ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Кваліфікаційна наукова праця на
правах рукопису

ТКАЧИК АНДРІЙ БОГДАНОВИЧ

УДК 343.98:343.34

ДИСЕРТАЦІЯ

ТАЄМНИЦЯ СПІЛКУВАННЯ ТА ЇЇ ОБМЕЖЕННЯ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

12.00.09 - кримінальний процес та криміналістика; судова експертиза;
оперативно-розшукова діяльність
081 - Право

Подається на здобуття наукового ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ А.Б. Ткачик

Науковий керівник Луцик Василь Васильович,
кандидат юридичних наук, доцент

Львів - 2021

АНОТАЦІЯ

Ткачик А.Б. Таємниця спілкування та її обмеження в кримінальному провадженні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» (081 - Право). - Львівський державний університет внутрішніх справ, Львів, 2021.

Дисертація охоплює комплексне вирішення наукового і прикладного завдання, спрямованого на з'ясування змісту таємниці спілкування та процесуальних способів її обмеження у кримінальному провадженні.

Наукова новизна праці полягає в тому, що дисертація є одним із перших у досліджень обмеження таємниці спілкування у кримінальному провадженні. Сформульовані положення спрямовані на розв'язання важливого наукового та практичного завдання, що полягає у визначенні процесуальних способів обмеження таємниці спілкування та використані отриманих результатів у доказуванні, а отримані висновки визначають перспективи наукового забезпечення протидії злочинності та підготовки фахівців для Національної поліції України.

Розроблені у дисертації рекомендації можуть використовуються в освітньому процесі та практичній діяльності органів досудового розслідування.

У Розділі 1 «Таємниця спілкування як засада кримінального провадження» проаналізовано стан наукової розробленості цієї проблеми, сформовано поняття цієї засади та виокремлено її елементи.

Згідно 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.

Перелік видів комунікації, що знаходяться під конституційної охороною, є відкритим і охоплює не тільки листування, телефонні розмови, телеграфні повідомлення, але і іншу кореспонденцію. Дана конструкція норми дозволяє відповідати рівню технічного розвитку суспільства і гарантувати недоторканність нових, невідомих на момент розробки Конституції видів комунікації.

Аналіз національного законодавства та наукових поглядів на поняття таємниці спілкування дав змогу сформулювати авторське визначення цієї засади, зокрема таємниця спілкування полягає у недопущенні розголошення інформації, яка передається особами під час листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування за умови, що особи бажають її зберегти в таємниці.

Залежно від суб'єктів спілкування таємницю спілкування можна розподілити на дві групи таємницю спілкування загальних суб'єктів та таємницю спілкування спеціальних суб'єктів. Виокремлення такого поділу зумовлено додатковими процесуальними гарантіями, якими наділені окремі суб'єкти.

Зроблено висновок, що міжнародно-правова регламентація охорони приватного життя, зокрема і таємниці спілкування, здійснила безпосередній вплив на національне законодавство багатьох держав. В результаті цього, право на таємницю спілкування, будучи міжнародним та європейським стандартом в сфері захисту прав і свобод людини, є об'єктом не лише міжнародно-правового, а і внутрішньодержавного регулювання. У міжнародно-правових та європейських актах не має вичерпної інтерпретації стандартів права на приватність та таємницю спілкування, що зумовлює потребу в дослідженні практики Європейського Суду з прав людини. У дисертаційному дослідженні здійснений її аналіз щодо дотримання критеріїв допустимості обмеження права на приватність.

Проаналізовано зарубіжний досвід правового регулювання закріплення права на таємницю спілкування у законодавстві зарубіжних держав (зокрема

у США, Великій Британії, ФРН, Швейцарії, Молдові, Казахстані, Узбекистані). При аналізі права на таємницю спілкування у США було зроблено акцент на дослідженні різних концепцій «прайвесі». Окрім цього, науковою новизною дисертаційного дослідження є аналіз зарубіжного досвіду допустимих обмежень цієї засади.

У Розділі 2 «Процесуальні дії спрямовані на обмеження таємниці спілкування» охарактеризовано систему та процесуальний порядок проведення дій спрямованих на обмеження таємниці спілкування.

Доведено, що питання щодо системи процесуальних дій в ході яких обмежується таємниця спілкування не знайшло свого достатнього висвітлення в науковій літературі. У більшості випадків обмеження таємниці спілкування зводиться до НСРД пов'язаних із втручанням у приватне спілкування. Однак, перелік таких випадків набагато ширший.

Виокремлено наступну систему процесуальних дій, спрямованих на обмеження таємниці спілкування.

Зокрема, на підставі ухвали слідчого судді суду першої інстанції проводяться наступні процесуальні дії спрямовані на обмеження таємниці спілкування:

- тимчасовий доступ до речей та документів;
- обшук.

На підставі ухвали слідчого судді апеляційного суду, слідчого судді Вищого антикорупційного суду проводяться такі негласні слідчі (розшукові) дії:

– аудіо-, відеоконтроль особи;

- накладення арешту на кореспонденцію, огляд і виїмка кореспонденції;
- зняття інформації з транспортних телекомунікаційних мереж;
- зняття інформації з електронних інформаційних систем;
- спостереження за особою;
- аудіо-, відеоконтроль місця.

Обґрунтовано, що під час обстеження публічно недоступних місць, житла чи іншого володіння особи слідчий, працівники оперативних підрозділів не мають права втручатися у таємницю спілкування, зокрема у особисте листування особи, інші форми спілкування зафіксовані на матеріальних чи електронних носіях, які знаходяться в публічно недоступних місць, житлі чи іншому володіння особи. Така позиція зумовлено змістом даної НСРД, яка в основному носить організаційно-допоміжний характер.

Наголошено, що ухвала слідчого суддя про дозвіл на проведення НСРД, які обмежують таємницю спілкування, обов’язково має бути розсекречена та долучена до матеріалів кримінального провадження, оскільки відсутність ухвали слідчого судді про дозвіл на проведення негласних слідчих (розшукових) дій унеможливлює використання їх результатів у доказуванні.

Неодноразово у практичній діяльності та науковій літературі виникає питання про можливі порушення прав людини оперативними підрозділами під час проведення НСРД у зв’язку з відсутністю належного судового контролю та прокурорського нагляду в ході їх здійснення.

Виходом з цієї ситуації є залучення особи, яка під час судового розгляду клопотань про НСРД буде забезпечувати дотримання прав осіб щодо яких будуть застосовуватися обмеження. В зв’язку з цим, пропонуємо викласти ч. 1 ст. 261 КПК в наступній редакції «Слідчий суддя зобов'язаний розглянути клопотання про надання дозволу на проведення негласної слідчої (розшукової) дії протягом шести годин з моменту його отримання. Розгляд клопотання здійснюється за участю особи, яка подала клопотання та адвоката делегованого центром безоплатної правової допомоги». Такий адвокат, повинен мати допуск до державної таємниці, а доступ до матеріалів клопотання про надання дозволу на проведення НСРД буде надаватися слідчим суддею перед його судовим розглядом.

Зроблено висновок, що на підставі аналізу ст. 162 КПК України можна виокремити дві групи даних, які можна отримати під час тимчасового

доступу до речей та документів, які становлять таємницю спілкування. До них зокрема належать особисте листування особи та інші записи особистого характеру та інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

Обґрунтовано доцільність необхідності закріплення окремої слідчої (розшукової) дії, як різновиду слідчого огляду – огляд електронної інформаційної системи. Такий огляд проводиться щодо електронних інформаційних систем, які вилучені в ході інших слідчих (розшукових) дій та здійснюється на підставі ухвали слідчого судді місцевого суду.

Доведено, що за своїм характером і аудіо-, відеоконтроль особи і місця мають на меті обмеження таємниці спілкування, та спрямовані на отримання доказової інформації, яка міститься в розмовах, рухах чи діях особи. Однак, якщо під час аудіо-, відеоконтролю особи нас цікавить конкретна особа, яка підозрюється у вчиненні кримінального правопорушення, то під час аудіо-, відеоконтролю місця коло осіб невизначене, в зв'язку з цим обмежується таємниця спілкування невизначеного кола осіб.

Запропоновано долучати до клопотання про тимчасовий доступ до речей та документів, що знаходяться в операторів та провайдерів телекомунікацій, матеріалів радіотехнічної розвідки, які дозволяють додатково ідентифікувати базові станції через які здійснювали спілкування підозрювані, а отже обмежити порушення таємниці спілкування невизначеної кількості абонентів.

Вдосконалено правове регулювання НСРД накладення арешту на кореспонденцію. Зокрема, запропоновано передбачити в ході її проведення право відшуковувати поштово-телеграфну кореспонденцію, на яку необхідно накладати арешт. Така кореспонденція може відшуковуватися за почерком, за виглядом упаковки, місцем відправки чи одержання тощо. У ч. 1 ст. 261 КПК потрібно встановити спеціальні вимоги до ухвали слідчого судді про

надання дозволу на накладення арешту на кореспонденцію. Зокрема, в ухвалі слідчого судді мають бути вказані: підстави на яких буде проводитись слідча (розшукова) дія, прізвище, ім’я та по батькові особи, кореспонденція якої має затримуватися, точна адреса цієї особи, види кореспонденції, на яку накладається арешт, строк дії ухвали, назва установи зв’язку, на яку покладається обов’язок затримувати кореспонденцію та повідомляти про це слідчого.

У Розділі 3 «Використання в доказуванні результатів процесуальних дій спрямованих на обмеження таємниці спілкування» розкрито правову природу доказів, які отримуються в ході процесуальних дій спрямованих на обмеження таємниці спілкування.

Наголошено, що особливу увагу потрібно звернути на особливості опису у протоколі НСРД вмісту електронного листування, яке становить таємницю спілкування. У такому протоколі повинні бути відображені такі відомості:

- виявлені адреси електронної пошти, по можливості - паролі до відповідних поштових скриньок;

- зміст повідомлень електронної пошти: текстова інформація, що пересилається, файли, їх реквізити (розмір, формат, дати створення і зміни, імена користувачів, які створили і змінювали їх зміст;.

- найменування організації, у власності якої знаходяться сервера, через які передавалася електронна пошта з метою подальшого зняття інформації з транспортних телекомунікаційних мереж;

- дата і час відправлення та отримання повідомлень, системні час і дата на комп'ютерному пристрої;

- наявність на комп'ютері програм для роботи з електронною поштою, наявність у вкладках, закладках, збережених сторінках і журналі відвідувань браузера відомостей про користування підозрюваним електронною поштою;

- наявність працюючих підключень до Інтернету і збережених налаштувань доступу (дротового і бездротового).

Обґрунтовано, що відмінність електронних носіїв інформації від «традиційних» речових доказів та інших документів призводить до необхідності використовувати різні прийоми і засоби роботи з зазначеними доказами. «Предметні» речові докази містять в якості доказової інформації сліди матеріального світу. Зміна цієї інформації неможлива без безпосереднього впливу на сам предмет. Тому для гарантування їх достовірності цілком достатньо традиційної упаковки, що забезпечує відсутність механічного впливу. Стверджувати це ж щодо електронних носіїв інформації неможливо. Тому вимога застосування спеціальних засобів, що виключають дистанційний вплив на них, є обов'язковою вимогою під час їх огляду та вилучення.

Ключові слова: таємниця спілкування, тимчасовий доступ до речей та документів, негласні слідчі (розшукові) дії, електронна інформаційна система, кореспонденція, аудіо-відео контроль особи, зняття інформації.

ANNOTATION

Tkachyk A.B. The secrecy of communication and its limitation in criminal proceedings. – Research paper (manuscript)

Dissertation on Doctor of Philosophy Degree on specialty 12.00.09 – «Criminal proceedings and criminalistics; forensic research; operative search activity» (081 Law). – Lviv State University of internal affairs, Lviv, 2021.

The dissertation covers a comprehensive solution of scientific and practical tasks, aimed at clarifying the content of the secrecy of communication and procedural methods of its limitation in criminal proceedings.

The scientific novelty is that the dissertation is one of the first researches on the limitation of the secrecy of communication in criminal proceedings. The formulated provisions are aimed at solving an important scientific and practical task, which is to determine the procedural methods of the secrecy of communication limitation and use the results in proving, and the findings of work determine the prospects for scientific support of crime prevention and training for the National Police of Ukraine.

The dissertation's recommendations may be used both in the educational process and practical activity of the National Police of Ukraine.

The status of scientific development of the issue was analyzed, the notion of this principle was formulated and it elements were divided in Section 1 «The secrecy of communication as principal of criminal proceedings».

According to Art. 31 of the Constitution of Ukraine everyone is guaranteed the secret of correspondence, telephone conversations, telegraph and other correspondence. The exceptions may be determined only by court in cases, determined by law in order to prevent a crime or to reveal the truth during investigation of a criminal case if it is impossible to obtain information in other ways.

The list of communication types, which are under the constitutional protection is open and includes not only correspondence, telephone conversations, telegraph correspondence, but also other types of correspondence. The construction

of this norm allows to correspond to the level of society technical development and to guarantee the inviolability of new, unknown on the moment of Constitution adoption types of communication.

The analysis of national legislation and scientific views on the notion of the secrecy of communication allowed to formulate the author's definition of this principle, in particular, the secrecy of communication is to prevent the disclosure of information transmitted by persons through correspondence, telephone conversations, telegraph and other correspondence, other forms of communication provided that persons want to keep it in a secret.

The secrecy of communication may be divided into two groups depending on the subjects of communication: the secrecy of communication of general subjects and the secrecy of communication of special subjects. The singling out of such a division is due to the additional procedural guarantees, which some subjects are endowed.

It is made a conclusion that an international legal regulation of privacy, including the secrecy of communication, had a direct impact on the national legislation of many states. As a result, the right to the secrecy of communication, being an international and European standard in the field of human rights protection, is the object not only of international, but also of domestic legal regulation. There is no comprehensive interpretation of the standards of the right to privacy and the secrecy of communication in international legal and European acts, that makes it necessary to research the case law of the European Court of Human Rights. It was analyzed concerning the observance of admissibility criteria of limitations of the right to privacy in the dissertation research.

The foreign experience of legal regulation of enshrining the right to the secrecy of communication in the legislation of foreign countries (in particular, in the USA, Great Britain, Germany, Switzerland, Moldova, Kazakhstan, Uzbekystan) was analyzed. While analyzing the right of the secrecy of communication in the United States, the emphasis was put on the study of various concepts of "privacy". Besides, the scientific novelty of the dissertation research is

the analysis of foreign experience of admissible limitations of this principle.

In Section 2 "Procedural actions aimed at limitation of the secrecy of communication" the system and procedure of conducting actions aimed at limitation of the secrecy of communication are described.

It is proved that the issue of procedural actions system during which the secrecy of communication is limited was not highlighted enough in the scientific literature. In the most cases, the limitation of the secrecy of communication is associated with covert investigative actions related to the interference in private communication. However, the amount of such cases is much bigger.

The following system of procedural actions aimed at limitation of the secrecy of communication is defined.

In particular, the following procedural actions aimed at the limitation of the secrecy of communication are conducted on the basis of the decision of the investigating judge of first instance court:

- temporary access to items and documents;
- search.

The following procedural actions are conducted on the basis of the decision of the investigating judge of appeal court, investigative judge of the High Anti-corruption court:

- audio-, video control of a person;
- correspondence inspection and seizure;
- interception of information from transport telecommunication network;
- interception of information from electronic informational system;
- person surveillance;
- audio-, video control of a place.

It is substantiated that during the inspection of publicly inaccessible places, housing or other property of the person investigator, investigators of operational units have no right to interfere with the secrecy of communication, including personal correspondence, other forms of communication, recorded on physical or digital objects in publicly inaccessible places, housing or other property of a

person. This position is due to the content of this covert investigative action, which has mainly organizational and supportive nature.

It is emphasized that the decision of the investigative judge on the permission of covert investigative actions conduction, aimed at the limitation of the secrecy of communication must be declassified and attached to the materials criminal proceedings, as the lack of the decision of the investigative judge on permission to conduct covert investigative actions makes it impossible to use their results in proving.

The issue of possible human rights violations by operational units during the conduction of covert investigative actions due to the lack of a proper judicial control and prosecutorial supervision during their conduction has repeatedly been raised in practice and in the scientific literature.

The solution of this situation is to involve a person who will ensure that the rights of the persons subjected to the limitations will be respected during the judicial review of covert investigative action request. In this regard, we propose the following wording of Part 1 of Art. 261 of the CPC «The investigating judge is obliged to consider the request for permission to conduct a covert investigative action within six hours from the moment of its obtaining. The consideration of the request should be carried out with the participation of the person who has submitted a request and the lawyer delegated by the free legal aid center". Such a lawyer should have the access to state secrets, and the access to the materials of the request for the permission to conduct covert investigative action will be provided by the investigative judge before this trial.

It was concluded that based on the analysis of Art. 162 of the CPC of Ukraine, two groups of data can be distinguished, that constitute a secret of communication that can be obtained during temporary access to items and documents. They include personal correspondence of a person and other personal records and information held by telecommunications operators and providers about communications, the subscriber, the providing of telecommunications services, including the receiving of services, their duration, content, transmission routes, and

so on.

The necessity of legal regulation of a separate investigative action as a type of investigative inspection – an inspection of electronic informational system was substantiated. Such inspection should be conducted concerning electronic information systems, that were seized during other investigative actions and should be conducted on the decision of the investigative judge in first instance court.

