04.2026 р.
Дата прийняття статті до друку після рецензування: 11.04.2026 р.
Дата публікації (оприлюднення): 26.05.2026 р.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~