

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ  
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
ВНУТРІШНІХ СПРАВ**

**Факультет № 6**

**Кафедра кримінального процесу, криміналістики та експертології**

**ЛЕКЦІЯ**

з навчальної дисципліни **Організація та проведення негласних  
слідчих (розшукових) дій**  
обов'язкових/вибіркових компонент  
освітньої програми першого (бакалаврського) рівня вищої освіти

**за темою –Зняття інформації з електронних інформаційних систем.**

**Харків 2023**

**ЗАТВЕРДЖЕНО**

Науково-методичною радою  
Харківського національного  
університету внутрішніх справ  
Протокол № 7 від 30.08.2023 р.

**СХВАЛЕНО**

Вченою радою факультету № 6  
Харківського національного  
університету внутрішніх справ  
Протокол № 7 від 25.08. 2023 р.

**ПОГОДЖЕНО**

Секцією науково-методичної ради  
ХНУВС з юридичних дисциплін  
Протокол № 7 від 29.08.2023 р.

Розглянуто на засіданні кафедри кримінального процесу, криміналістики та експертології факультету № 6 ХНУВС (протокол від 21.08.2023 № 7)

Розробник:

1. Професор кафедри кримінального процесу, криміналістики та експертології факультету № 6 ХНУВС, доктор юридичних наук, професор Пчолкін В.Д.

Рецензенти:

1. Професор кафедри криміналістики, судової експертології та медичної підготовки факультету № 1 Харківського національного університету внутрішніх справ, доктор юридичних наук, професор Степанюк Р.Л.

2. Доцент кафедри криміналістики Національного юридичного університету ім. Ярослава Мудрого кандидат юридичних наук, доцент Мусієнко О.Л.

## План лекції

- 1. Правове регулювання зняття інформації з електронних інформаційних систем.**
- 2. Порядок отримання інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту.**
- 3. Організація проведення НСРД – зняття інформації з електронних інформаційних систем.**

## Рекомендована література:

1. Конституція України // Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
2. Про захист прав людини і основоположних свобод: Конвенція Ради Європи від 4 листопада 1950 р. (в ред. від 1 червня 2010 р.) (Зі змінами та доповненнями, внесеними Протоколом № 11 від 11 трав. 1994 р., Протоколом № 14 від 13 трав. 2004 р.): URL: [http://zakon2.rada.gov.ua/laws/show/995\\_004](http://zakon2.rada.gov.ua/laws/show/995_004).
3. Про Національну поліцію: Закон України від 2 лип. 2015 р. № 580- VIII: URL: <http://zakon5.rada.gov.ua/laws/show/580-19>.
4. Закон України «Про оперативно-розшукову діяльність» // Відомості Верховної Ради України, 1992, N 22, ст.303 : <https://zakon.rada.gov.ua/laws/show/2135-12/ed20130811#Text>
5. Закон України «Про судову експертизу» // Відомості Верховної Ради України, 1994, N 28, ст.232 : <https://zakon.rada.gov.ua/laws/show/4038-12#Text>
6. Закон України «Про наркотичні засоби, психотропні речовини і прекурсори» // Відомості Верховної Ради України, 1995, N 10, ст.60 : <https://zakon.rada.gov.ua/laws/show/60/95-%D0%B2%D1%80#Text>
7. Кримінальний кодекс України // Відомості Верховної Ради України, 2001, № 25-26, ст.131 : <https://zakon.rada.gov.ua/laws/show/2341-14#Text>
8. Кримінальний процесуальний кодекс України від 13 квітня 2012 р.// Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88 : <https://zakon.rada.gov.ua/laws/show/4651-17#Text>
9. Закон України «Про прокуратуру» від 14.10.2014 № 1697-18 [Електронний ресурс] // База даних «Законодавство України». Верховна Рада України : URL : <https://zakon.rada.gov.ua/laws/show/1697-18>Закон України «Про службу безпеки України» прийнятий 25 березня 1992 року N 2229-XII // Відомості Верховної Ради України, 1992, №27, ст.382.
10. Закон України «Про державну таємницю» прийнятий 21 січня 1994 року N 3855-XII (із змінами і доповненнями від 19 червня 2003 року)
- 11.акон України «Про контррозвідувальну діяльність» прийнятий 26 грудня 2002 року N 374-IV // Відомості Верховної Ради України. 2003. № 374.