It was proved that by their nature both audio- and video control of a person and place are aimed at limitation of the secrecy of communication and at obtaining evidentiary information, contained in conversations, movements or actions of a person. However, if during the audio- and video control of a person we are interested in a specific person who is suspected of committing a criminal offense, then during the audio- and video control of a place the quantity of people is unidentified, therefore the secrecy of communication of unidentified quantity of people would be limited.

It was proposed to include radio intelligence materials to the request for a temporary access to items and documents held by telecommunications operators and providers, that allow identify additionally the base stations through which the suspects had communicated, and thus to limit the secrecy of communication of an indefinite quantity of subscribers.

Legal regulation of covert investigative action - seizure of correspondence has been improved. In particular, to provide the right to search for postal and telegraphic correspondence, that should be seizure. Such correspondence can be searched by handwriting, type of packaging, place of sending or receiving, etc. In Part 1 of Art. 261 of the CPC it is necessary to establish special requirements for the decision of the investigative judge to give a permission for seizure of correspondence. In particular, in the decision of the investigative judge the following information should be specified: the grounds for the conduction of investigative action, the surname, name, name with patronymic of the person whose correspondence is to be detained, the exact address of this person, the types of correspondence that would objects of seizure, terms of the decision, the name of

the communication institution, which is obliged to detain correspondence and notify the investigator about it.

The legal nature of evidence obtained during procedural actions aimed at the limitation of the secrecy of communication is highlighted in Section 3 «The use of the results of procedural actions, aimed at the limitation of the secrecy of communication in proving».

It is emphasized that a special attention should be paid to the peculiarities of the description of the content of electronic correspondence, which is a secret of communication in the covert investigative action protocol. The following information shall be reflected in such a protocol:

- detected e-mail addresses, if possible - passwords to the relevant mailboxes;

- the content of e-mails: textual information sent, files, their details (size, format, dates of creation and changes, names of users who created and changed their content);.

- the name of the organization that owns the servers through which the e-mails were transmitted in order to further remove information from the transport telecommunications networks;

- date and time of sending and receiving messages, system time and date on the computer device;

- the availability of programs on the computer for working with e-mail, the availability in tabs, bookmarks, saved pages and the log of visits to the browser information about the use of e-mail by the suspect;

- the availability of working Internet connections and saved access settings (wired and wireless).

It is substantiated that the difference between electronic information carrier and "traditional" physical evidence and other documents leads to the need of using different methods and means of working with this evidence. "Subjective" physical evidence contains traces of the material world as evidentiary information. The changing of this information is impossible without a direct impact on the subject

itself. Therefore, to ensure their authenticity, a traditional packaging is enough, which ensures the absence of mechanical impact. It is impossible to confirm the same about electronic information carrier. Therefore, the requirement to use special means that exclude remote impact on them is a compulsory requirement during their inspection and seizure.

Key words: the secrecy of communication, contemporary access to items and documents, temporary access to items and documents, covert investigative actions, electronic informational system, correspondence, audio-video control of a person, interception of information.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

в яких опубліковані основні наукові результати дисертації:

1. Ткачик А.Б. Поняття та зміст таємниці спілкування у кримінальному провадженні. *Юридична наука*. 2020. №1. С. 156-161. *(стаття в науковому виданні, включеному до переліку наукових фахових видань України з присвоєнням категорії «Б»)*.
2. Ткачик А.Б. Зарубіжний досвід правового регулювання таємниці спілкування. *International Journal Law & Society.* Issue 3. 2021. С. 79-86. *(стаття в періодичному науковому виданні іншої держави, яка входить до Організації економічного співробітництва та розвитку та/або Європейського Союзу)*.
3. Ткачик А. Обмеження таємниці спілкування в ході проведення тимчасового доступу до речей та документів. *KELM*. 2020. № 6. С. 224-229 *(стаття в періодичному науковому виданні іншої держави, яка входить до Організації економічного співробітництва та розвитку та/або Європейського Союзу)*.

які додатково відображають наукові результати дисертації:

4. Ткачик А.Б. Європейські стандарти забезпечення таємниці спілкування у кримінальному провадженні. *Вісник Чернівецького факультету Національного університету «Одеська юридична академія»*. 2019. Вип. 2. С. 208-218.
5. Забезпечення відшкодування шкоди у злочинах, пов'язаних з торгівлею людьми, на стадії досудового розслідування: довідник / Хитра А.Я., Кучер В.О., Ткачик А.Б. Видавництво: ЛьвДУВС, Львів, 2019. 128 с.
6. Кримінально-правова характеристика злочинів, пов’язаних з незаконним обігом зброї та вибухівки: посібник для підрозділів Національної поліції у схемах / Мармура О.З., Письменський Є.О., Ткачик А.Б. Видавництво: ЛьвДУВС, Львів, 2019. 44с.

які засвідчують апробацію матеріалів дисертації:

7. Ткачик А.Б. Обмеження таємниці спілкування в практиці європейського суду з прав людини. Процесуальне та криміналістичне забезпечення досудового розслідування: збірник тез науково-практичного семінару (01 грудня 2017 року) / упор. А.Я. Хитра, Р.М. Шехавцов, Є.В. Пряхін, С.І. Марко. Львів: ЛьвДУВС. С. 112-115.
8. Ткачик А.Б. Обмеження таємниці спілкування шляхом проведення зняття інформації з транспортних телекомунікаційних мереж. Процесуальне та криміналістичне забезпечення досудового розслідування: тези доповідей учасників науково-практичного семінару (30 листопада 2018 року) / упор. А.Я. Хитра. Львів: ЛьвДУВС. С. 93-96.
9. Ткачик А.Б. Обмеження таємниці спілкування в ході проведення аудіо-, відеоконтролю особи та місця. Правова система України: сучасний стан та актуальні проблеми: Збірник матеріалів восьмої Всеукраїнської науково-практичної конференції (Івано-Франківськ, 13 листопада 2020 року). Івано-Франківськ: видавник Голіней О.В., 2020. С. 114-117.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВРУ - Верховна Рада України

ЄРДР - Єдиний реєстр досудових розслідувань

ЗУ - Закон України

КК України - Кримінальний кодекс України

КПК України - Кримінальний процесуальний кодекс України

МВС України - Міністерство внутрішніх справ України

НПУ - Національна поліція України

НСРД - негласна слідча (розшукова) дія

ОРД - оперативно-розшукова діяльність

ОРЗ - оперативно-розшукові заходи

США - Сполучені Штати Америки

ВСТУП

Обґрунтування вибору теми дослідження. Згідно статті 8 Конвенції про захист прав людини і основоположних свобод кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб.

Прийняття у 2012 році нового Кримінального процесуального кодексу України запровадило нову систему засад кримінального провадження, що зумовило потребу нового осмислення їх змісту та зміни підходів до їх застосування. Передача інформації будь-яким шляхом – це рушійна сила розвитку, прогресу й становлення інформаційного суспільства в Україні. Тому спілкування відіграє вирішальну роль у житті кожної особи, територіальної громади, суспільства й держави. Важливість правовідносин в інформаційній сфері зумовила необхідність конституційного закріплення основних прав і свобод людини і громадянина через гарантування кожному таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції через заборону втручання в особисте і сімейне життя людини, крім випадків, передбачених Конституцією України.

Багато проблем, пов'язаних із процесуальними способами обмеження таємниці спілкування осмислення в світлі прийнятих законодавчих новацій і свого вирішення. Варто уточнити процесуальні та організаційні підстави та умови обмеження таємниці спілкування, з’ясувати європейські стандарти втручання у приватне спілкування та відповідність норм кримінального процесуального законодавства України цим стандартам, виявити і знайти шляхи вирішення проблемних питань, що виникають під час обмеження даної засади у кримінальному провадженні.

Варто відзначити також й відсутність детальної регламентації обмеження таємниці спілкування у чинному законодавстві.

Наведене безумовно вказує на актуальність та необхідність вирішення ряду теоретичних і практичних проблем забезпечення таємниці спілкування та її обмеження у кримінальному провадженні.

Дослідження таємниці спілкування, як засади конституційного права та кримінального процесу були предметом досліджень науковців різних галузей знань. Із-поміж фахівців конституційного права варто виокремити Л.В. Ємчук, В.О. Серьогіна, С.В. Шевчука. Серед фахівців науки кримінального права та кримінології значний внесок у дослідження цієї проблематики зробили О.П. Горпинюк, О. Г. Кальман, П. М. Коваленко, О. В. Лисодєд, А. В. Микитчик, В. Р. Мойсик, К. Л. Попов, О. В. Смаглюк, Г.М. Чернишов, Ю. Л. Шуляк.

Теоретичне підґрунтя для розроблення концепції таємниці спілкування у кримінальному провадженні заклали вітчизняні представники науки кримінального процесу, криміналістики та оперативно-розшукової діяльності, зокрема: Л.І. Аркуша, М.В. Багрій, І.В. Басиста, Р.І. Благута, І.В. Гловюк, С.О. Гриненко, О.М. Дроздов, С.В. Єськов, О.В. Капліна, М.І. Костін, В.А. Колесник, О.П. Кучинська, Л.М. Лобойко, В.В. Луцик, А.В. Мовчан, В.Т. Нор, М.А. Погорецький, І.І., В.В. Рогальска, І.І. Савляк, Д.Б. Сергєєва, Є.Д. Скулиш, В.Г. Уваров, Р.М. Шехацов, О.Г. Шило, М.Є. Шумило, В.М. Юрчишин та інші.

Варто виокремити дисертаційне дослідження Савляк І.І. на тему «Таємниця спілкування як засада кримінального провадження» у якому автор охарактеризувала зміст даної засади та окремі проблеми правозастосування. Однак, у даній праці не досліджено усі можливі механізми обмеження таємниці спілкування, не враховано розвиток сучасних комунікаційних технологій, що обумовлюють пошук нових підходів до отримання доказової інформації.

Попри наукову і практичну важливість напрацювань зазначених

дослідників, варто зауважити, що наукових розробок зі створення цілісного уявлення про таємницю спілкування та можливостей її законного обмеження у кримінальному провадженні, яке б базувалося на сучасних підходах до телекомунікаційного прайвесі, міжнародних стандартах та практиці ЄСПЛ, новітніх положеннях теорії криміналістики, кримінального процесу та оперативно-розшукової діяльності на сьогодні немає, що і обумовило вибір теми дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано з Тематикою наукових досліджень і науково-технічних розробок на 2020-2024 роки, затвердженого наказом Міністерства внутрішніх справ України №454 від 11.06.2020 р. та відповідно до Плану науково-дослідної роботи Львівського державного університету внутрішніх справ (у межах теми «Протидія злочинам, підслідним Національній поліції: правові, кримінологічні та криміналістичні аспекти», номер державної реєстрації 0118U005374). Тема дисертаційного дослідження відповідає науковому напрямку кафедри кримінального процесу та кафедри криміналістики факультету №1 Львівського державного університету внутрішніх справ. Тему дисертації затверджено Вченою радою Львівського державного університету внутрішніх справ 31.10.2017 року (протокол №3).

Мета і завдання дослідження. Метою дослідження є отримання нових знань щодо змісту таємниці спілкування у кримінальному провадженні та способів її обмеження.

Відповідно до окресленої мети визначено основні завдання дослідження:

з'ясувати поняття та сутність таємниці спілкування у кримінальному провадженні;

визначити й описати міжнародні стандарти захисту таємниці спілкування;

проаналізувати зарубіжний досвід правового регулювання обмеження таємниці спілкування;

висвітлити систему та порядок проведення процесуальних дій спрямованих на обмеження таємниці спілкування;

окреслити можливості використання в доказуванні результатів процесуальних дій спрямованих на обмеження таємниці спілкування;

сформулювати пропозиції щодо удосконалення кримінального процесуального законодавства у контексті предмета дослідження.

Об'єктом дослідження є кримінальні процесуальні правовідносини, що виникають, розвиваються та припиняються під час обмеження таємниці спілкування у кримінальному провадженні.

Предметом дослідження є таємниця спілкування та її обмеження в кримінальному провадженні.

Методи дослідження. Для досягнення поставленої мети, з урахуванням об'єкта та предмета дослідження, у роботі використано загальнонаукові та спеціальні методи, які є засобами наукового пошуку. Методологічну основу становлять діалектико - матеріалістичний метод, що сприяє розумінню предмета дослідження у контексті поєднання потреб науки та практики, а також положення теорії пізнання.

У роботі використано такі методи: історико-правовий (дав змогу розкрити еволюцію формування наукових поглядів на окремі наукові проблеми - підрозділ 1.1); порівняльно-правовий (під час аналізу положень міжнародних стандартів таємниці спілкування та її регулювання в законодавстві зарубіжних держав - підрозділи 1.2, 3.3); *системного аналізу*, а також *системно-структурний* та *формально-логічний* методи дали можливість розкрити зміст таємниці спілкування, дослідити питання про процесуальні дії спрямовані на обмеження таємниці спілкування (підрозділи 2.1, 2.2).; формальної логіки (для визначення та класифікації елементів таємниці спілкування - підрозділ 1.1); догматичний (з метою тлумачення юридичних категорій - підрозділи 1.2, 2.1, 2.2); методи *моделювання* і *прогнозування* використано для формулювання пропозицій щодо вдосконалення окремих положень КПК України, які регулюють порядок

проведення слідчих (розшукових) та негласних слідчих (розшукових) дій (підрозділи2.1, 2.2, 3.1, 3.2). морфологічного аналізу (задля уточнення понятійно-категоріального апарату за проблемою - Розділи 1, 2, 3); статистичний (у процесі об'єктування статистичних даних та вивчення матеріалів слідчої та судової практики); абстрактно-логічний (для проведення теоретичних узагальнень та формулювання висновків); графічний (для наочного відображення результатів дослідження).

Емпірична база дослідження охопила зведені дані офіційні статистичні дані Генеральної прокуратури України за 2016-2020 рр., узагальнені матеріали вивчення 435 кримінальних проваджень; аналітично-довідкові матеріали Верховного Суду України, а також особистий досвід, набутий під час розслідування кримінальних проваджень.

Наукова новизна отриманих результатів полягає в тому, що дисертація є одним із перших у досліджень обмеження таємниці спілкування у кримінальному провадженні. Сформульовані положення спрямовані на розв'язання важливого наукового та практичного завдання, що полягає у визначенні процесуальних способів обмеження таємниці спілкування та використані отриманих результатів у доказуванні, а отримані висновки визначають перспективи наукового забезпечення протидії злочинності та підготовки фахівців для Національної поліції України. Зокрема:

вперше:

- запропоновано закріпити окрему слідчу (розшукову) дію «огляд електронної інформаційної системи», яка проводиться на підставі ухвали слідчого судді місцевого суду та має на меті отримання інформації з електронної інформаційної системи, яка знаходиться в розпорядженні слідчого, прокурора;

розроблено рекомендації щодо використання в доказуванні електронної інформації отриманої під час процесуальних дій, які обмежують таємницю спілкування;

запропоновано розширити сферу НСРД - арешт, огляд і виїмка

кореспонденції і зокрема передбачити в ході її проведення право відшуковувати поштово-телеграфну кореспонденцію, на яку необхідно накладати арешт. Така кореспонденція може відшуковуватися за почерком, за виглядом упаковки, місцем відправки чи одержання тощо;

обґрунтовано потребу та можливість запровадження інституту залучення особи, яка під час судового розгляду клопотань про НСРД буде забезпечувати дотримання прав осіб щодо яких будуть застосовуватися обмеження. В зв’язку з цим, запропоновано викласти ч. 1 ст. 261 КПК в наступній редакції «Слідчий суддя зобов'язаний розглянути клопотання про надання дозволу на проведення негласної слідчої (розшукової) дії протягом шести годин з моменту його отримання. Розгляд клопотання здійснюється за участю особи, яка подала клопотання та адвоката делегованого центром безоплатної правової допомоги». Такий адвокат, повинен мати допуск до державної таємниці, а доступ до матеріалів клопотання про надання дозволу на проведення НСРД буде надаватися слідчим суддею перед його судовим розглядом.

удосконалено:

розуміння поняття та змісту таємниці спілкування у кримінальному провадженні;

наукові погляди на систему процесуальних дій під час яких може обмежуватися таємниця спілкування;

теоретичні положення, що визначають процесуальний порядок проведення слідчих (розшукових) дій, які обмежують таємницю спілкування;

процесуальний порядок отримання дозволу на тимчасовий доступ до речей та документів. Рекомендовано долучати до клопотання про тимчасовий доступ до речей та документів, що знаходяться в операторів та провайдерів телекомунікацій, матеріали радіотехнічної розвідки, які дозволяють додатково ідентифікувати базові станції через які здійснювали спілкування підозрювані, а отже обмежити порушення таємниці спілкування невизначеної кількості абонентів.

дістали подальший розвиток:

положення, що шляхом тимчасового доступу до речей документів які знаходяться в операторів та провайдерів телекомунікацій може отримуватися лише інформація про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання, яка за своїм змістом охороняється таємницею спілкування.

підходи до розуміння змісту окремих негласних (слідчих) розшукових дій, зокрема, що своїм характером і аудіо-, відеоконтроль особи і місця мають на меті обмеження таємниці спілкування, та спрямовані на отримання доказової інформації, яка міститься в розмовах, рухах чи діях особи. Однак, якщо під час аудіо-, відеоконтролю особи нас цікавить конкретна особа, яка підозрюється у вчиненні кримінального правопорушення, то під час аудіо-, відеоконтролю місця коло осіб невизначене, в зв'язку з цим обмежується таємниця спілкування невизначеного кола осіб;

твердження, що у ч. 1 ст. 261 КПК потрібно встановити спеціальні вимоги до ухвали слідчого судді про надання дозволу на накладення арешту на кореспонденцію. Зокрема, в ухвалі слідчого судді мають бути вказані: підстави на яких буде проводитись слідча (розшукова) дія, прізвище, ім'я та по батькові особи, кореспонденція якої має затримуватися, точна адреса цієї особи, види кореспонденції, на яку накладається арешт, строк дії ухвали, назва установи зв'язку, на яку покладається обов'язок затримувати кореспонденцію та повідомляти про це слідчого.

Практичне значення отриманих результатів. Теоретичні положення, узагальнення та висновки, викладені у дисертації, можуть бути використані у:

науково-дослідницькій сфері - як підґрунтя для подальшої розробки проблем проведення процесуальних дій спрямованих на обмеження таємниці спілкування;

освітньому процесі - у межах викладання навчальних дисциплін «Кримінальний процес», «Криміналістика», «Доказування в кримінальному

процесі», для підготовки підручників, навчально-методичних і дидактичних матеріалів;

правоохоронній діяльності - як рекомендації щодо вдосконалення процесуального порядку та тактики проведення окремих процесуальних дій (акт впровадження в діяльність СУ ГУНП України у Львівській області від 05.03.2021 №3).

Особистий внесок здобувача. Теоретичні висновки і результати дисертаційної роботи отримано на підставі особистих досліджень автора. Дисертацію виконано автором самостійно.

Апробація матеріалів дисертації. . Наукова робота підготовлена накафедрі кримінального процесу та криміналістики факультету № 1 Інституту підготовки фахівців для підрозділів Національної поліції Львівського державного університету внутрішніх справ, обговорена на засіданні кафедри, схваленаі рекомендована до захисту. Результати дослідження оприлюднено на таких науково-практичних конференціях: «Процесуальне та криміналістичне забезпечення досудового розслідування (м. Львів, 01 грудня 2017 року)», «Процесуальне та криміналістичне забезпечення досудового розслідування» (м. Львів, 30 листопада 2018 року), «Правова система України: сучасний стан та актуальні проблеми» (м. Івано-Франківськ, 13 листопада 2020 р.).

Структура та обсяг дисертації. Дисертація складається з анотації українською та англійською мовами, вступу, трьох розділів, які містять дев’ять підрозділів, висновків, списку використаних джерел (всього 189 найменувань на 25 сторінках), додатків. Повний обсяг дисертації становить 185 сторінок, з яких основний текст - 160 сторінок.

РОЗДІЛ 1
ТАЄМНИЦЯ СПІЛКУВАННЯ ЯК ЗАСАДА КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

1.1. Поняття та зміст таємниці спілкування у кримінальному провадженні

Однією із фундаментальних цінностей світове співтовариство визнає таємницю спілкування – відповідні міжнародно-правові гарантії якої передбачені, зокрема, ст. 12 Загальної декларації прав людини 1948 р. [84], ст. 8 Конвенції про захист прав людини та основоположних свобод 1950 р. [93] та ст. 17 Міжнародного пакту про громадянські та політичні права 1966 р. [117]

Згідно 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.

Конституційний Суд України рішенням від 20.01.2012 р. у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України у п. 3.1 зазначив, що особистим життям фізичної особи є її поведінка у сфері особистісних, сімейних, побутових, інтимних, товариських, професійних, ділових та інших стосунків поза межами суспільної діяльності, яка здійснюється, зокрема, під час виконання особою функцій держави або органів місцевого самоврядування. КСУ резюмував, що неможливо визначити абсолютно всі види поведінки фізичної особи у сферах особистого та сімейного життя, оскільки особисті та сімейні права є частиною природних прав людини, які не є вичерпними, і реалізуються в різноманітних і динамічних відносинах майнового та немайнового характеру, стосунках, явищах, подіях тощо. Право

на приватне та сімейне життя є засадничою цінністю, необхідною для повного розквіту людини в демократичному суспільстві, та розглядається як право фізичної особи на автономне буття незалежно від держави, органів місцевого самоврядування, юридичних і фізичних осіб [143].

Важливо відзначити, що перелік видів комунікації, що знаходяться під конституційної охороною, є відкритим і охоплює не тільки листування, телефонні розмови, телеграфні повідомлення, але і іншу кореспонденцію. Дана конструкція норми дозволяє відповідати рівню технічного розвитку суспільства і гарантувати недоторканність нових, невідомих на момент розробки Конституції видів комунікації.

Закріплення у цій нормі таємниці спілкування в Конституції повністю відповідає міжнародним зобов'язанням України та визнаним стандартам захисту інформаційних прав людини.

Слушною є думка, що право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції є одним з основоположних прав людини і громадянина. тому його захист повинен бути одним із пріоритетних напрямів діяльності держави [68, с. 65].

Також необхідно відзначити й те, що динамічний розвиток телекомунікаційної інфраструктури суспільства й розробка нових технологічних рішень в області обміну інформацією містить і ряд негативних обставин, серед яких, насамперед, необхідно відзначити використання злочинцями засобів зв'язку при координації дій, плануванні, підготовці й реалізації злочинних задумів.

Таким чином, підвищена увага саме до даного елементу прав громадян на приватне життя - таємницю листування, телефонного зв'язку, телеграфної й іншої кореспонденції - не випадково, оскільки зазначений правовий інститут, з одного боку, у значній мірі пов'язаний з виконанням правоохоронними органами своїх обов'язків, а з іншого боку - містить у собі безліч нерозв'язаних теорією й практикою питань, пов'язаних із забезпеченням і захистом зазначеного конституційного права. Дана

обставина актуалізує проблему детальної законодавчої регламентації повноважень суб'єктів, пов'язаних з обмеженням конституційних прав громадян.

Зміст таємниці кореспонденції викладено у ст. 306 Цивільного кодексу України, відповідно до якої: 1) листи, телеграми та інші види кореспонденції можуть використовуватися, зокрема шляхом опублікування, лише за згодою особи, яка направила їх, та адресата; 2) якщо кореспонденція стосується особистого життя іншої фізичної особи, для її використання, зокрема шляхом опублікування, потрібна згода цієї особи; 3) у разі смерті фізичної особи, яка направила кореспонденцію, і адресата використання кореспонденції, зокрема шляхом її опублікування, можливе лише за згодою фізичних осіб – їх законних представників; 4) у разі смерті фізичної особи, яка направила кореспонденцію, і адресата, а також у разі смерті фізичних осіб – їх законних представників, кореспонденція, яка має наукову, художню, історичну цінність, може бути опублікована в порядку, встановленому законом; 5) 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; 6) порушення таємниці кореспонденції може бути дозволено судом у випадках, встановлених законом, з метою запобігання злочинові чи під час кримінального провадження, якщо іншими способами одержати інформацію неможливо.

Як вірно зазначає Л.В. Ємчук, право на таємницю кореспонденції можна визначити як гарантовану державою автономну можливість суб’єкта вільно та негласно обмінюватися інформацією, зокрема особистого характеру, у вигляді поштово-телеграфних відправлень (листів, телеграм, бандеролей, посилок, переказів та ін.), телефонних переговорів, електронного обміну повідомленнями тощо. Право на таку таємницю гарантується, зокрема, встановленням заборони на вчинення без достатніх правових підстав третіми особами будь-яких дій, спрямованих на збирання,

привласнення, збереження, розкриття чи інше використання, а також на поширення відповідної інформації про факт повідомлення, способи його доставки, вигляду, зміст повідомлення особу його відправника чи одержувача [79, с. 57].

Питання порушення таємниці спілкування неодноразово розглядалося Європейським судом з прав людини, який визначив, що право на конфіденційність листування та телефонних розмов не є абсолютним. Як зазначив Європейський суд з прав людини у рішенні в справі «Класс та інші проти ФРН» (1978 р.), існування законодавства, що дає повноваження із здійснення спостереження за листуванням, поштовими відправленнями і телефонними розмовами, є у виключних випадках необхідним у демократичному суспільстві в інтересах національної безпеки і/або для попередження безладдя та злочинів.

На думку Європейського суду з прав людини, захист приватного життя повинна враховуватися як при здійсненні телеконтролю, так і прослуховуванні [16]. З іншого боку, Європейський суд з прав людини вважає також, що офіційні органи для розслідування кіберзлочинів повинні мати можливість отримання даних про відправника, повідомлень від телеоператора тоді, коли це необхідно для розкриття злочину, який посягає на приватне життя потерпілого.

У справі Попеску проти Румунії оскаржувалося прослуховування і розшифровка телефонних розмов румунської розвідкою під час відсутності санкції прокурора щодо підозрюваного і відсутності законодавчої бази, яка надає достатні гарантії проти зловживань. Європейський суд зазначив недостатній рівень незалежності органів влади, уповноважених санкціонувати втручання у приватне життя [17].

Розгляд справи Копланд проти Сполученого королівства спричинив зміну англійського законодавства щодо загальних гарантій захисту приватного життя, при яких роботодавці не могли записувати або контролювати повідомлення працівників без їх згоди. За вимогою керівника

коледжу був встановлений контроль за використанням телефону, електронної пошти та Інтернету співробітником навчального закладу. Телефонні дзвінки з службових приміщень, що охоплюють поняття «особистого життя» і «кореспонденції», представляли собою втручання в її право на повагу до особистого життя і кореспонденції [8].

Так, О.В. Негодченко слушно пропонує замінити в законодавстві термін «листування, телефонних розмов, телеграфної чи іншої кореспонденції» на термін «таємниця спілкування» та визначити її як таємну інформацію, що міститься в листах, телеграмах, електронних повідомленнях фізичних та представників юридичних осіб, доступ до якої обмежено іншим суб'єктам, крім адресата й адресанта з метою реалізації їхніх інтересів, режим якої може бути порушено тільки у виняткових випадках, передбачених законом, за рішенням суду [123, с. 59]. Загалом погоджуючись з автором щодо заміни термінів варто зауважити, що його визначення не охоплює безпосереднього спілкування осіб, яке безумовно повинно охоплюватися таємницею спілкування.

С.В. Шевчук, на підставі аналізу практики Європейського суду з прав людини, однією з основних складових права на повагу до приватного життя виокремив його комунікативний елемент (безпека та приватність листування, електронної пошти, телефонних розмов та інших видів приватних комунікацій)[180, с. 362]

Однак, враховуючи розвиток суспільних відносин та інформатизацію усіх сфер життя суспільства та способів комунікації перелік видів комунікації, яка охороняється законодавством значно розширився. В зв'язку з цим, із прийняттям КПК України у 2012 році зміст конституційної норми про таємницю спілкування був розширений у ст. 14 КПК, згідно якої під час кримінального провадження кожному гарантується **таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування.**

Як зазначає І.І. Савляк, таємниця спілкування, як засада кримінального

провадження, – це правове положення, згідно з яким під час кримінального провадження кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування, яка може бути обмежена лише на підставі судового рішення у випадках, визначених законом [145, с. 25].

Втручання в таємницю спілкування можливо лише на підставі судового рішення у випадках, з метою виявлення та запобігання тяжкому чи особливо тяжкому злочину, встановлення його обставин, особи, яка вчинила злочин, якщо в інший спосіб неможливо досягти цієї мети. Інформація, отримана внаслідок втручання у спілкування, не може бути використана інакше, як для вирішення завдань кримінального провадження

Водночас ч. 3 ст. 358 КПК визначає, що 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.

Слушною є думка, що краще виходити з принципу нерозривної єдності спілкування й діяльності, а не зводити спілкування до однієї з його сторін – або до обміну інформацією, або до взаємодії, до впливу однієї сторони, що спілкується, на іншу, чи до процесу міжособистісної перцепції [119, с. 91].

Доцільно також звернути увагу на функції спілкування, які залежно від його мети поділяються на такі види: 1) контактна, мета якої – установлення контакту як стану обопільної готовності до приймання і передачі повідомлень і до підтримання взаємозв'язку у вигляді постійної взаємоорієнтованості; 2) інформаційна, мета якої – обмін повідомленнями (прийом-передача даних у відповідь на запит), а також обмін думками, задумами, рішеннями тощо; 3) спонукальна, мета якої – стимуляція активності партнера для спрямування його на виконання певних дій; 4) координаційна, мета якої – взаємне орієнтування й узгодження дій при

організації спільної діяльності; 5) функція розуміння, мета якої – не тільки адекватне сприйняття і розуміння змісту повідомлення, а і взаємне розуміння намірів, установок, переживань, станів тощо; 6) емотивна, мета якої – збудження в партнері потрібних емоційних переживань (обмін емоціями), а також зміна з його допомогою власних переживань і станів; 7) функція установлення відносин, мета якої – усвідомлення і фіксація свого місця в системі рольових, статусних, ділових, міжособистісних та інших зв'язків співтовариства, у якому діє індивід; 8) функція надання впливу, мета якої – зміна стану, поведінки, індивідуально-смислових утворень партнера, у тому числі його намірів, установок, думок, рішень, уявлень, потреб, дій, активності [139, с. 511 -512].

Відсутність застереження з боку законодавця щодо можливої обізнаності будь-кого із сторони спілкування про факт втручання в нього означає, що втручанням у приватне спілкування слід вважати кожний факт, який вказує на те, що будь хто із учасників такого спілкування не знав про доступ під час спілкування сторонніх осіб до його змісту. Порушення прав такого учасника приватного спілкування полягає в тому, що він позбавлений можливості своєчасно відмовитися від спілкування і не брати в ньому участі з огляду на наявну або й уявну загрозу його інтересам [91, с. 40].

Таким чином, за своїм змістом приватне спілкування є частиною таємниці спілкування та підлягає охороні в порядку ст. 14 КПК.

С. В. Єськов зазначає, що втручання в приватне спілкування є окремим елементом системи негласних слідчих (розшукових) дій, що відзначається такими ознаками, як: 1) спрямованість на отримання (збирання) доказів або перевірку вже отриманих доказів у кримінальному провадженні; 2) здійснення на підставі ухвали слідчого судді у кримінальному провадженні щодо тяжких або особливо тяжких злочинів у випадках, якщо відомості про злочин та особу, яка його вчинила, неможливо отримати в інший спосіб; 3) специфічність мети – отримання доступу до інформації, що зберігається чи передається за таких фізичних чи юридичних умов, при яких учасники

спілкування розраховують на захист інформації від втручання інших осіб [82, с. 270].

Не можна погодитися з думкою О. Білічак, яка вважає, що поняттям «приватне спілкування» охоплюються взаємні стосунки, ділові, дружні зв'язки особистого характеру, що не мають офіційного значення, не ділового характеру та існують поза державною службою. Тобто буквальне тлумачення змісту слів, які утворюють поняття «приватне спілкування», дає змогу дійти висновку, що ним охоплюється лише передача інформації від однієї особи до іншої у неофіційному порядку, коли кожен з учасників виступає від свого імені і діє як приватна особа, а не представник державного органу чи органу місцевого самоврядування [58, с. 99]. Продовжуючи свою позицію, автор вважає доцільно внести зміни до ст. 258 КПК України, згідно яких, приватним спілкуванням не вважатиметься спілкування особи, яка є державним службовцем чи представником органів місцевого самоврядування під час виконання ними своїх службових чи професійних обов'язків та реалізації передбачених законом повноважень [58, с. 101].

Такий підхід суперечить, як законодавчому визначенню, де приватне спілкування розглядається через призму суб'єктивного усвідомлення учасниками на приватність спілкування, так і практиці ЄСПЛ, яка визначає, що приватність спілкування повинна забезпечуватися у всіх випадках коли особи вважать, що їх спілкування не може бути відоме стороннім особам.

Правильною в цьому аспекті є точка зору авторів, які, визнаючи тісний зв'язок права на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції з правом на невтручання в особисте і сімейне життя, передбачене у ст. 32 Конституції України, зазначають, що норми ст. 31 Основного Закону України та ст. 14 КПК України виходять за межі виключно приватного життя і не можуть бути зведені тільки до забезпечення особистої або сімейної таємниці. Вони рівною мірою стосуються й сфери службових, ділових та інших суспільних відносин [102, с. 71].

Аналізуючи ст. 14 КПК можна виокремити наступні складові таємниці

спілкування:

- таємниця листування;
- таємниця телефонних розмов;
- таємниця телеграфної кореспонденції;
- таємниця іншої кореспонденції;
- таємниця інших форм спілкування [160, с. 158].

Розглянемо зміст кожної з таємниць окремо.

Таємниця листування. Згідно ст. 1 Закону України «Про поштовий зв'язок» лист це поштове відправлення у вигляді поштового конверта з вкладенням письмового повідомлення або документа, розміри і масу якого встановлено відповідно до законодавства України [138]. Таким чином виходячи із змісту цієї норми закон до листів відносить виключно матеріальні об'єкти. Водночас, згідно ст. 6 вказаного закону гарантується таємниця електронних повідомлень, що пересилаються (передаються) засобами зв'язку. На виконання даної норми були внесені зміни у Правила, які закріпили визначення відправлення електронної пошти - повідомлення, що подається для пересилання на паперовому або електронному носії інформації, передається з використанням інформаційно-комунікаційних технологій і доставляється/вручається одержувачу відтвореним на паперовому або електронному носії інформації. Відправлення електронної пошти, відтворене на паперовому носії інформації, доставляється/вручається одержувачу упакованим як письмова кореспонденція [135].