Ст. 482.

12. Закон України «Про Державну прикордонну службу України» прийнятий 3 квітня 2003 року N 661-IV
13. Закон України «Про державний захист працівників суду і правоохоронних органів» від 23 грудня 1993 р. № 3781-XII [Електронний ресурс]: Офіційний веб-портал Верховної Ради України. Реж. доступу: <http://zakon4.rada.gov.ua/laws/show/3781-12>
14. Закон України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» від 23 грудня 1993 р. № 3782-XII [Електронний ресурс]: Офіційний веб-портал Верховної Ради України. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/3782-12>
15. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, затверджена Наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України 16.11.2012 № 14/1042/516/1199/936/1687/5
16. Про організацію діяльності органів досудового розслідування Національної поліції України : наказ МВС України від 06.07.2017 № 570 [Електронний ресурс]. URL : <https://zakon.rada.gov.ua/laws/show/z0918-17>
17. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : наказ МВС України від 07.07.2017 № 575 [Електронний ресурс] // База даних «Законодавство України». Верховна Рада України. URL : <http://zakon5.rada.gov.ua/laws/show/z0937-17>

### Інформаційні ресурси

- – Національна парламентська бібліотека України.
- офіційний веб-сайт Генеральної прокуратури України.
- <http://www.minjust.gov.ua> – Офіційний веб-сайт Міністерства юстиції України.
- <http://www.mvs.gov.ua> – офіційний веб-сайт МВС України.
- <http://www.nbu.gov.ua> – Національної бібліотеки України ім. В.І. Вернадського.
- <http://www.police.ua> – Форум працівників МВС України.
- <http://www.portal.rada.gov.ua> – офіційний веб-сайт Верховної Ради України.
- – єдиний реєстр судових рішень в Україні.
- <http://www.scourt.gov.ua> – офіційний веб-сайт Верховного Суду України.

## **1. Правове регулювання зняття інформації з електронних інформаційних систем.**

**Право на таємницю листування, телефонних переговорів, телеграфної та іншої кореспонденції** є особистісним, немайновим правом, що традиційно належить до основних природних прав людини. Особисте життя кожного громадянина не повинне виходити за межі, які визначила для себе кожна людина. Саме наявність такого права забезпечує особі захист від будь-якого проникнення в її особисте життя, а саме прослуховування телефонних розмов, знайомлення з її листами чи повідомленнями, а також розголошення їх змісту чи самого факту листування або розмови.

Держава, яка визнається демократичною, повинна забезпечити реалізацію таких прав і свобод, а також надати механізм правового захисту в разі їх незаконного порушення.

**Правовою основою зняття інформації з електронних інформаційних систем є ст. 31 Конституції України, Глава 21 Кримінального процесуального кодексу України, а також п. 9 ч. 1 ст. 8 та ч. 2 ст. 8 Закону України «Про оперативно-розшукову діяльність», ст. 15 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю», ст.ст. 5, 8 Закону України «Про державний захист працівників суду і правоохоронних органів», ч. 1 ст. 7 Закону України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві».**

Відповідно до ст. 31 Конституції України кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.

Верховною Радою України у 2003р. було прийнято Закон «Про телекомунікації», ст. 9 якого зазначає, що таємниця телефонних розмов, листування, телеграфної та іншої кореспонденції захищається Конституцією та Законами України. Те ж саме стосується таємниці поштових відправлень, про що йдеться в ст.6 Закону України «Про поштовий зв'язок».

Органи виконавчої влади не мають повноваження безпідставно обмежувати право людини на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. Такі обмеження визнаються законними лише в разі наявності судового арешту на вилучення відомостей, процесуальний порядок отримання якого зазначений у ст. 165 КПК України.

Особи, що здійснюють законне зняття інформації з каналів зв'язку, зобов'язані вжити заходів з метою нерозголошення виявленої інформації іншим фізичним чи юридичним особам.

**Більш вичерпніший зміст права на таємницю кореспонденції знаходимо у ст. 306 ЦК України:**

– фізична особа має право на таємницю листування, телеграм, телефонних розмов, телеграфних повідомлень та інших видів кореспонденції. Листи, телеграми тощо є власністю адресата.