Варто звернути увагу, що закон говорить не про таємницю листування, а про таємницю поштових відправлень, яка за своїм змістом є значно ширшою. Зокрема до поштових відправлень належать листи, поштові картки, бандеролі, секограми, дрібні пакети, міжнародні відправлення з оголошеною цінністю, посилки, прямі поштові контейнери, оформлені відповідно до законодавства України (ст. 1 Закону України «Про поштовий зв'язок»).

В зв'язку з цим, вважаємо що таємниця спілкування охоплює не тільки таємницю листування (поштового чи електронного), а також таємницю

вказаних поштових відправлень.

Таємниця телефонних розмов. Телефонний зв'язок це передача на відстань мовної інформації, здійснюваної електричними сигналами телефонною мережею загального користування або радіосигналами. Таким чином, телефонними розмовами потрібно вважати спілкування осіб із використанням телефонного зв’язку.

Окремі правила режиму такого виду інформації з обмеженим доступом містяться в Законі України «Про телекомунікації», так 1) охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантуються Конституцією та законами України; 2) зняття інформації з телекомунікаційних мереж заборонено, крім випадків, передбачених законом; 3) оператори, провайдери телекомунікацій зобов’язані вживати відповідно до законодавства технічних та організаційних заходів із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами. Водночас дотримання таємниці кореспонденції та телефонних переговорів забезпечується наявністю юридичної відповідальності персоналу оператора, провайдера телекомунікацій за порушення вимог законодавства України щодо збереження таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв’язку або через комп’ютер, а також інформації з обмеженим доступом щодо організації та функціонування телекомунікаційних мереж в інтересах національної безпеки, оборони та охорони правопорядку.

Відповідно до ч. 1 ст. 34 Закону України «Про телекомунікації» оператори, провайдери телекомунікацій повинні забезпечувати і нести відповідальність за схоронність відомостей щодо споживача, отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

Відповідно до ч. 4 ст. 39 цього Закону оператори телекомунікацій зобов'язані за власні кошти встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових та розвідувальних заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових та розвідувальних заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення. Оператори телекомунікацій зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу.

Таємниця телеграфної кореспонденції. Що стосується поняття телеграфного відправлення, то в Законі «Про поштовий зв’язок» про нього взагалі не згадується. *Телеграма* — (від грецьких «далеко» та «літера, написання») – узагальнена назва офіційних та неофіційних документів, що становлять особливу групу за способом передачі повідомлення, листа або іншої інформації на відстань засобами телеграфного зв’язку. *Телеграфний зв’язок* (від грецьких слів «далеко» та «писати, записувати») – різновид зв’язку, що ґрунтується на передаванні певної інформації за допомогою спеціальних електричних (електронних) засобів. Здійснюється підприємствами та організаціями електрозв’язку або на договірних з ними засадах підприємствами поштового зв’язку [120, с. 32]. Технологія телеграфних повідомлень містить у собі вручення письмового тексту операторові зв’язку, перетворення його в електросигнали, їхню передачу каналами електричного зв’язку, зворотне перетворення отриманого повідомлення в письмовий вигляд і вручення тексту одержувачеві. Таким чином, телеграфні повідомлення можна одночасно відносити як до поштового, так і до електричного видів зв’язку [146, с. 62]. Водночас, варто заважити, що станом на сьогодні телеграфний зв'язок фактично не використовується.

Таємниця іншої кореспонденції. В даний час такі види повідомлень, як телеграфні та поштові в Україні користуються все меншою популярністю.

Однак паралельно з цим зростає кількість відправників і одержувачів електронних повідомлень, в тому числі за допомогою електронних поштових скриньок. Таке електронне листування теж є різновидом кореспонденції. Тому в ст. 6 Закону України «Про поштовий зв'язок» зазначено, що таємниця електронних повідомлень захищається нарівні з таємницею поштових відправлень, у тому числі листування та іншої письмової кореспонденції, що пересилається (передається) засобами зв'язку та гарантується Конституцією й законодавством України. У сучасних умовах поширення різних комп'ютерних комунікаційних систем постає актуальне питання правового забезпечення режиму таємниці спілкування, що здійснюється за їх допомогою [123, с. 58].

Електронна пошта - це система, за допомогою якої користувач комп'ютера має можливість обмінюватися повідомленнями з іншими користувачами (або групою користувачів) віддалених комп'ютерів через комп'ютерну мережу.

Всі електронні поштові скриньки можна розділити на 2 категорії:

1. Електронні поштові скриньки, які створюються користувачами самостійно на власних поштових сервісах.

2. Електронні поштові скриньки, які створюються на публічних поштових сервісах.

Електронні поштові скриньки першої категорії менш популярні, так як для їх створення необхідно володіти спеціальними знаннями в сфері інтернет-технологій, а також мати доменне ім'я, в основному такі скриньки створюються для потреб організацій [115, с. 271]. Електронні поштові скриньки, що належать до другої категорії, більш поширені серед громадян, для створення такої скриньки будь-які спеціальні знання не потрібні, а необхідно просто заповнити у форму на сайті публічного сервісу і отримати електронну поштову скриньку в своє користування.

Таємниця інших форм спілкування.

В науковій літературі немає єдності щодо розуміння змісту інших форм

спілкування. В. Т. Нор зауважує, що іншими «формами спілкування є повідомлення осіб за допомогою сучасних форм зв’язку – телефаксом, пейджинговим зв’язком, електронним зв’язком тощо» [103, с. 62]. М. І. Пашковський дотримується позиції, що до «інших форм спілкування можна віднести безпосереднє спілкування осіб (не опосередковане технічними чи іншими засобами), спілкування за допомогою телекомунікаційних засобів (електронної пошти, ICQ тощо) і т.п.» [104, с. 55].

Загалом підтримуючи, думки вказаних авторів, варто зауважити, що серед сучасних видів інших форм спілкування найбільшого поширення отримали: інтернет месенджери (WhatsApp, Telegram, Viber, Signal та інші), IP- телефонія, Skype, факсимільний зв'язок.

Разом з тим, технологічні процеси розглянутих видів зв'язку є досить складними для їх кримінально-процесуального та криміналістичного відображення. Технології зв'язку зазначених видів телекомунікаційних послуг виражаються шляхом визначення їх змісту.

Сучасні Telegram й інші захищені месенджери (англ. Instant messaging - служба миттєвих повідомлень) та окремі телекомунікаційні технології дають змогу забезпечувати закритий від сторонніх осіб обмін інформацією. Унаслідок зростання конфіденційності інформаційно-телекомунікаційних технологій і зумовлюється сьогоднішній інтерес до месенджерів і деяких апаратно-програмних засобів як інструмента створювання належних умов посередницького зв’язку учасників НСРД [107, с. 83].

Зокрема, у мегаполісах і великих містах під час проведення антитерористичних операцій (наприклад, листопад 2015 р. в Парижі та березень 2016 р. в Брюсселі) припиняються послуги стільникового телефонного зв’язку й рух громадського транспорту, але інтернет-провайдерам держава залишає можливість передавати телекомунікаційними мережами фото-, відео- контент користувачів із місць подій, тобто в умовах терористичної загрози наявні технічні канали взаємного сповіщення через глобальну мережу. Наприклад, 13 листопада 2015 р. в Парижі терористи

організовували шифровані комунікації із залученням технологій Tor і blockchain, а також використовували Telegram та інші захисні месенджери [107, с. 84-85].

Зокрема, кросплатформове програмне забезпечення Telegram із закритим кодом для передавання повідомлень працює на потужностях кількох американських і німецьких компаній, завдяки його патентуванню на сьогодні майже виявлені уразливості месенджера не дають змоги «зламати» його захист від читання листування в чаті. Інформація в Telegram у зашифрованому вигляді зосереджується на хмарному хостингу, а сервери розміщено в різних країнах, що надає можливість миттєво розсилати повідомлення. Листування розробником не зберігається заради таємності ключів шифрування, які для кожної пари осіб, що спілкуються за конкретний проміжок часу, лише свої. Ключі зберігаються від інших даних окремо, у різних юрисдикціях і лише на період спілкування осіб. У Telegram передаються файли розміром до 1 Гб і створюються мультичати до 100 осіб. Сьогодні всі ці переваги викликали зростаючу популярність цього месенджера, порівняно з іншими, у США, Чилі, Бразилії, Мексиці, Німеччині, Нідерландах, Іспанії, Італії та країнах Близького Сходу.

WhatsApp - це пропріетарний месенджер для смартфонів (програма обміну повідомленнями), який дозволяє пересилати текстові повідомлення, зображення, відео та аудіо. Буквально англійське proprietary значить «приватний», від латинського proprius - «володіння, власність». Messenger - від англійського слова «кур'єр» або «зв'язковий». Це програма для миттєвого обміну повідомленнями між користувачами. Саме в швидкості полягає їх головна перевага перед звичайною електронною поштою. Тут повідомлення передається блискавично, при цьому, оновлення поштової скриньки відбувається раз на кілька хвилин.

IP-телефонія - технологія, що дозволяє використовувати телекомунікаційну мережу, наприклад Інтернет, як засіб організації і ведення міжнародних і міжміських телефонних розмов і передачі факсів в режимі

реального часу. Для цього необхідно перевести звук в цифрову форму і передати його аналогічно тому, як пересилаються цифрові дані [47, с. 214].

Факсимільний зв'язок - телекомунікаційна технологія передачі зображень електричними сигналами. Історично включався до складу телеграфного зв`язку і є різновидом електрозв’язку.

Розглянуті технології зв'язку за поширеністю, дешевизною і швидкістю випереджають звичайні з'єднання між стаціонарними і мобільними телефонами, дозволяючи вести спілкування між двома і більше користувачами.

Крім того, до інших видів спілкування потрібно віднести таємницю особистого спілкування (у вербальній та невербальній формі), яка може бути обмежена в ході аудіо-відео контролю, спостереження за особою.

Таким чином, **таємниця спілкування полягає у недопущенні розголошення інформації, яка передається особами під час листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування за умови, що особи бажають її зберегти в таємниці.**

З’ясувавши зміст таємниці спілкування варто зауважити, що залежно від суб’єктів спілкування її можна розподілити на дві групи таємницю спілкування загальних суб’єктів та таємницю спілкування спеціальних суб’єктів. Виокремлення такого поділу зумовлено додатковими процесуальними гарантіями, якими наділені окремі суб’єкти.

Зокрема до спеціальних суб’єктів таємниця спілкування яких охороняється з дотриманням додаткових гарантій належать народні депутати.

Так, відповідно до ст. 482^2 КПК України клопотання про порушення таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції, а також про застосування інших заходів, у тому числі негласних слідчих (розшукових) дій, що відповідно до закону обмежують права і свободи народного депутата України, розгляд яких віднесено до повноважень слідчого судді, мають бути погоджені Генеральним прокурором (особою, що виконує обов’язки Генерального прокурора).

1.2. Міжнародні та європейські стандарти забезпечення таємниці спілкування

Стрімкий науково-технічний розвиток та світові глобалізаційні процеси сприяють передачі та обміну інформацією різноманітними способами. Протягом останнього десятиліття значно зросли масштаби цих процесів за допомогою різноманітних засобів зв'язку. Це в свою чергу породжує проблематику належного забезпечення таємниці спілкування, особливо в тоді, коли доступ до технічного засобу отримують представники правоохоронних органів. Демократичне суспільство може існувати тільки за наявності певного рівня автономії та конфіденційності [32, с. 19].

На сучасному етапі розвитку української держави євроінтеграційні процеси мають стратегічно важливе значення в контексті утвердження демократичних начал. Обрання Україною європейського вектору розвитку вимагає ґрунтовних, комплексних змін у її правовому середовищі, зокрема щодо кримінального процесуального законодавства стосовно відповідності його до міжнародних та європейських стандартів. Ці стандарти уособлюють найвдаліші приклади нормотворення та законодавчої техніки, є квінтесенцією багаторічної праці юристів, піднесеною в ранг глобальних або регіональних політико-правових еталонів [81, с. 107].

Цим обумовлюється потреба ретельного аналізу стандартів кримінального провадження, зокрема тих, які стосуються засади таємниці спілкування.

Базовим документом закріплення права на приватне життя стала Загальна декларація прав людини, яка була прийнята 10 грудня 1948 року Генеральною Асамблеєю ООН [84]. Стаття 12 Загальної Декларації проголошує: «Ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, тайну його кореспонденції або на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань».

Слід зауважити, що історичні витоки норми, яка закріплює право на

таємницю спілкування були у кримінальному законі. Схожа стаття була у кримінальному кодексі Бельгії у 1867 р., а згодом знайшла своє юридичне відображення і у Кримінальному кодексі Нідерландів 1881 р [113, с. 221].

Міжнародний пакт про громадянські та політичні права розширив сферу застосування цього права, передбачивши норму про те, що «жодна особа не може бути без її добровільної згоди піддана медичним чи науковим дослідам; що ніхто не може зазнавати безпідставного і незаконного втручання в його особисте та сімейне життя, свавільних чи незаконних посягань на недоторканість його житла, таємницю його кореспонденції чи незаконних посягань на його честь і репутацію; що кожна людина має право на захист закону від такого втручання або таких посягань (статті 7,17) [117].

Більш розгорнуто право на недоторканість приватного життя закріплене у Американській Конвенції про права людини 1969 р [49]. Ст. 11 цього документу передбачає, що «кожен має право на повагу його честі та визнання його гідності. Ніхто не може бути об'єктом довільного і образливого втручання в його приватне життя, життя його сім'ї, порушення недоторканості його житла чи таємниці його кореспонденції». Ця Конвенція дає можливість громадянам держав, які її підписали, ефективно відстоювати свої права та законні інтереси. Адже, у ст. 33 Американської Конвенції передбачено, що якщо громадяни вважають, що їх право порушене, то вони можуть звертатися за захистом у Міжамериканський Суд з прав людини.

Право особи на таємницю спілкування знаходить своє юридичне відображення також і у Арабській Хартії прав людини 1994 р [51]. У ст. 17 Хартії передбачено, що особисте життя недоторкане, порушення цієї недоторканості є кримінальним правопорушенням. Особисте життя включає в себе невтручання в сімейне життя, недоторканість житла, таємницю спілкування та інші види приватного спілкування [158, с. 209].

Щодо аналізу європейських стандартів забезпечення таємниці спілкування, то варто зазначити, що у ст. 2 Договору про Європейський Союз зазначено: «Союз засновано на цінностях поваги до людської гідності,

свободи, демократії, рівності, верховенства права та поваги до прав людини, зокрема осіб, що належать до меншин» [94]. Відповідно, демократичні начала, верховенство права та основоположні права людини – є тими цінностями, на основі яких існує Європейська Спільнота. Тому, приватність спілкування як фундаментально важливу засаду в розвиненому інформаційному суспільстві слід вважати одним з прагнень Союзу щодо забезпечення вищезгаданих цінностей [32, с. 19].

Іншим важливим актом, який на європейському рівні передбачає право особи на приватність є Хартія основних прав ЄС [177] (далі – Хартія), у ст. 7 якої закріплено, що «кожна людина має право на повагу до її приватного та сімейного життя, на недоторканість житла та таємницю кореспонденції». . Однак, аналізуючи ст. 7 Хартії, можна дійти висновку, що у ній прямо не зазначено перелік випадків допустимого обмеження органами державної влади права особи на спілкування. Однак, як вбачається із Пояснення до Хартії [29], зміст ст. 7 Хартії кореспондує ст. 8 Конвенції та всі обмеження цього права особи, закріпленні у Конвенції (які були згадані вище) є аналогічними і у розумінні Хартії.

Одним з базових актів ЄС, які регламентують засаду таємниці спілкування є Конвенція про захист прав людини та основоположних свобод (далі – Конвенція) [93]. Важко переоцінити значення та роль цієї Конвенції у забезпеченні захисту прав людини, адже вона є основним документом прийнятим Радою Європи у цій сфері. Страсбурзький Суд також підкреслив роль Конвенції як "конституційного інструменту європейського громадського порядку" у сфері прав людини [5]

Ст. 8 Конвенції передбачає, що кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. Слід зауважити, що вищезгадана ст. 8 Конвенції покладає на держави не лише негативний обов’язок утримуватися від свавільного втручання в особисте життя (тобто від будь яких дій обмежувального характеру, які не відповідають вищезазначеним трьом критеріям), а й також позитивний

обов’язок забезпечувати ефективні можливості для реалізації прав, закріплених у ст. 8 Конвенції та захист від втручання третіх осіб (шляхом прийняття будь-яких законодавчих, адміністративних та судових заходів). Як зазначав О. Дроздов, ці позитивні зобов’язання можуть включати в себе вжиття заходів, призначених забезпечити повагу до приватного життя навіть у сфері відносин індивідуумів один з одним [129, с. 9 -10].

О.П. Кучинська абсолютно слушно зауважує, що наявні певні розбіжності у формулюванні міжнародних стандартів цього права [108, с. 38]. Декларація захищає від безпідставного втручання, а Пакт у свою чергу від свавільного та незаконного втручання. Окрім цього, цінностями у розумінні Конвенції є «приватне, сімейне життя, житло та кореспонденція». У Пакті та ж окрім цих цінностей, згадані ще честь та репутація. О.І. Коровайко вважає, що в цьому контексті поняття «безпідставне» та «свавільне» варто розглядати як синонімічні, а з приводу кола охоронюваних цінностей, то зазначає, що « є наслідком більшої деталізації змісту самого права» [98, с. 78].

Відповідно до ч. 2 ст. 8 Конвенції право на приватність може бути обмежено органами державної влади, якщо дотримані наступні критерії:

- законність втручання;
- досягнення однієї із законних цілей (які перелічені у цій же ч. 2 ст. 8 Конвенції) та включають в себе широке коло інтересів держави та суспільства: «в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров’я чи моралі або для захисту прав і свобод інших осіб»;
- необхідність у демократичному суспільстві для досягнення іншої мети. Тобто втручання держави має бути пропорційним переслідуваним законним цілям.

У науковій літературі ст. 8 Конвенції справедливо називали черговою ілюстрацією поширеного в міжнародно-правових актах та в більшості

сучасних конституцій певного конфлікту між ліберальним закріпленням прав людини (ч. 1) і вимушеним обмеженням їхньої реалізації з підстав, що мають в переважній більшості чітко виражений комунітаристський відтінок (ч. 2) [127, с. 380].

Проаналізувавши ст. 8 Конвенції можна зауважити, що у ній закріплене саме право особи (на повагу до приватного і сімейного життя), заборону держави безпідставно втручатися у здійснення цього права та випадки допустимого втручання. Вищезазначене можна вважати структурою відповідного міжнародного стандарту. Однак, міжнародно-правові акти не дають вичерпної інтерпретації цих стандартів. Саме це зумовлює потребу звернення до прецедентної практики Європейського Суду з прав людини, в якій знаходять своє відображення окремі аспекти цього права.

Заслуговує уваги твердження про те, що ЄСПЛ є впливовим та автономним органом влади, покликаним уніфікувати міжнародні правозахисні стандарти у контексті відмінностей правових систем держав-учасниць Конвенції та безупинного розвитку правовідносин [66, с. 34]. Слід погодитися із думкою про те, що практика ЄСПЛ перетворила Конвенцію на живий механізм; вона розширила закріпленій в ній права й застосувала їх до ситуацій, які не можна було передбачити на час їх прийняття [72, с. 12]. ЄСПЛ поступово розробляв інноваційну інтерпретацію ст. 8 Конвенції, що призвело до розширення сфери її застосування [35, с. 152].

З аналізу положень Конвенції можна дійти висновку, що у ній немає тлумачень понять "приватне життя", "приватне спілкування" та вичерпного переліку суспільних відносин, що включаються до цих понять, а також чітких і зрозумілих критеріїв, яким повинно відповідати втручання у приватне спілкування осіб. Більш того, і у правових позиціях ЄСПЛ відсутнє уніфіковане визначення «приватного» життя. Більш того, Страсбурзький Суд не вважає за доцільне давати вичерпне визначення поняття «приватне життя» та вважає, що неправильно обмежувати його «внутрішнім колом», де кожен має право жити своїм власним життям, якому він надає перевагу, і

виключити з нього зовнішній світ, який не охоплюється складом цього кола (справа «Німіц проти Німеччини» [15]). Повага до приватного життя також має певною мірою охоплювати право встановлювати та розвивати відносини з іншими людьми [20].

Щодо згаданих вище трьох критеріїв (О.П. Горпинюк називає ці критерії «трискладовий тест») [72, с. 150] допустимості обмеження права на приватність органами державної влади, які зазначені у ст. 8 Конвенції (законність втручання, досягнення однієї із законних цілей, необхідність втручання у демократичному суспільстві), видається за доцільне здійснити їх аналіз в контексті практики ЄСПЛ.

Варто зауважити, що фраза *«згідно із законом»* не лише вимагає дотримання національного закону, а й стосується *якості* такого закону («Галфорд проти Сполученого Королівства» [11] та «Барановський проти Польщі» [6]. ЄСПЛ зазначає, що національне законодавство повинне досить чітко встановлювати межі та способи здійснення дискреційного права, яке надається органам державної влади, для того, щоб забезпечувати громадянам необхідний мінімальний ступінь захисту, на який вони мають право згідно з принципом верховенства права в демократичному суспільстві («Доменічіні проти Італії» [9]).

Окрім вимог щодо чіткості закону та встановлення у ньому обсягу дискреційних повноважень, цього, Європейський Суд встановлює вимоги *передбачуваності та адекватної доступності національного законодавства* [19].

Загальні формулювання у законі, та як наслідок, широкі дискреційні повноваження також являють практику, яка не відповідає вимогам ст 8 Конвенції. ЄСПЛ неодноразово вказував, що перевірка кореспонденції в'язнів, яка здійснювалася в автоматичному режимі на підставі норм, що сформульовані в досить загальній формі і які надають адміністрації місць позбавлення волі широкі дискреційні повноваження у цьому зв'язку, є такою яка не відповідає вимогам статті 8 Конвенції (див. справи «Нєдбала проти

Польщі» [14], Салапа проти Польщі» [18].

Варто зауважити, що існують справи про порушення ст. 8 Конвенції в контексті критерію «відповідно до закону» у практиці Європейського суду з прав людини і щодо України. Зокрема, у рішенні «Бєляєв та Дігтяр проти України» [7]. Суд встановив порушення щодо прав заявників на повагу до кореспонденції під час попереднього ув'язнення в Сумському СІЗО у зв'язку з тим, що відповідне національне законодавство не відповідало стандартам «якості закону» і що відсутність відповідних гарантій могла призвести до незаконної відмови надіслати деякі листи заявників.

Можна зробити припущення про те, що перший критерій – законність втручання – є в певній мірі першочерговим щодо двох інших критеріїв. З цього приводу слушно зазначала Т.І. Фулей, що якщо ЄСПЛ дійде висновку, що національне законодавство не відповідало вимогам якості закону, тобто що втручання не було «встановлене законом», він констатує порушення, не вдаючись до аналізу інших критеріїв, таких як відповідність втручання легітимній меті чи його необхідність [176, с. 145].

Визначення критерію *необхідності втручання у демократичному суспільстві* вважається найскладнішим [176, с. 148]. Загалом існують два різнополюсні інтереси в даному контексті: інтерес особи у захисті її приватності у кримінальному провадженні та інтерес органів досудового розслідування у збиранні доказів. Слушною видається думка про те, що «правильна» правова система – та система, у якій вдається досягти та підтримувати розумний баланс між вищезазначеними інтересами [1, с. 86].

ЄСПЛ розтлумачив це «необхідність в демократичному суспільстві» як «нагальна соціальна потреба» у такому втручанні. Державним органам влади перед таким втручанням необхідно здійснити аналіз нагальної соціальної потреби у кожному випадку індивідуально [10]. Також для того, щоб вищезазначений критерій вважався дотриманим, Суд враховуватиме чи були причини, з урахуванням обставин справи загалом, виправданими, належними та достатніми, і чи були ці заходи пропорційними законним цілям [21]. У

справі «Ляшко проти України» зазначено, що «Суд повинен перевірити, чи було втручання виправданим та необхідним у демократичному суспільстві, та, зокрема, чи було воно пропорційним, і чи були причини, надані національними органами влади на його виправдання, важливими та достатніми» [13].

Враховуючи, що право на приватність найчастіше підлягає обмеженню в кримінальному провадженні під час здійснення негласних слідчих (розшукових) дій, виникає необхідність проаналізувати стандарти ЄСПЛ з щодо таких дій, зокрема і прослуховування телефонних повідомлень, яким має відповідати національне законодавство країн-членів Ради Європи.

Згідно з цими стандартами закон, що обмежує право на таємницю телефонних розмов, повинен відповідати таким вимогам: 1) містити список злочинів, вчинення яких може привести до прослуховування; 2) включати фактичні підстави підозрювати особу у вчиненні злочину: вони повинні бути вже виявлені іншими засобами; 3) дозволяти прослуховування лише на підставі мотивованої письмової заяви певної високої посадової особи; 4) встановлювати необхідність отримання санкції органу або посадової особи, що не належить до виконавчої влади, бажано судді; 5) встановлювати обмеження на тривалість прослуховування: має бути вказаний період, протягом якого санкція на прослуховування дійсна; 6) визначати правила, що стосуються звітів, що містять матеріали перехоплених повідомлень; 7) передбачати запобіжні заходи проти обміну цими матеріалами між різними державними органами; 8) визначати обставини, за якими записи можна чи потрібно знищити; 9) встановлювати, що треба робити з копіями або переписаними матеріалами, якщо обвинувачену особу буде виправдано [38, с. 67].

Окрім таємниці спілкування, іншим важливим складовим елементом права на приватність є право особи на захист персональних даних. Однак, важливою новелою Хартії є закріплення права особи на охорону даних особистого характеру (ч. 1 ст. 8), а ч. 2 ст. 8 передбачає, що ці дані повинні

використовуватися відповідно до встановлених правил з відповідною метою, а також на основі згоди зацікавленої особи або ж на інших законних підставах, передбачених законом. Очевидно, вищезгадана стаття Хартії є юридичним відображенням захисту персональних даних, які разом з таємницею спілкування є одним з невід'ємних елементів приватності.

У 1981 році була відкрита для підписання Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (далі Конвенція про персональні дані) [92]. Її норми підлягають застосуванню до будь-якого процесу обробки даних, що здійснюється як у приватному, так і у державному секторах. Окрім цього, не можливо не згадати Директиву 95/46/ЄС Європейського парламенту та Ради Європи від 24 жовтня 1995 року «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» [76]. Її метою була гармонізація національного законодавства у сфері захисту персональних даних та розширення викладених у Конвенції принципів права на приватність.

Одним з недавніх актів ЄС щодо захисту персональних є Директива Європейського Парламенту та Ради про захист фізичних осіб щодо обробки їх персональних даних компетентними органами в цілях попередження, розслідування, виявлення та переслідування кримінальних злочинів чи виконання кримінальних покарань, а також вільної передачі таких даних № 2016/680 від 27 квітня 2016 р. [27, с. 101]. Окрім цього, не можна не згадати Регламент Європейського Парламенту і Ради ЄС про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільних рух таких даних 2016 /679 від 27 квітня 2016 р ., який набрав чинності 25 травня 2018 р. [42] (далі – Регламент про персональні дані), відомий як GDPR). Особливо пріоритетне значення цього акту у тому, що він є загальнообов'язковим документом без необхідності імплементації його норм до національного законодавства кожної країни-члена ЄС, а його норми мають пряму дію. Важливою метою розроблення Регламенту про персональні дані було

створення умов, за яких громадяни держав-членів ЄС довірятимуть цифровим послугам настільки, що будуть ними все частіше користуватися у повсякденному житті. Більш того, цей Регламент вважається як розроблення «нових механізмів контролю, які дозволять громадянам самостійно визначити якою кількістю даних вони готові ділитися і з ким» [24, с. 2].

Виникає актуальне питання розмежування сфери застосування вищезгаданих актів у сфері захисту персональних даних. Р. А. Климкевич вважає, що для застосування норм Директиви про персональні дані є необхідна наявність двох критеріїв:

- персональний – обробка персональних даних повинна здійснюватися компетентним органом;
- матеріальний – наявність спеціальної мети обробки цих персональних даних. Обробка цих даних повинна здійснюватися з метою попередження, розслідування, виявлення та обвинувачення злочинів чи виконання кримінальних покарань, а також для захисту та запобіганню загрозам громадській безпеці.

Якщо немає одного із двох необхідних критеріїв – будуть застосовуватися норми Регламенту про захист персональних даних [88, с. 50 - 51].

Суд Європейського Союзу у свої рішеннях визначив, який саме обсяг даних слід відносити до персональних даних: ім’я особи, телефонний номер, інформація про її місце роботи [43, с. 6], а також відбитки пальців, оскільки їх можна використовувати для точної ідентифікації осіб [43, с. 21].

Цікаво зауважити, що на початку 2020 року була дискусія з приводу збирання органами державної влади персональної інформації щодо коронавірусної інфекції осіб. Ця дискусія виникла в контексті права особи на захист своїх персональних даних, зокрема даних про стан здоров’я, які відповідно до Регламенту про персональні дані належать до особливої категорії персональних даних.

Таким чином, міжнародно-правова регламентація охорони приватного

життя та таємниці спілкування здійснила безпосередній вплив на національне законодавство багатьох держав. Як наслідок, право на таємницю спілкування, будучи міжнародним та європейським стандартом в сфері захисту прав і свобод людини, є об'єктом не лише міжнародно-правового, а і внутрішньодержавного регулювання. Право на недоторканість приватного життя та таємниці спілкування закріплене у низці міжнародно-правових та європейських актів, серед яких базовим є Конвенція про захист прав людини та основоположних свобод. Науковий інтерес становить дослідження критеріїв допустимості обмеження права на недоторканість приватного життя. Ст. 8 Конвенції видається недостатньо інформативною в цьому контексті та такою, що містить абстрактні законодавчі конструкції, такі як «необхідність у демократичному суспільстві». Це є одна з причин необхідності звернення до практики Європейського Суду з прав людини. Слід зазначити, що Суд не намагається дати визначення поняттю «приватне життя», а більшість його справ стосується тлумачення критеріїв допустимості обмеження права на недоторканість приватного життя.

Окрім права на таємницю спілкування, іншим важливим елементом приватного життя є персональні дані, проблематика захисту яких останнім часом набула особливої актуальності. Видається, що це пов'язане з нещодавнім прийняттям Регламенту про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільних рух таких даних 2016 /679 від 27 квітня 2016 р. (більш відомого як GDPD), який можна вважати справжнім «проривом» у сфері забезпечення охорони персональних даних..

1.3. Зарубіжний досвід правового регулювання таємниці спілкування та її обмеження у кримінальному провадженні

Соціально-економічні реформи, демократизація держави і суспільства, формування відповідної правової системи зумовлюють актуальність наукових досліджень щодо проблем юридичного забезпечення прав і свобод людини, зокрема і права на таємницю спілкування. Ці наукові дослідження не можуть уявлятися без вивчення аналогічного досвіду зарубіжних держав. Адже розвиток вітчизняного законодавства в сфері прав людини не відбувався сам по собі, а це частина загальносвітового процесу щодо визнання прав і свобод людини основними цінностями в суспільстві та державі [53, с. 187] Саме це зумовлює необхідність у дослідженні зарубіжного досвіду правового регулювання права на таємницю спілкування у законодавстві зарубіжних країн.

Не можна оминути увагою досвід правового регулювання права на таємницю спілкування у США, оскільки вперше сама ідея про недоторканість приватного життя вперше була закріплена в Конституції США 1787 р. [45] та Біллі про права 1791 р. [44]. В цих документах гарантії прав громадян на недоторканість приватного життя були встановлені досить обмежено. Це право розглядалося як право народу на гарантії недоторканості особистості, житла, документів та майна від незаконних обшуків та арештів.

Право осіб на захист приватного життя закріплений у Четвертій Поправці до Конституції США. У цій поправці зазначено, що «право народу на охорону особистості, житла, документів, майна не повинно порушуватися від необґрунтованих обшуків та арештів. Жодний ордер не повинен видаватися інакше, як за наявності достатньої підстави, підтвердженою присягою чи офіційною заявою; при цьому ордер повинен містити точний опис місця, яке підлягатиме обшуку та предметів, яку будуть арештовані» [116, с. 209]. Цією поправкою було створено прецедент, після якого така норма стала невід’ємним елементом каталогу основних прав людини [61, с. 21 - 22].

Верховний Суд США неодноразово у своїх рішеннях зазначав, що ця поправка являє собою «конституційну гарантію громадян від незаконного, необґрунтованого втручання у ті сфери приватного життя, які можна об'єднати одним терміном «прайвесі» [78, с. 53]. Відповідно виникає доцільність у більш детальному аналізі цієї концепції.

Спочатку захист «прайвесі» життя відповідно до цієї Поправки був схожий з формулюваннями, які були викладені у Біллі про права. Тобто інформація, яка отримана під час прослуховування під будинком особи не стосується обшуків чи виїмки, тому Поправка не поширювала свою дію на прослуховування. Однак, таке тлумачення захисту приватного життя було змінене рішенням у справі «Катц проти США» [12] , у якому зазначалося, що «прайвесі» у розумінні Четвертої Поправки – це не лише про фізичне вторгнення та завдання цієї Поправки є захист особи, а не місця [25, с. 20 - 21].

Першою спеціальною публікацією, присвяченою питанням «прайвесі», вважається стаття американських юристів 1890 р. С. Уоррена і Л. Брендіс «Право на приватне життя». Головна ідея публікації полягала у тому, що кожен громадянин має законні інтереси в сфері приватного життя, які повинні бути захищені. Вони тлумачили поняття «прайвесі» як «право бути залишеним в спокої». Значною перевагою концепції «прайвесі» запропонованої вченими було те, що вони не розглядати це поняття як константу. Тобто вони стверджували, що нові винаходи та технології (принтер та камера зокрема) заохочують робити нові кроки для мінімалізації втручання в приватне життя особи з боку ЗМІ для того, щоб захистити загальне право особи на недоторканість особи, а також право контролювати поширення інформації щодо себе та членів своєї сім'ї.

Інші правники тлумачать це поняття як право контролювати власну особистість, власний життєвий простір, відомості про самого себе [57, с. 39].

Варто зазначити, що саме поняття «прайвесі» є складним, різноманітним та неоднозначним. У науковій літературі немає одностайності

у поглядах щодо його розуміння.

Як зазначає І.В. Вегера-Іжевська, право на «прайвесі» часто ототожнюється з правом на приватність (the right to be let alone), яке розглядається як законна вимога індивідуума визначити міру, за якою він бажає контролювати доступ сторонніх осіб до сфери власного приватного життя, а також право індивідуума контролювати інформацію про самого себе, яка може вийти за межі власного інформаційного простору [61, с. 22].