– листи, телеграми та інші види кореспонденції можуть використовуватися, зокрема шляхом опублікування, лише за згодою особи, яка направила їх, та адресата. Якщо кореспонденція стосується особистого життя іншої фізичної особи, для її використання, зокрема шляхом опублікування, потрібна згода цієї особи.

– кореспонденція, яка стосується фізичної особи, може бути долучена до судової справи лише у разі, якщо в ній містяться докази, що мають значення для вирішення справи. Інформація, яка міститься в такій кореспонденції, не підлягає розголошенню.

– порушення таємниці кореспонденції може бути дозволено судом у випадках, встановлених законом, з метою запобігання злочинів чи під час кримінального провадження, якщо іншими способами одержати інформацію неможливо.

**За порушення таємниці листування чи іншої кореспонденції, що передається через комп'ютер, передбачена кримінальна відповідальність за ст. 163 КК України.** Отже, приватне життя громадянина охороняється державою, а втручання в його сферу законодавчо регламентовано.

Захист цього права гарантує також **КПК України, а саме ч. 2 ст.14 «Таємниця спілкування»:** де зазначається, що втручання у таємницю спілкування можливе лише на підставі судового рішення у випадках, передбачених цим Кодексом, з метою виявлення та запобігання тяжкому чи особливо тяжкому злочину, встановлення його обставин, особи, яка вчинила злочин, якщо в інший спосіб неможливо досягти цієї меті».

**Глава 21 Кримінального процесуального кодексу України** регламентує порядок проведення НСРД, що тимчасово обмежують права та свободи громадян.

Наприклад, згідно ст. 254 КПК України передбачено – «Заходи щодо захисту інформації, отриманої в результаті проведення негласних слідчих (розшукових) дій», а ст. 255 КПК – «Заходи щодо захисту інформації, що не використовується у кримінальному провадженні».

Загальні положення про втручання у приватне спілкування викладені у ст.. 258 КПК де зазначається, що;

- 1. Ніхто не може зазнавати втручання у приватне спілкування без ухвали слідчого судді.*
- 2. Прокурор, слідчий за погодженням з прокурором зобов'язаний звернутися до слідчого судді з клопотанням про дозвіл на втручання у приватне спілкування в порядку, передбаченому статтями 246, 248, 249 цього Кодексу, якщо будь-яка слідча (розшукова) дія включатиме таке втручання.*
- 3. Спілкуванням є передання інформації у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою засобів зв'язку будь-якого типу. Спілкування є приватним, якщо інформація передається та зберігається за*

*таких фізичних чи юридичних умов, при яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб.*

*4. Втручанням у приватне спілкування є доступ до змісту спілкування за умов, якщо учасники спілкування мають достатні підстави вважати, що спілкування є приватним. Різновидами втручання в приватне спілкування є:*

*1) аудіо-, відеоконтроль особи;*

*2) арешт, огляд і виїмка кореспонденції;*

*3) зняття інформації з транспортних телекомунікаційних мереж;*

*4) зняття інформації з електронних інформаційних систем.*

*5. Втручання у приватне спілкування захисника, священнослужителя з підозрюваним, обвинуваченим, засудженим, виправданим заборонене.*

Зняття інформації з електронних інформаційних систем є різновидом втручання у приватне спілкування. Ст. 264 КПК України передбачає – «Зняття інформації з електронних інформаційних систем», як на підставі ухвали слідчого судді, так і порядок здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту для проведення яких не потрібен дозвіл слідчого судді.

Сутність зняття інформації з електронних інформаційних систем полягає в тому, що орган, який її здійснює, на підставі ухвали слідчого судді проводить запис певної інформації, якою обмінюються обвинувачений (підозрюваний) з іншими особами, або інші особи з підозрюваним (обвинуваченим), або підозрювані (обвинувачені) між собою, і повідомляє про це слідчого, який її досліджує.

**Підставами проведення** негласної слідчої (розшукової) діє, зокрема зняття інформації з електронних інформаційних систем – є необхідність отримання відомостей про злочин та особу, яка його вчинила, якщо неможливо отримати їх в інший спосіб.

Проведення зняття інформації з електронних інформаційних систем здійснюється лише **за вмотивованим рішенням слідчого судді** і мають винятковий та тимчасовий характер. Зазначені дії застосовуються з метою запобігання тяжкого чи особливо тяжкого злочину, якщо іншим способом одержати інформацію неможливо.