В одній з концепції, «прайвесі» за свою суттю є етичним поняттям, яке розуміється як протилежне обов'язку людини показувати та розповідати все. В цій концепцій поняття «особистість» є ключовим та передбачає створення приватної сфери, відокремленої від інших сфер та суспільства в цілому. Статус рабів частково визначається саме відсутністю будь-якого права на приватність. Прайвесі також означає таємницю, якою людина може поділитися на власний розсуд з одною або декількома особами, а не суспільством в цілому [33, с. 40]. Е. Блустейн, аналізуючи поняття «особистість», вважав, що такі її позитивні риси як цілісність, гідність, самовизнання, незалежність тісно пов'язані із захистом приватного життя [4, с. 158].

Відповідно до іншої концепції, «прайвесі» розуміється як «вища цінність». Цей підхід був спробою знайти у приватному житті більш глибоку цінність або вигоди для задоволення власних потреб. На думку Позера вигоди від захисту «прайвесі» включають в себе майнову вигоду, захист репутації, захист від психологічних травм [41, с. 115].

Р. Пост виділяє три концепції «прайвесі»:

1.Перша концепція розглядає «прайвесі» для того, щоб створювати знання. Прайвесі блокує потік інформації для того, щоб уникнути спотворення або викривлення цієї інформації. Конфіденційність запобігає розкриттю інформації, яка не може бути правильно зрозумілою за певних обставин.

2. Друга концепція пов'язує «прайвесі» з гідністю. Прихильники цієї

теорії вважають, що необхідно закріпити приватність у соціальних формах поваги, яку ми повинні дотримуватися один щодо одного як члени єдиної соціальної спільноти. Ця концепція передбачає, що люди є перша за все соціальні істоти, чия особистість та власна гідність залежать від виконання соціальних норм, порушення яких становитиме «внутрішню» шкоду для них самих.

3. Третя концепція розуміє «прайвесі» крізь призму поняття свобода. На перший погляд можна помітити певну схожість цієї концепції концепцією гідності. Однак, основна відмінність полягає у тому, що концепція гідності апелює до виконання соціальних норм, а концепція свободи передбачає радше призупинення соціальних норм. Тобто відповідно до концепції свободи індивіди розглядаються як незалежні та автономні суб'єкти, яким створюється певний простір, у межах якого їм дозволено «самовизначатися» [39, с. 2087].

Щодо визначення «прайвесі», то С. Лі під «прайвесі» розуміє стан (а також правові та соціальні установки, що підтримують цей стан) відповідно до якого особи мають захищений ступінь контролю над тим, як вони представлені публічно з точки зору інформації про себе, яка є доступною для інших [36, с. 48]. А. Мур підтримував цю точку зору, вважаючи, що ідея контролю у концепції «прайвесі» є центральною [37, с. 216].

Слід зауважити, що ця точка зору знайшла підтримку і у вітчизняних правників. В. Серьогін визначив поняття прайвесі (право на недоторканість приватного життя) як соціально зумовлену й гарантовану міру можливої поведінки особи, визначену нормами об'єктивного права (як національного, так і міжнародного), що полягає в її можливості утримувати під повним контролем (фізичним, психологічним, інформаційним тощо) сферу свого приватного життя. Це право має на меті забезпечити автономію людини у сфері приватного життя для задоволення її власних потреб та інтересів щодо усамітнення та приватного спілкування. Воно на лежить до числа основних (конституційних) прав особи, особистих (громадянських) прав людини і

громадянина [150, с. 97].

У науковій літературі виділяють наступні елементи «прайвесі»:

- інформаційне «прайвесі» - передбачає встановлення правил збирання та обробки персональних даних;
- фізичне «прайвесі» - передбачає захист тіла людини від стороннього впливу, в тому числі і від випробування лікарських засобів та дослідження внутрішніх органів;
- комунікативне «прайвесі» - передбачає збереження та недоторканість поштових повідомлень, телефонних розмов, електронної пошти та інших видів зв'язку;
- територіальне «прайвесі» - передбачає обмеження вторгнення в житло, а також робоче місце [3, с. 6].

Варто зазначити, що зміст поняття «прайвесі» протягом останніх десятиліть зазнала значних змін в сторону розширення. Це пов'язане із розвитком суспільних відносин та виникнення нових інститутів суспільного життя. Одними із новітніх елементів «прайвесі» є право на штучне самовідтворення (клонування), право на смерть (евтаназія).

Враховуючи це, вищезазначена структура «прайвесі» видається дещо застарілою. На наш погляд, більш вдалою системою «прайвесі» слід вважати наступну:

1. За аспектами приватного життя: право на фізичну (тілесну, тактильну) приватність; право на фонетичну (звукову) приватність; право на візуальну (зорову) приватність; право на одорологічну (запахову) приватність; право на географічну (дислокаційну) приватність; право на інформаційну приватність (у т. ч. на таємницю особистого та сімейного життя).

2. За станами приватності: право на усамітненість (особисту автономію); право на інтимність (обмежене й захищене спілкування); право на анонімність (бути невпізнаним); право на нестриманість (емоційне вивільнення); право на автономність (регулятивно-вольову автономію); право

на утаємниченість (таємниці приватного життя).

3. За вимірами: право на просторову приватність (власний фізичний простір); право на часову приватність (час для приватного життя) [150, с. 95 - 96].

Щодо законодавчого регулювання прайвесі у США, то варто згадати *Федеральний закон про прайвесі 1974 р.* [40], який регламентує функціонування систем збору персональних даних осіб у федеральних відомствах та права осіб контролювати таку передачу іншим відомствам та *Закон про прайвесі електронних комунікацій 1986 р.* [28], який розширив обмеження на прослуховування телефонних дзвінків, передачу електронних даних за допомогою комп'ютера. Закон про прайвесі електронних комунікацій поділив усі повідомлення на 3 категорії: «суспільно доступні», «частково приватні», «приватні». Якщо повідомлення містило пароль і було передане через лінії чату, то цей вид повідомлень буде класифікуватися як «частково приватний». Якщо ж повідомлення передавалося електронною поштою, то воно розцінюється як «приватне».

Окрім цього, цей закон дозволяє перегляд провайдером приватних повідомлень у певних випадках - якщо він підозрює, що відправник вживає заходів із метою завдати шкоди системі або іншому користувачеві. Іншим випадком ймовірного перегляду провайдером електронних повідомлень є ситуації, коли відправник дає згоду на такий перегляд [151, с. 895].

Перехоплення телефонних та електронних повідомлень регламентується *розділом 18 глави 119 Зводу Законів США,* яка називається «Перехоплення дротових та електронних переговорів та прослуховування усних розмов». У цьому законодавчому акті передбачено дефініції таких понять як «дротова передача повідомлень», «усна передача повідомлень», «перехоплення», «електронний, механічний чи інший пристрій» та інші базові терміни.

За клопотанням уповноваженого прокурора федеральний суддя видає ордер на перехоплення телефонної, електронної, телеграфної комунікації та

повідомлень, яке здійснюється компетентними співробітниками ФБР або федерального агентства, яке займається розслідуванням тяжких кримінальних правопорушень, в тому числі і тими, що вчиняються членами злочинних організацій. При розгляді клопотання на проведення цієї слідчої (розшукової) дії суддя має право попросити додаткові дані, що які підтверджують необхідність отримання ордеру [46].

Європейські держави. Більшість конституцій держав європейський держав не мають спеціальної норми щодо охорони приватного життя громадян. До цих держав належать Австрія, Німеччина, Данія, Ірландія, Італія, Люксембург, Нідерланди, Фінляндія, Франція. Однак, в законодавстві цих держав передбачені засоби захисту приватного життя: недоторканість житла та таємниця листування, телефонних розмов, телеграфних і інших повідомлень [77, с. 209]. Так, основний закон Австрії 1867 р. передбачає, що втручання в особисте життя за виключенням передбачених законом випадків арешту та обшуку, може здійснюватися лиш в умовах війни або ж на основі рішення суду відповідно до чинного законодавства [95, с. 94]. Конституція Італійської Республіки 1947 р. передбачає, що недоторканість житла та таємниця листування можуть бути обмежені в випадках та порядку, передбачених законом і у відповідності до гарантій, встановлених для охорони особистої свободи [95, с. 425]. Конституція Данії 1953 р. допускає обмеження вищезгаданих прав тільки на основі рішення суду [95, с. 311]. Конституція Іспанії 1978 р. також обмежує використання інформації з тим, щоб «повною мірою охороняти честь, сімейне і особисте життя громадян і сприяти повній реалізації їх прав» [95, с. 374-375].

Досить детальною можна вважати правову регламентацію прав особи у Конституції Португалії 1976 р. Основний Закон гарантує громадянам таємницю приватного та сімейного життя. Окрім цього, у Конституції цієї країни зазначено, що не можна використовуватися в кримінальному процесі докази, отримані «в результаті незаконного втручання в приватне життя, порушення недоторканності житла, таємниці листування та повідомлень».

Органам державної влади заборонено «розкриття кореспонденції та прослуховування розмов, здійснених за допомогою електротехнічних засобів зв’язку, за винятком випадків, передбачених законом та пов’язаних зі здійсненням кримінального провадження» [95, с. 528 - 529].

Проаналізувавши конституційні положення щодо закріплення права на повагу до особистого життя окремих держав-членів ЄС, можна дійти висновку, що вони мають певну схожість у формулюваннях. Очевидно, що це пов’язане з впливом міжнародно-правових стандартів забезпечення прав людини, оскільки держави були зобов’язані привести своє національне законодавство у відповідність до цих стандартів [159, с. 80].

У більшості європейських держав основною процесуальною дією, яка обмежує таємницю спілкування є перехоплення комунікацій (interception of communication). На підставі аналізу і узагальнення зарубіжного законодавства можна зробити висновок про те, що даним терміном охоплюються чотири самостійних заходи:

1) перехоплення повідомлень електронної пошти;

2) прослуховування телефонних переговорів;

3) віддалений пошук;

4) прослуховування в приміщеннях або транспортних засобах.

Перехоплення повідомлень електронної пошти (interception of post) полягає в затриманні та огляді поштових і телеграфних відправлень, що надходять на ім'я певної особи через організації поштового зв'язку.

Прослуховування телефонних переговорів (wiretapping) полягає в застосуванні спеціальних технічних засобів, за допомогою яких переговори через лінії електрозв'язку (провідні і безпровідні) доступні як для аудіоконтролю, так і для запису на фізичні носії. У більшості держав, даним видом заходу охоплюється отримання відомостей про номери телефонів і тривалість трафіку (так званий білінг).

Віддалений пошук (remote searches) полягає у доступі за допомогою спеціальних програм до комп'ютера або до мобільного пристрою

підозрюваного віддалено через всесвітню інформаційну комп'ютерну мережу (Інтернет або іншим способом) певного абонента без його відома. Останнім часом до даного спеціального слідчого заходу більшість держав відносить віддалене зняття будь-якої комп'ютерної інформації.

Прослуховування в приміщеннях і в транспортних засобах (bugging) полягає в можливості аудіоконтролю і передачі (або запису) мови та інших звукових сигналів, що виходять з приміщення або транспортного засобу. Даний захід часто поєднується з спостереженням [86, с. 11].

Перейдемо до більш детального аналізу правового регулювання права на таємницю спілкування в окремих державах Європи. В КПК **Федеративної Республіки Німеччина** принцип недоторканості приватного життя та таємниця спілкування не знайшли своє юридичне відображення серед принципів кримінального провадження [31]. Однак, досить лаконічно це право закріплене у ст. 10 Конституції ФРН, у якій закріплено, що «таємниця листування, а також поштового, телеграфного та телефонного зв’язку недоторкана.

Обмеження можуть бути встановлені тільки на основі закону» [23]. З цієї норми можна зробити висновок, що допустимими обмеженнями прав особи (в тому числі і права на таємницю спілкування) є закон, в якому повинні визначатися передумови, сутність та межі відповідної дії (заходу), спрямованого на обмеження прав особи у кримінальному провадженні. У кримінальному процесуальному праві ФРН слідчі дії, пов’язані з обмеженням основних прав громадян можуть призначатися та проводитися лише компетентними органами. Такою компетенцією володіють (слідчий) суддя, прокуратура, посадові особи, які здійснюють досудове розслідування за дорученням поліції або поліція. При цьому законом встановлена залежність цієї компетенції від ступеня обмежень прав. Особливо суттєві обмеження основних прав осіб можуть здійснюватися лише на підставі рішення суду [70, с. 42].

Слідчими діями, які обмежують право особи на таємницю спілкування

є:

1. *Контроль та запис телекомунікацій* щодо підозрюваного та обвинуваченого регламентується § 100a КПК ФРН . Перш за все, слід з'ясувати, що буде охоплюватися поняттям «телекомунікації» у розумінні цієї статті. У КПК ФРН немає визначення цього поняття, однак Верховний Суд ФРН дає тлумачення цього поняття. Під телекомунікацією слід вважати розмови по міському та мобільному телефону, а також через Інтернет, включаючи розмови, що здійснюються поруч з телефоном під час контрольованих телефонних переговорів, а також розмови, прослуховування яких забезпечується одним із співрозмовників, навіть якщо він є (негласним) співробітником. Окрім цього, сфера дії цієї статті поширюється і на повідомлення, що надсилаються та отримуються по електронній пошті, в процесі передачі або зберігання на себрвері оператора; повідомлення, що передаються по факсу, телексу, СМС та повідомлення на автовідповідачі мобільного телефону [70, с. 151 -152].

Ця негласна слідча дія може проводитися, якщо:

1) певними фактами обґрунтовується підозра, що хто-небудь в ролі виконавця або співучасника виконав кримінальне карне діяння, зазначене у абз. 2 або у випадках, коли замах є кримінально карним, намагався вчинити злочин або готувався до його вчинення

2) саме діяння є тяжким

3) дослідження обставин справи або встановлення місця перебування обвинуваченого іншим способом було б неможливо або суттєво ускладнено.

Окрім обвинуваченого, такому контролю може піддаватися приватне спілкування і інших осіб, якщо є підстави вважати, що вони є «посередниками в передачі інформації», тобто передають або приймають повідомлення, призначені для підозрюваного або виходять від підозрюваного або ж обвинувачений користується їх телефоном. Ця слідча дія може проводитися, якщо є підтверджена конкретними фактами підозра у вчиненні тяжкого злочину, передбаченого у § 100a КПК та встановлення обставин

справи іншим способом було б істотно ускладненим. Значною перевагою є визначення німецьким законодавцем, що варто розуміти під тяжкими злочинами у контексті § 100а КПК. До злочинів, щодо яких допускається проведення контролю та запису телекомунікацій належать: державна зрада, підкуп депутата, вбивство, розбій, вимагання, відмивання грошей і приховання неправомірно отриманих цінностей, шахрайство, комп'ютерне шахрайство, отримання або дача хабара. Цікавим є те, що, що ця негласна слідча дія може застосовуватися не лише до злочинів, що визначенні кримінальним законодавством, а також і щодо правопорушень, передбачених податковим законодавством (ухилення від сплати податків, приховування доходів для оподаткування). Окрім цього цю негласну слідчу дію можна застосовувати у справах про незаконні діяння, передбачені іншими законами (Закон про провадження у справах біженців, Законом про внутрішню торгівлю, Закон про обіг наркотичних засобів та інші).

Контроль телекомунікацій здійснюється на підставі рішення суду за клопотанням прокуратури. без інформування про це особи, щодо якої проводиться ця дія. У виняткових випадках ця слідча дія може проводитися на підставі рішення прокурора з подальшим інформуванням про це відповідного суддю протягом трьох днів. Термін проведення цієї дії становить 3 місяці та при необхідності може бути продовжений. Про результати дії повідомляється суддя, який давав дозвіл на таке проведення.

Кримінальний процесуальний закон особливу увагу приділяє захисту таємниці листування, телефонних розмов, поштових, телеграфних та інших повідомлень, отриманих під час проведення цієї слідчої дії. Прослуховування телефонних розмов дозволяється без рішення суду у винятковому випадку: у разі виникнення загрози життю чи здоров'ю певної особи.

Прогресивною слід вважати норму, яка передбачає, що якщо існують фактичні підстави для припущення, що внаслідок здійснення контролю за телекомунікаціями буде отримана інформація, яка стосується виключно внутрішньої сфери приватного життя особи, то в такому випадку контроль за

телекомунікацією не допускається. КПК не тлумачить зміст поняття «внутрішня сфера приватного життя». Однак, вважається що, що таких комунікацій належить таке спілкування, коли співрозмовником близький родич, священнослужителі, служба довіри, захисники, лікарі, психологи [70, с. 153].

Застосування інформації про внутрішню сферу приватного життя особи, отримане внаслідок цієї негласної слідчої дії є недопустимим та відповідні записи повинні бути негайно знищені. Використання таких доказів є недопустимим.

Слід зауважити, що якщо один із користувачів мережі дає працівнику правоохоронного органу можливість підслухати його розмову з іншою особою, то в такому випадку відсутній контроль телекомунікацій в розумінні цієї статті КПК ФРН [60, с. 153].

2. *Встановлення телекомунікаційних даних.* Ця слідча дія передбачає застосування відповідних технічних засобів без відома особи для отримання негласного доступу до системи інформаційних технологій, що використовуються особою та для отримання даних з цієї системи. Тобто це передбачає встановлення контролю усіх телекомунікаційних даних у мережі (стільниковий зв'язок, інші види електронно-оптичного зв'язку). Ця слідча дія може застосовуватися лише до обвинувачених, а також щодо особливо тяжких злочинів, вичерпний перелік яких зазначений у тому ж параграфі.

3. *Прослуховування та запис непублічних висловлювань*. За межами житла можуть прослуховуватися та записуватися непублічні висловлювання без відома осіб щодо яких застосовується ця дія, якщо на основі конкретних фактів є припущення про те, що ця конкретна особи вчинила злочин, зазначений у § 100a КПК ФРН. Ця слідча дія може здійснюватися лише щодо обвинуваченого, а також і щодо інших осіб , коли на підставі певних факторів можна припустити, що вони із обвинуваченим перебуваються або такий зв'язок буде встановлений, застосування заходів призведе до з'ясування обставин справи або встановлення місця перебування

обвинуваченого, що іншим способом було би неможливо або суттєво ускладнено.

Аналогічно до інших слідчих дій, які обмежують право особи на таємницю спілкування, прослуховування та запис непублічних висловлювань може здійснюватися з дозволу суду, а у виняткових випадках на підставі рішення прокурора із подальшим повідомленням відповідного суддю.

4. *Виїмка поштово-телеграфних відправлень* передбачена § 99 КПК ФРН та передбачає вилучення у відділеннях зв'язку поштових відправлень, телеграм та листів, що були направлені обвинуваченому або відправлені ним, які знаходяться у фактичному володінні осіб чи підприємств, до сфери діяльності яких належить надання поштово-телеграфних послуг або участь в наданні таких послуг. Виїмка проводиться тільки на підставі рішення суду.

Варто зазначити, що Конституція **Швейцарії** окрім класичного та типового права особи на повагу до її приватного та сімейного життя, житла, а також таємниці кореспонденції передбачає право особи на захист від незаконного використання їх персональних даних [30].

Особливістю швейцарської негласної діяльності є відсутність оперативно-розшукових заходів поза межами кримінального процесуального регулювання. Швейцарський законодавець вважає, що всі дії, які спрямовані на виявлення, розкриття та розслідування кримінальних правопорушень мають єдині кримінально-процесуальні корені, тому немає необхідності їх диференціювати [163, с. 305 -306].

Значною нетиповою особливістю правового регулювання права особи на таємницю спілкування у законодавстві Швейцарії є переважання приватних інтересів над публічними. В КПК Швейцарії є норма, яка закріплює перелік предметів, які не можуть бути вилучені за жодних обставин. Мова йде про особисту документацію та кореспонденцію підозрюваного, якщо інтереси щодо захисту його особистості переважають над інтересами кримінального провадження; документація та кореспонденція, яка появилася в результаті спілкування обвинуваченого з

особами, які мають право відмовитися від бути свідками у кримінальному провадженні. Таку норму однозначно слід вважати прогресивно.

Однієї із слідчих дій, яка обмежує право особи на таємницю спілкування є *нагляд за поштовими та іншими відправленнями.* Це можливо зробити у разі якщо існують істотні підозри вважати, що було вчинене кримінальне правопорушення, тяжкість цього правопорушення виправдовує мету нагляду, попередні слідчі дії були не ефективні. Нагляд може здійснюватися за адресом поштових та інших відправлень обвинуваченого та третіх осіб, щодо яких є підстави вважати, що обвинувачений використовує адреса поштових та інших відправлень третьої особи. Ця негласна слідча діє може здійснюватися лише з дозволу суду по питаннях примусових заходів.

Нагляд за допомогою технічних засобів передбачає застосування прокуратурою технічних засобів з метою прослуховування або документування непублічних висловлювань або фіксування подій, що відбуваються у непублічних місцях. Ця слідча дія може застосовуватися лише щодо обвинуваченого [162, с. 275].

Окрім США та держав Європи, науковий інтерес становить аналіз правової регламентації права особи на таємницю спілкування та обмеження цього права у окремих **державах СНГ.**

Глава 2 Розділу 1 Кримінального процесуального кодексу **Республіки Молдова** встановлює загальні принципи кримінального провадження, серед них зокрема таємниця листування (ст. 14) та недоторканість приватного життя (ст. 15) [166].

У ст. 14 зазначено, що таємниця листування, телеграм і інших поштових відправлень, телефонних розмов та інших законних видів зв’язку забезпечується державою. Під час кримінального провадження ніхто не може бути позбавлений або обмежений цього права. Однак, ч. 2 цієї ж статті встановлює винятки із цієї загальної норми, зазначаючи, що «обмеження цього права допускається тільки на основі судового ордеру, виданого у відповідності до цього кодексу».

Під судовим ордером молдовський законодавець розуміє офіційний судовий документ, яким дозволяється проведення дій в кримінальному провадженні, спеціальних розшукових заходів, застосування заходів процесуального примусу або проведення інших процесуальних; містить в собі розпорядження, його обґрунтування та повноваження особи, що діє на підставі цього ордеру.

Ст. 15 КПК Молдови закріплює право особи на недоторканість приватного життя, таємниці інтимного і сімейного життя, захисту честі та гідності особи. В ході кримінального провадження ніхто не має права самостійно втручатися в інтимне життя особи. Особи, від яких органи кримінального переслідування вимагають надання відомостей про приватне та інтимне життя, мають право переконатися в тому, що ці відомості необхідні для конкретної кримінальної справи.

Варто зазначити, що у КПК Молдови представлена досить розгалужена система спеціальних розшукових дій ы використовується термін «спеціальні розшукові дії». Видається, що український відповідник цьому терміну «негласні слідчі (розшукові) дії.

До спеціальних розшукових дій, які можуть обмежувати право особи на таємницю спілкування належать:

1. *Прослуховування та запис розмов, запис зображень.* Суть цієї розшукової дії полягає у використанні технічних засобів з метою отримання інформації про зміст розмов між двома або більше особами, а в свою чергу запис розмов передбачає збереження отриманої при прослуховуванні інформації на технічний носій. Цікаво зазначити, що КПК Молдови дозволяє прослуховувати розмови не лише підозрюваного, обвинуваченого, а і також інших осіб, щодо яких є інформація, яка може привести до висновку про те, що ці особи або сприяли певним чином підготовці, здійсненню або приховуванню злочину, або отримують або передають важливу інформацію, яка має відношення до кримінального провадження. Видається, що коло суб’єктів, щодо яких можна провести цю спеціальну розшукову дію є надто

широким, що може призвести до втручання у приватне спілкування осіб, які в кінцевому результаті, як може виявитися, не мали відношення до кримінального провадження. Однак, перевагою законодавчого закріплення цієї спеціальної розшукової діє є вичерпний перелік кримінальних правопорушень, щодо яких допускається таке проведення.

2. *Затримання, дослідження, передача, огляд, виїмка поштових відправлень* (ст. 134 КПК Молдови). Якщо наявні достатні підстави вважати, що поштові відправлення можуть містити інформацію, яка має доказове значення, орган досудового розслідування має право здійснити затримання, дослідження, передачу, огляд та виїмку поштових відправлень. Однак, варто зазначити, що молдавський законодавець встановлює дві передумови щодо проведення цієї спеціальної розшукової дії. Перш за все, це ступінь тяжкості злочину. Ця дія може проводитися лише щодо тяжким, особливо тяжким або надзвичайно тяжким злочинам. Другою передумовою є то, що докази не можуть бути отримані іншим способом доказування.

До поштових відправлень, які можуть бути затримані, досліджені, передані, оглянуті або щодо яких може бути здійснена виїмка належать всі види листів, телеграми, радіограми, бандеролі, поштові посилки, поштові контейнери, грошові перекази, повідомлення по факсу та електронній пошті. Окремі науковці вважають не зовсім виправданим віднесення до поштових відправлень не лише традиційні види, а також і ті, що передаються засобами телекомунікаційного зв'язку та мережею Інтернет [112, с. 658].

3. *Моніторинг з'єднань, які стосуються телеграфних та електронних повідомлень.* Суть цієї спеціальної розшукової дії полягає у доступі та перевірці без повідомлення відправника та отримувача повідомлень, які були відправлені установам, що надають послуги по доставці електронних повідомлень чи інших повідомлень, а також вхідних та вихідних дзвінків абонента. Проведення цієї дії допускається у разі існування ймовірних підстав вважати, що вони містять або можуть містити інформацію про обставини діяння, які необхідно доказати.

4. *Збір інформації від постачальників послуг електронних комунікацій.* Ця дія являє собою збирання від установ зв'язку, операторів стаціонарного або мобільного телефонного зв'язку, інтернет-операторів інформації, яка передається по технічних каналах зв'язку (телеграф, телефакс, пейджер, комп'ютер, радіо та інші канали зв'язку), негласний запис інформації, що передається або отримується по технічних лініях зв'язку особами, щодо яких проводяться спеціальні розшукові заходи. А також отримання від операторів, наявної в них інформації про користувачів послуг зв'язку, а також щодо послуг зв'язку, які надаються цим особам. Це зокрема інформація про:

- власників номерів телефонів;
- телефонні номера, зареєстровані на ім'я одної особи;
- послуги зв'язку, які надавалися;
- джерело зв'язку (номер телефону особи, що телефонувала, прізвище, ім'я та місце проживання абонента);
- тип, дата, час тривалості зв'язку, включаючи невдалі спроби виклику;
- місцезнаходження пристрою мобільного зв'язку з моменту зв'язку.

Варто зазначити, що вищевказані дії можуть здійснюватися лише з дозволу суду. Наявність судового контролю за додержанням прав людини під час здійснення досудового розслідування є безперечною перевагою кримінального процесуального законодавства Молдови.

У Казахстані право особи на приватність та таємниця спілкування закріплені на конституційному рівні. У ст. 18 Конституції Казахстану зазначено, що «кожен має право на недоторканість приватного життя, особисту та сімейну таємницю, захист своєї честі та гідності». Окрім цього, кожен має право на таємницю особистих вкладів та збережень, телефонних розмов, поштових, телеграфних та інших повідомлень. Обмеження цього права допускається лише у випадках та порядку, прямо передбачених законом [96].

Окрім цього, вищезгадані принципи закріплені у ст. 16 КПК

Казахстану [165]. Ця стаття передбачає, що приватне життя громадян, особиста та сімейна таємниця знаходяться під охороною закону. Кожен має право на таємницю особистих вкладів і заощаджень, листування, телефонних розмов, поштових, телеграфних та інших повідомлень. При здійсненні кримінального провадження кожному гарантується право на недоторканість приватного життя. Обмеження цього права допускаються лише у випадках та порядку, прямо визначених законом. Окрім цього, передбачено, що ніхто не має права збирати, зберігати, використовувати та поширювати інформацію про приватне життя особи без її згоди, крім випадків, передбачених законом. Інформація про приватне життя особи, отримана в порядку передбаченому КПК Казахстану, не може використовуватися інакше як для цілей кримінального провадження.

Норма КПК Казахстану, яка закріплює право особи на недоторканість приватного життя фактично дублює відповідну статтю Конституції. Однак, варто зауважити, що недоторканість приватного життя у розумінні КПК значно ширша та охоплює собою ще і захист персональних даних. З аналізу цієї норми можна дійти висновку, що казахський законодавець встановлює досить чітке, детальне та вичерпне правове регулювання права особи на недоторканість приватного життя у порівняні з законодавцями інших держав.

Окремою главою казахський законодавець виділив слідчі дії, що можуть обмежувати право особи на недоторканість приватного життя та таємницю спілкування, які отримали назву «негласні слідчі дії». До таких дій належать:

1. *Негласний аудіо-, відеоконтроль особи* регламентована ст. 242 КПК Казахстану та передбачає негласний контроль словесної та іншої інформації, який проводиться шляхом негласного проникнення та (або) обстеження з використанням відео-, та аудіотехніки або інших спеціальних науково-технічних засобів з одночасною фіксацією їх змісту на матеріальному носії

2. *Негласний контроль, перехоплення та зняття інформації, що передається по мережі електричного (телекомунікаційного) зв'язку.*

Юридичним відображенням цієї негласної слідчої дії є ст. 243 КПК Казахстану, яка передбачає негласний контроль є негласним прослуховування та (або) запис голосової інформації із застосуванням науково-технічних засобів та (або) комп'ютерних програм, що передається по телефону або інших пристроях, які дозволяють передавати голосу інформацію. В свою чергу, перехопленням та зняттям інформації відповідно до казахського законодавства є перехоплення та зняття знаків, сигналів, голосової інформації, письмового тексту, зображень, відеозображень, звуків та іншої інформації, що передається по провідній, радіо, оптичній та іншій електромагнітних системах.

3. Негласне знаття інформації з комп'ютерів, серверів та інших пристроїв, призначених для збирання, обробки, накопичення та зберігання інформації (ст. 245 КПК Казахстану). Зміст цієї негласної слідчої дії полягає у негласному знятті спеціальними науково-технічними засобами та (або) комп'ютерними програмами інформації з комп'ютерів, серверів та інших приладів, призначених для збирання, обробки, накопичення та зберігання інформації, що здійснюється за необхідності шляхом негласного проникнення та обстеження.

4. Негласний контроль поштових та інших відправлень (ст. 246 КПК Казахстану). Ця слідча дія може здійснюватися щодо листів, телеграм, радіограм, бандеролей, посилок та інших видів поштових відправлень, якщо є підстави вважати, що вони можуть містити відомості, документи та предмети, які мають значення для кримінального провадження. Передбачає обов'язок поштової установи або особи, яка надає поштові послуги негайно інформувати слідчого, дізнавача про надходження поштового або іншого відправлення, що підлягає контролю.

Ці дії проводяться, якщо необхідно отримати відомості про факти для з'ясування обставин, що підлягають доказуванню в кримінальному провадженні без інформування особи. Ці дії проводяться уповноваженим підрозділом правоохоронного або спеціального державного органу з

використанням форм і методів оперативно-розшукової діяльності за дорученням органу досудового розслідування (за винятком негласного контролю поштових відправлень). Процесуальною підставою проведення вищезазначених негласних слідчих дії є рішення слідчого судді спеціалізованого слідчого суду, спеціалізованого міжрайонного слідчого суду. Можемо зробити висновок про існування судового контролю на стадії досудового розслідування, що є безперечною гарантією захисту прав підозрюваних, обвинувачених.

Негласні слідчі дії в Казахстані можуть проводитися щодо кримінальних правопорушень, санкція за які передбачає покарання у вигляді позбавлення волі строком понад 1 рік, а також щодо злочинів, вчинених злочинною організацією. Видається, що відповідно до цієї норми КПК Казахстану негласні слідчі дії можна проводити до досить широкого кола кримінальних правопорушень. Як наслідок, це призводить до того, що практичне здійснення цих дій відбувається часто і, відповідно, часто обмежується право особи на таємницю спілкування. Вбачаємо, що доцільно було б змінити цю норму КПК Казахстану, обмеживши коло діянь щодо яких допустимо обмежувати право особи на таємницю спілкування більш серйозними кримінальними правопорушеннями.

Іншим недоліком правового регулювання негласних слідчих дій у Казахстані є доволі широке коло суб'єктів щодо яких їх можна проводити. До цих суб'єктів належать підозрюваний; потерпілий (з його письмової згоди); третя особа, яка є відомості, що вона отримує або передає інформацію, яка має значення для кримінального провадження; особа, на яку у заяві або повідомленні про вчинення кримінального правопорушення вказано як на особу, що його підготовлювала, вчиняла або вчинила, або щодо якої є інші підстави вважати, що вона має відношення до розслідуваного правопорушення або володіє інформацією про підготовлене, вчинюване або вчинене кримінальне правопорушення.

Конституція **Республіки Узбекистан** у ст. 27 встановлює право особи

на захист від посягань на її честь та гідність, втручання в приватне життя, недоторканість житла, таємницю листування та телефонних розмов [97].

Однак, це право не є абсолютним та у Конституції передбачено можливість його обмеження: такі обмеження повинні здійснюватися у випадках та в порядку передбаченому законом.

Варто зауважити, що у КПК Узбекистану не має окремої статті, яка закріплює право особи на повагу до приватного життя чи таємницю спілкування [167]. Ст. 18 КПК Узбекистану має назву «Охорона прав і свобод громадян», у якій з поміж інших гарантій прав осіб зазначено, що «приватне життя громадян, їх недоторканість їх житла, таємниця листування, телеграфних повідомлень та телефонних розмов охороняється законом. Окрім цього, узбецький законодавець зазначає, що дії, які обмежують права громадян можуть проводитися лише в випадках та порядку, передбаченому в законодавстві. Мова йде про такі дії, як обшук, виїмка, огляд житла чи іншого приміщення, прослуховування розмов, які здійснюються за допомогою телефонів та інших телекомунікаційних приладів, зняття переданої з них інформації.

Способи збору інформації шляхом проведення оперативно-розшукових і інших слідчих дій правоохоронними органами часто супроводжується прямим втручанням в приватне життя громадян, обмеженням та порушенням їх прав і свобод [89, с. 10]. Для цього твердження існує декілька причин.

По перше, значним недоліком правового регулювання негласної діяльності органів правопорядку Республіки Узбекистан (орд та негласних слідчих (розшукових дій) є відсутність прописаних в законі чітких підстав для їх застосування. Це суперечить не лише Конституції Узбекистану, а і міжнародними договорам (зокрема, Міжнародному Пакту про громадянські та політичні права).

По-друге, відповідно до КПК Узбекистану право санкціонувати проведення оперативно-розшукових заходів, а також прослуховування розмов та обшуку має право прокурор. Однак, кодекс не передбачає судового

контролю за проведенням цих дій, що також є значним недоліком КПК Узбекистану.