**Ініціаторами** зняття інформації з електронних інформаційних систем є слідчий, який здійснює досудове розслідування злочину, або за його дорученням – уповноважені оперативні підрозділи НП України, органів безпеки, органів, що здійснюють контроль за додержанням податкового законодавства, органів Державної пенітенціарної служби України, органів Державної прикордонної служби України, органів Державної митної служби України. За рішенням слідчого чи прокурора до проведення негласних слідчих (розшукових) дій можуть залучатися також інші особи.

**Суб'єктами** застосування зняття інформації з електронних інформаційних систем, як негласної слідчої (розшукової) дії, що пов'язана з тимчасовим обмеженням конституційних прав людини є працівники оперативно-технічних підрозділів.

**Об'єктами зняття інформації з електронних інформаційних систем є:** *електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі, мережі електрозв'язку, які накопичують, обробляють, зберігають, або передають відомості про тяжкі та особливо тяжкі злочини.*

Зазначена негласна слідча (розшукові) дія проводиться у випадках, якщо відомості про злочин та особу, яка його вчинила, неможливо отримати в інший спосіб. Вона проводиться виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів.

**Слідчий зобов'язаний** повідомити прокурора про прийняття рішення щодо проведення зняття інформації з електронних інформаційних систем та отримані результати. **Прокурор** має право заборонити проведення або припинити подальше проведення даної негласної слідчої (розшукової) дії. У рішенні про проведення зняття інформації з електронних інформаційних систем зазначається строк її проведення. Строк проведення зняття інформації з електронних інформаційних систем може бути продовжений (ст. 249 КПК).

## **2. Порядок отримання інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту.**

**Поняття «інформація»** в широкому розумінні слова є однією з первинних філософських категорій і значною мірою збігається з таким поняттям як «знання». За означенням Академічного тлумачного словника української мови **інформація** – це «**відомості, про які-небудь події, чиясь діяльність і т. ін.; повідомлення про щось**».

Інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах або пересилається каналами електрозв'язку, має притаманні ознаки фізичного, юридичного та економічного характеру. Інформація (як сукупність даних і програм) є об'єктом права власності громадян, організацій (юридичних осіб) і держави, може бути об'єктом права власності як у повному обсязі, так і об'єктом лише володіння, користування чи розпорядження. Інформація, як предмет злочину, є для винного чужою (не перебуває у його власності чи законному володінні).

Робота електронних інформаційних систем включає інформаційний обмін між окремими їх частинами, а також між собою. Зазвичай такі системи називають просто електронними системами (ЕС), маючи на увазі саме електронні інформаційні системи.



До електронних інформаційних систем відносяться: *електронно-обчислювальні машини (комп'ютери); автоматизовані системи; комп'ютерні мережі; мережі електрозв'язку.*

**Електронно-обчислювальна машина (ЕОМ, комп'ютер)** являє собою сукупність технічних засобів та системного програмного забезпечення, створює можливість автоматизованого оброблення інформації та отримання результату в необхідній формі.

Крім того, відповідно до державних стандартів, комп'ютер – це функційний пристрій, що складається з одного або кількох взаємопов'язаних центральних процесорів і периферійних пристроїв й може виконувати обчислення без участі людини. Комп'ютер, призначений для обслуговування одного користувача, що характеризується невеликими габаритами, підвищеною надійністю, простотою зміни конфігурації та розвинутими засобами діалогу, є персональним комп'ютером.

**Автоматизованою є система**, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення.

**Комп'ютерна (інформаційна) мережа** – це сукупність територіально розосереджених систем оброблення даних, засобів та/або систем зв'язку і пересилання даних, що забезпечує користувачам дистанційний доступ до її ресурсів і колективне використання цих ресурсів.

**Мережа електрозв'язку** являє собою комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

Основними компонентами ЕОМ (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку є їх правове, організаційне, програмне, інформаційне, лінгвістичне та технічне забезпечення, а також персонал та користувачі.

Пунктом 2 ст. 264 КПК України передбачено, що не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту.

До відомостей, доступ до яких не обмежується її власником, володільцем або утримувачем відносяться відомості які вільно викладені в мережі «Інтернет» (файлообмінниках, форумах, сайтах та ін.).

**Під здобуттям відомостей** з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту розуміють негласну слідчу (розшукову) дію, яка полягає у пошуку та отриманні інформації з комп'ютерних систем та мереж ( п. 2 ст. 264 КПК).

Необхідністю проведення даної негласної слідчої дії є особливості сучасної злочинності. Так як комп'ютерні мережі, насамперед Інтернет, все більше активно використовується зловмисниками для створення нелегальних ринків збуту зброї, наркотиків, людських органів, порнографічної продукції, вибухових пристроїв, пропозиції щодо надання «кілерських» послуг, а також є способом розповсюдження інформації щодо виготовлення саморобних вибухових пристроїв, пропаганди національної ворожнечі й закликів до розв'язання війни.

У даному випадку проведення даної негласної слідчої (розшукової) дії, метою якої є здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, не обмежують конституційні права особи.

Отримання інформації з електронних інформаційних систем здійснюється виключно через канали зв'язку (комп'ютерні лінії). Отримання інформації з електронних інформаційних систем, призначеної для загального користування, визначається терміном «**комп'ютерна розвідка**» і відносить: зміст сайтів та Web-сторінок фізичних і юридичних осіб, а також повідомлення на форумах та електронних дошках об'яв. В зв'язку з цим «комп'ютерну розвідку» мають право проводити – як слідчі, оперативні підрозділи, так і оперативно-технічні підрозділи.

Водночас, слід зауважити, що порядок проведення комп'ютерної розвідки сьогодні на рівні відомчих інструкцій не регламентований.

**До основних напрямів здійснення комп'ютерної розвідки відносять:**

- пошук інформації, яка може свідчити про вчинення протиправних дій;
- збирання матеріалів, щодо певних об'єктів: фізичних та юридичних осіб, предметів та подій у зв'язку з їх відношенням до протиправної діяльності;
- здійснення в комп'ютерній мережі активних заходів.

**Метою комп'ютерної розвідки** є отримання інформації, яка міститься в комп'ютерних мережах (на серверах).

Знаючи IP-адресу комп'ютера або мережного обладнання ймовірного злочинця та розуміючи правила надання доменних імен і закріплення їх за зонами, працівник правоохоронного органу, у більшості випадків, має змогу самотійно визначити фізичне місцезнаходження комп'ютера, за яким дана адреса закріплена.

Місцезнаходження програмно-технічних засобів у мережі Інтернет визначається за IP-адресою, яка належить певному провайдеру і є взаємопов'язаною з номером телефону користувача послуг доступу до мережі. А знаючи номер телефону користувача легко визначити і фізичну адресу, а саме де встановлено телефон, тобто місце ймовірного знаходження програмно-технічних засобів (потерпілого, правопорушника, серверів провайдерів тощо), що використовують даний телефон для доступу до мережі Інтернет.

Однак, для отримання інформації про трафік ініціатор направляє провайдеру ухвалу слідчого судді про зняття інформації з технічних каналів зв'язку,

комп'ютерних систем та інших технічних засобів, а також запит на офіційному бланку з грифом.

У запиті повинен вказуватися номер абонента і (або) IP-адресу та термін часу, за який необхідно надати відомості за здійсненими з'єднанням. Постанова на проведення заходу по зняттю інформації з технічних каналів зв'язку, комп'ютерних систем та інших технічних засобів не повинно містити відомостей, віднесених до державної таємниці України. Провайдер Інтернету реєструє видачу відомостей про зняття інформації з технічних каналів зв'язку, комп'ютерних систем та інших технічних засобів в окремих облікових документах з обмеженим доступом і повертає ініціатору ухвалу.

### **3. Організація проведення НСРД – зняття інформації з електронних інформаційних систем.**

Зняття інформації з електронних інформаційних систем – один із найбільш ефективних способів отримання інформації про осіб, які становлять інтерес в досудовому розслідуванні, який може дати позитивний результат, лише в разі проведення відповідних дій оперативного і технічного характеру.

**Під організацією проведення зняття інформації з електронних інформаційних мереж**, яке проводиться за дозволом слідчого судді із застосуванням технічних засобів, розуміємо систему цілеспрямованих дій з планування, підготовки, проведення і документального оформлення негласних слідчих (розшукових) дій, які здійснюються з дотриманням вимог законів, підзаконних актів та принципів кримінального процесу.

**До етапів організації підготовки та проведення зняття інформації з електронних інформаційних мереж, яке проводиться за дозволом слідчого судді із застосуванням технічних засобів відносяться:**

- вивчення, аналіз і оцінка ситуації, яка складається в процесі кримінального провадження;
- складання відповідних документів та отримання дозволу слідчого судді;
- планування заходів;
- організація взаємодії;
- підготовка до проведення даної негласної слідчої (розшукової) дії;
- проведення даної негласної слідчої (розшукової) дії;
- контроль за проведенням даної негласної слідчої (розшукової) дії;
- документальне оформлення отриманих результатів;
- аналіз та оцінка ефективності проведення зняття інформації з електронних інформаційних систем.

**У клопотанні на отримання дозволу на зняття інформації з електронних інформаційних систем слідчий або прокурор повинні зазначити наступні відомості:** найменування кримінального провадження та його реєстраційний номер; короткий виклад обставин злочину, у зв'язку з розслідуванням якого подається клопотання; правова кваліфікація злочину із зазначенням статті (частини статті) закону України про кримінальну

відповідальність; відомості про особу (осіб), місце або річ, щодо яких необхідно провести негласну слідчу (розшукову) дію; обставини, що дають підстави підозрювати особу у вчиненні злочину; обґрунтування строку проведення зняття інформації з електронних інформаційних систем; обґрунтування неможливості отримання відомостей про злочин та особу, яка його вчинила, в іншій спосіб; відомості про ідентифікаційні ознаки ЕІС; обґрунтування можливості отримання під час проведення даної негласної слідчої (розшукової) дії доказів, які самостійно або в сукупності з іншими доказами можуть мати суттєве значення для з'ясування обставин злочину або встановлення осіб, які його вчинили.

До клопотання слідчого, прокурора додається **витяг з Єдиного реєстру досудових розслідувань** щодо кримінального провадження, у рамках якого подається клопотання.

**Рішення** про проведення зняття інформації з електронних інформаційних систем приймає **слідчий суддя за поданням слідчого або прокурора**.

**В ухвалі слідчого судді про дозвіл** на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки електронної інформаційної системи, в якій може здійснюватися втручання у приватне спілкування.

**Ідентифікаційними ознаками електронної інформаційної системи є:** – ІР-адреса (ІР – Internet Protocol), яка є унікальним ідентифікатором (адресою) пристрою (звичайно комп'ютера або маршрутизатора), підключеного до локальної мережі або Інтернету;

– доменне ім'я, що дозволяє ідентифікувати в мережі Інтернет веб-сайт або адресу електронної пошти;

– серійний номер та характеристики автоматизованої системи та ПОМ.

У відповідності до поданого клопотання слідчий суддя **не пізніше як шість годин з моменту отримання даного клопотання** виносить ухвалу в наданні дозволу або відмови проведення зняття інформації з електронних інформаційних систем.

У випадках позитивного надання дозволу в ухвалі обов'язково конкретизуються строки зняття інформації з електронних інформаційних систем, зокрема дозвіл слідчого судді на проведення негласної слідчої (розшукової) дії не може перевищувати два місяці. Також дозволяється продовжити дані строки за наявності відповідних підстав та визначається загальний строк, протягом якого в одному кримінальному провадженні може тривати проведення негласної слідчої (розшукової) дії, дозвіл на проведення якої дає слідчий суддя, який не може перевищувати **шести місяців**.

У виняткових випадках, пов'язаних з урятуванням життя людей та запобіганням здійсненню тяжкого або особливо тяжкого злочину, КПК України допускає можливість почати проведення зняття інформації з електронних інформаційних систем до отримання дозволу слідчого судді. При цьому прокурор зобов'язаний невідкладно звернутися з відповідним клопотанням до слідчого судді та, якщо останній не дасть свого дозволу, то почата вказана

негласна слідча (розшукова) дія повинна бути негайно припинена, а отримана інформація - знищена (ст. 250 КПК України).

**Проводити** зняття інформації з електронних інформаційних систем має право, як сам слідчий, так і вповноважені ним оперативні підрозділи правоохоронних органів, які надають завдання до оперативно-технічного підрозділу та складають спільний план проведення.

**Ухвала слідчого судді** про надання дозволу на здійснення зняття інформації з електронних інформаційних систем підписується слідчим суддею, скріплюється гербовою печаткою, реєструється в апараті суду за правилами таємного діловодства.

При знятті інформації з комп'ютерних мереж, з жорсткого диска комп'ютера програми, які становлять оперативний інтерес, нерідко налаштовані на самознищення у разі несанкціонованого доступу. Подолати діючу систему захисту оперативний працівник самотійно, як правило, не в змозі, в зв'язку з чим проводити дану негласну слідчу (розшукову) дію повинен **спеціаліст**.

**За результатами** здійснення зняття інформації з електронних інформаційних систем, що пов'язано з тимчасовим обмеженням конституційних прав складається **протокол з відповідними додатками**.

**Згідно ст. 104 КПК України протокол про проведення зняття інформації з електронних інформаційних систем складається з:**

**1) вступної частини, яка повинна містити відомості про:**

- місце, час проведення та назву даної процесуальної дії;
- особу, яка проводить дану процесуальну дію (прізвище, ім'я, по батькові, посада);
- всіх осіб, які присутні під час проведення зняття інформації з електронних інформаційних систем (прізвища, імена, по батькові, дати народження, місця проживання);
- інформацію про те, що особи, які беруть участь у даній процесуальній дії, заздалегідь повідомлені про застосування технічних засобів фіксації, характеристики технічних засобів фіксації та носіїв інформації, які застосовуються при проведенні процесуальної дії, умови та порядок їх використання;

**2) описової частини, яка повинна містити відомості про:**

- послідовність дій;
- отримані в результаті даної процесуальної дії відомості, важливі для цього кримінального провадження, в тому числі виявлені та/або надані речі і документи;

**3) заключної частини, яка повинна містити відомості про:**

- вилучені речі і документи та спосіб їх ідентифікації;
- спосіб ознайомлення учасників зі змістом протоколу;
- зауваження і доповнення до письмового протоколу з боку учасників даної процесуальної дії.

Відомості про осіб, які проводили зняття інформації з електронних інформаційних систем або були залучені до її проведення, у разі здійснення

щодо них заходів безпеки можуть зазначатися із забезпеченням конфіденційності даних про таких осіб у порядку, визначеному законодавством.(ч.1 ст. 252 КК України).

Згідно ст. 105 КПК України **додатками до протоколу** проведення зняття інформації з електронних інформаційних систем можуть бути: спеціально виготовлені копії, зразки об'єктів, речей і документів; письмові пояснення спеціалістів, які брали участь у проведенні відповідної процесуальної дії; стенограма, аудіо-, відеозапис даної процесуальної дії; фототаблиці, схеми, зліпки, носії комп'ютерної інформації та інші матеріали, які пояснюють зміст протоколу.

Протоколи щодо проведення зняття інформації з електронних інформаційних систем, інші результати, здобуті за допомогою застосування технічних засобів, вилучені під час їх проведення речі і документи або їх копії можуть використовуватися в доказуванні на тих самих підставах, що і результати проведення інших слідчих (розшукових) дій під час досудового розслідування.

Протоколи про проведення зняття інформації з електронних інформаційних систем, з додатками, не пізніше ніж через двадцять чотири години з моменту припинення вказаних негласних слідчих (розшукових) дій передаються прокурору (ч. 3 ст. 252 КПК України).

Зміст інформації, одержаної внаслідок здійснення зняття відомостей з електронних інформаційних систем, фіксується на відповідному носіїві особою, яка здійснювала зняття та зобов'язана забезпечити обробку, збереження або передання інформації. Носії інформації та технічні засоби, за допомогою яких отримано інформацію, можуть бути предметом дослідження відповідних спеціалістів або експертів.

**Забороняється** використання відомостей, речей та документів, отриманих в результаті проведення зняття інформації з електронних інформаційних систем для цілей, не пов'язаних з кримінальним провадженням (ч. 2 ст.255 КПК України). Відомості, речі та документи, отримані в результаті проведення зняття інформації з електронних інформаційних систем, які прокурор не визнає необхідними для подальшого проведення досудового розслідування, повинні бути невідкладно знищені.

**Отже, у зв'язку зі стрімким розвитком програмного забезпечення проведення працівниками правоохоронних органів негласної слідчої (розшукової) дії – «зняття інформації з електронних інформаційних систем» є одним із найефективніших способів отримання інформації про осіб, які становлять інтерес у досудовому розслідуванні.**