Зупинимося більш детально на тих слідчих діях, які можуть обмежувати право особи на таємницю спілкування. Дивним видається той факт, що у КПК Узбекистану не виокремлені негласні слідчі (розшукові) дії в окремий структурний елемент кодексу, а знаходяться разом зі всіма слідчими діями у третьому Розділі, який має назву «Доказування і обставини, що підлягають доказуванню». Більш того, узбецький законодавець не використовує спеціального терміну для негласних слідчих дій. З аналізу цього третього розділу, можна дійти висновку, що у КПК Узбекистану є лише одна слідча дія, яка може порушувати право особи на таємницю спілкування. Це *прослуховування розмов, які здійснюються за допомогою телефонів та інших телекомунікаційних приладів.* В контексті цієї слідчої дії можна виділити два види прослуховування. Перший вид прослуховування досить класичний, стосується підозрюваного, обвинуваченого. У КПК Узбекистану зазначено, що якщо зібрані у справі докази дають достатньо підстав вважати, що можуть бути отримані дані, які мають значення для провадження, то відповідні суб'єкти (дізнавач, слідчий) видають постанову про проведення цієї дії. При прослуховуванні повинен бути здійснений звукозапис розмови.

Другий вид прослуховування є досить нетиповим. У КПК Узбекистану є норма, яка передбачає втручання у приватне спілкування з дозволу певних суб'єктів. Мова йде про згадану вище слідчу дію, яка може проводитися щодо потерпілого, свідка та їх близьких родичів, якщо існує щодо них загроза здійснення насильства, вимагання чи інших протиправних дій. У такому разі може здійснюватися прослуховування розмов, що здійснюються з їх телефонів або інших телекомунікаційних приладів. Для цього виду прослуховування потрібна заява вищезгаданих суб'єктів або їх письмовий дозвіл, а також обов'язковим є санкціонування прокурора або ж суду. З огляду на вищезазначене, цей вид прослуховування можна назвати

«легітимним».

Варто зазначити, що право на спілкування може обмежуватися не лише під час проведення негласних слідчих (розшукових) дій у межах кримінального провадження, а також і під час проведення оперативно-розшукової діяльності. Взагалі, щодо розмежування оперативно-розшукової та негласної кримінальної процесуальної діяльності, варто сказати, що у межах пострадянських країн склалося три різні моделі:

- відсутність нормативної регламентації негласних дій поза межами кримінального процесуального закону (Естонія)
- визначення негласних дій як в межах кримінально-процесуальної, так і оперативно-розшукової діяльності (Казахстан, Латвія, Литва, Молдова, Україна)
- визначення оперативно-розшукової та кримінально-процесуальної діяльності в якості двох відокремлених правових режимів (Азербайджан, Вірменія, Білорусь, Росія, Узбекистан) [50, с. 100].

З метою уніфікації положень нормативно-правових актів країн СНГ, що регулюють оперативно-розшукову діяльність на пленарному засіданні Міжпарламентської Асамблеї держав-учасників СНГ було прийнято Модельний Закон «Про оперативно-розшукову діяльність». У цьому законі є перелік 17 оперативно-розшукових заходів. Однак, у законодавстві держав СНГ відображені не усі ці заходи. Наприклад, у законодавстві Узбекистану є 15 заходів орд, у Вірменії – 16, у Казахстані – 23, у Киргизстані – 21 [124, с. 53]. У цьому Модельному Законі є заходи, які обмежують право особи на таємницю спілкування. До таких захотів належать контроль поштових відправлень, телеграфних та інших повідомлень, прослуховування телефонних розмов, слуховий контроль, зняття інформації з технічних каналів зв’язку, оперативне втручання, моніторинг інформаційно-комунікативних систем. У національному законодавстві всіх вищезгаданих державах закріплені такі заходи як контроль поштових відправлень, телеграфних та інших повідомлень, прослуховування телефонних розмов,

зняття інформації з технічних каналів зв'язку, оперативне втручання [124, с. 54].

Таким чином, аналіз правового регулювання права на таємницю спілкування у різних зарубіжних державах дає змогу дійти висновку про різний ступінь захисту цього права. США справедливо вважають «батьківщиною» «прайвесі». У науковій літературі існує плюралізм концепцій «прайвесі»: як етична категорія, як «вища цінність», як похідне від гідності, як похідне від свободи. Щодо змісту цього поняття, то варто зазначити, що із розвитком суспільних відносин, це поняття зазнає відповідного логічного розширення. Класична чотирьохелементна структура «прайвесі» (фізичне, територіальне, інформаційне, комунікативне) на даний час видається неактуальною, оскільки поняття «прайвесі» тепер охоплює і новітні елементи.

Щодо обмеження прайвесі у законодавстві США, то не можна оминути увагою Закон про прайвесі електронних комунікацій 1986 р., який у певних випадках дозволяє перегляд приватних повідомлень провайдером.

Щодо європейський держав, було проаналізовано правову регламентацію права на таємницю спілкування ФРН та Швейцарії. У останній менша кількість негласних слідчих дій, що можуть обмежувати право особи на таємницю спілкування. У Швейцарії до таких дій належать нагляд за поштовими та іншими відправленнями та нагляд за допомогою технічних засобів, в той час як кримінальне процесуальне законодавство ФРН до такої категорії дій відносить контроль та запис телекомунікацій, негласний віддалений пошук систем інформаційних технологій, прослуховування та запис непублічних висловлювань та виїмка поштової кореспонденції.

Серед держав СНГ особливо виділяється системністю та чіткою структурністю КПК Казахстану, який передбачив негласні слідчі дії окремою главою. До таких негласних слідчих дій, які можуть обмежувати право особи на таємницю спілкування належать негласний аудіо-, відеоконтроль особи,

негласний контроль, перехоплення та зняття інформації, що передається по мережі електричного (телекомунікаційного) зв'язку, Негласне знаття інформації з комп'ютерів, серверів та інших пристроїв, призначених для збирання, обробки, накопичення та зберігання інформації, негласний контроль поштових та інших відправлень. Однак, незважаючи на переваги КПК Казахстану, він не позбавлений певних недоліків, які мають негативний вплив на право особи на таємницю спілкування (зокрема, широке коло кримінальних правопорушень, щодо яких можна застосовувати ці дії). Від КПК Казахстану суттєво відрізняється в негативному КПК Узбекистану. Найбільшим недоліком кримінального процесуального законодавства Узбекистану, яке впливає на таємницю спілкування, є відсутність чітких підстав для застосування слідчих дій, які можуть обмежувати право особи на таємницю спілкування, а також відсутність судового контролю за проведенням таких дій.

Висновки до Розділу 1

1. Можна виокремити наступні складові таємниці спілкування:

- таємниця листування;
- таємниця телефонних розмов;
- таємниця телеграфної кореспонденції;
- таємниця іншої кореспонденції;
- таємниця інших форм спілкування.

2. Таємниця спілкування полягає у недопущенні розголошення інформації, яка передається особами під час листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування за умови, що особи бажають її зберегти в таємниці.

3. Залежно від суб'єктів спілкування таємницю спілкування можна розподілити на дві групи: таємницю спілкування загальних суб'єктів та таємницю спілкування спеціальних суб'єктів. Виокремлення такого поділу зумовлено додатковими процесуальними гарантіями, якими наділені окремі суб'єкти кримінального провадження.

4. Міжнародно-правова регламентація охорони приватного життя та таємниці спілкування здійснила безпосередній вплив на національне законодавство багатьох держав. Як наслідок, право на таємницю спілкування, будучи міжнародним та європейським стандартом в сфері захисту прав і свобод людини, є об'єктом не лише міжнародно-правового, а і внутрішньодержавного регулювання. Право на недоторканість приватного життя та таємниці спілкування закріплене у низці міжнародно-правових та європейських актів, серед яких базовим є Конвенція про захист прав людини та основоположних свобод. Науковий інтерес становить дослідження критеріїв допустимості обмеження права на недоторканість приватного життя. Ст. 8 Конвенції видається недостатньо інформативною в цьому контексті та такою, що містить абстрактні законодавчі конструкції, такі як «необхідність у демократичному суспільстві». Це є одна з причин необхідності звернення до практики Європейського Суду з прав людини.

Слід зазначити, що Суд не намагається дати визначення поняттю «приватне життя», а більшість його справ стосується тлумачення критеріїв допустимості обмеження права на недоторканість приватного життя.

5. Аналіз правового регулювання права на таємницю спілкування у різних зарубіжних державах дає змогу дійти висновку про різний ступінь захисту цього права. США справедливо вважають «батьківщиною» «прайвесі». У науковій літературі існує плюралізм концепцій «прайвесі»: як етична категорія, як «вища цінність», як похідне від гідності, як похідне від свободи. Щодо змісту цього поняття, то варто зазначити, що із розвитком суспільних відносин, це поняття зазнає відповідного логічного розширення. Класична чотирьохелементна структура «прайвесі» (фізичне, територіальне, інформаційне, комунікативне) на даний час видається неактуальною, оскільки поняття «прайвесі» тепер охоплює і новітні елементи. Щодо обмеження прайвесі у законодавстві США, то не можна оминути увагою Закон про прайвесі електронних комунікацій 1986 р., який у певних випадках дозволяє перегляд приватних повідомлень провайдером.

6. Щодо європейських держав, було проаналізовано правову регламентацію права на таємницю спілкування ФРН та Швейцарії. У останній менша кількість негласних слідчих дій, що можуть обмежувати право особи на таємницю спілкування. У Швейцарії до таких дій належать нагляд за поштовими та іншими відправленнями та нагляд за допомогою технічних засобів, в той час як кримінальне процесуальне законодавство ФРН до такої категорії дій відносить контроль та запис телекомунікацій, негласний віддалений пошук систем інформаційних технологій, прослуховування та запис непублічних висловлювань та виїмка поштової кореспонденції.

РОЗДІЛ 2
ПРОЦЕСУАЛЬНІ ДІЇ СПРЯМОВАНІ НА ОБМЕЖЕННЯ ТАЄМНИЦІ СПІЛКУВАННЯ

2.1. Система та процесуальний порядок проведення дій спрямованих на обмеження таємниці спілкування

За наявності конституційних гарантій прав громадян в інформаційній сфері законодавством України передбачено тимчасові обмеження реалізації цих прав. Такі винятки з прав на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції встановлюються лише судом у випадках, передбачених законом, з метою запобігання злочинові чи з'ясування істини під час розслідування кримінальних справ, якщо іншими способами одержати інформацію неможливо.

Даючи офіційне тлумачення положень частин першої, другої ст. 32 Конституції України у системному зв'язку з ч. 2 ст. 34 Конституції, Конституційний Суд України дійшов висновку, що збирання, зберігання, використання та поширення державою, органами місцевого самоврядування, юридичними або фізичними особами конфіденційної інформації про особу без її згоди є втручанням в її особисте та сімейне життя, яке допускається винятково у визначених законом випадках і лише в інтересах національної безпеки, економічного добробуту та прав людини [143].

Дане конституційне положення логічно продовжено в ч. 2 ст. 14 КПК згідно якої, втручання у таємницю спілкування можливе лише на підставі судового рішення у випадках, передбачених КПК, з метою виявлення та запобігання тяжкому чи особливо тяжкому злочину, встановлення його обставин, особи, яка вчинила злочин, якщо в інший спосіб неможливо досягти цієї мети.

Чинне законодавство встановлює, що процесуальні дії спрямовані на обмеження таємниці спілкування, як правило, проводяться на підставі узвали слідчого судді. Такий складний порядок доступу правоохоронних органів до матеріальних носіїв інформації, що складає таємницю спілкування, свідчить

про пріоритетний характер цього виду таємниці в системі інформації з обмеженим доступом, передбаченій вітчизняним законодавством.

На користь зазначеного висновку свідчить і факт наявності у Кримінальному кодексі норми, що передбачає відповідальність за порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер. Так, відповідно до ст. 163 КК України порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер. Таким чином потреба у правовому захисті прав громадян на таємницю спілкування з часом тільки зростає та вимагає нових правових механізмів, які б враховували сучасний стан розвитку телекомунікаційної сфери [123, с. 59].

Питання щодо системи процесуальних дій в ході яких обмежується таємниця спілкування не знайшло свого достатнього висвітлення в науковій літературі. У більшості випадків обмеження таємниці спілкування зводиться до НСРД пов'язаних із втручанням у приватне спілкування. Однак, перелік таких випадків набагато ширший.

Як слушно вказує С. Грібов не зрозуміло, чому НСРД, під час яких цілком може мати місце втручання у приватне спілкування, не належать до цієї категорії. Зазначене, зокрема, стосується візуального спостереження за особою, річчю або місцем, аудіо-, відеоконтролю місця. Окремі науковці, досліджуючи питання втручання в приватне спілкування, пропонують доповнити цей інститут НСРД, що матиме назву «безпосереднє спостереження та технічне документування юридично значущих фактів», до якої належатимуть НСРД, передбачені ст. 260, 269 та 279 КПК України. Аналіз змісту НСРД, передбачених ст. 271, 272 КПК України, як за матеріалами практики, так і згідно з положеннями наукових праць, дає підстави стверджувати, що вони пов'язані втручанням у приватне спілкування. Ці дії передбачають участь у конфіденційному спілкуванні інших людей особи, яка без їх відома збирає щодо них інформацію, зокрема

таку, що стосується їхнього особистого життя. Сторони спілкування при цьому розраховують на збереження в таємниці змісту спілкування, будучи введеними в оману з використанням неправдивих відомостей – дезінформації [74, с. 244 -245].

Варто погодитися з думкою, що втручання в спілкування може відбуватися не лише під час проведення негласних слідчих (розшукових) дій, перелік яких визначено в ст. 258 КПК України, а й під час інших слідчих дій, у тому числі гласних [110].

Таким чином, можна виокремити наступну систему процесуальних дій, спрямованих на обмеження таємниці спілкування.

Зокрема, на підставі ухвали слідчого судді суду першої інстанції проводяться наступні процесуальні дії спрямовані на обмеження таємниці спілкування:

- тимчасовий доступ до речей та документів;
- обшук.

На підставі ухвали слідчого судді апеляційного суду, слідчого судді Вищого антикорупційного суду проводяться такі негласні слідчі (розшукові) дії:

– аудіо-, відеоконтроль особи;

- накладення арешту на кореспонденцію, огляд і виїмка кореспонденції;
- зняття інформації з транспортних телекомунікаційних мереж;
- зняття інформації з електронних інформаційних систем;
- спостереження за особою;
- аудіо-, відеоконтроль місця.

Неоднозначним залишається питання щодо того чи може таємниця спілкування обмежуватися в ході проведення обстеження публічно недоступних місць, житла чи іншого володіння особи. Згідно ч. 1 ст. 267 КПК слідчий має право обстежити публічно недоступні місця, житло чи інше володіння особи шляхом таємного проникнення в них, у тому числі з

використанням технічних засобів.

Відповідно до п.п. 1.11.7 Інструкції обстеження публічно недоступних місць, житла чи іншого володіння особи полягає в таємному проникненні слідчого чи уповноваженої особи без відома власника чи володільця, приховано, під псевдонімом або із застосуванням технічних засобів у приміщення та інше володіння для встановлення технічних засобів аудіо-, відео контролю особи або безпосередньо з метою виявлення і фіксації слідів злочину, проведення огляду, виявлення документів, речей, що мають значення для досудового розслідування, виготовлення копій чи їх зразків, виявлення осіб, які розшукуються, або з іншою метою для досягнення цілей кримінального провадження.

На законодавчому рівні право на проведення негласного обстеження житла особи надано слідчому або в порядку ст.ст. 41, 246 КПК України за його письмовим дорученням оперативному підрозділу. Так, у випадку, коли під час досудового розслідування слідчий або прокурор встановили, що іншим шляхом, окрім проведення негласного проникнення до житла особи, досягнути вищевказаної мети неможливо, прокурор або слідчий вносить клопотання, оформлене відповідно до вимог ч. 2 ст. 248 КПК України, та узгоджене з прокурором до слідчого судді про надання дозволу на проведення обстеження публічного недоступного місця, житла чи іншого володіння особи, до якого додається витяг з Єдиного реєстру досудових розслідувань щодо кримінального провадження, у рамках якого подається клопотання. Після отримання ухвали суду про надання дозволу про проведення негласного обстеження житла особи слідчий може прийняти рішення про залучення до проведення вказаної НСРД експерта, осіб, які співпрацюють з правоохоронними органами на конфіденційних засадах, а також використання спеціальних технічних засобів. Після чого негласно, тобто приховано від осіб, що є власниками житла, користувачами або розпорядниками, а також їх близького оточення безпосередньо здійснюється негласне проникнення до житла особи. Однак, слід зазначити, що виявлені в

ході негласного проникнення предмети, документи не вилучаються, оскільки законодавчо закріплено, що в межах проведення цієї негласної слідчої (розшукової) дії сліди вчинення тяжкого або особливо тяжкого злочину фіксуються шляхом фото -, відеозйомки, виготовлення відтисків, відбитків, зліпків тощо [118, с. 268].

Метою зазначеної НСРД відповідно до наведених вище положень КПК та Інструкції є:

а) виявлення і фіксація слідів вчинення тяжкого або особливо тяжкого злочину, речей і документів, що мають значення для їх досудового розслідування;

б) виготовлення копій чи зразків зазначених речей і документів;

в) виявлення та вилучення зразків для дослідження під час досудового розслідування тяжкого або особливо тяжкого злочину;

г) виявлення осіб, які розшукуються;

д) встановлення технічних засобів аудіо-, відео контролю особи.

Таким чином, обстеження включає в себе дії, які дозволяють зібрати відомості, речі і документи, що мають значення для досудового розслідування або дії, без проведення яких є неможливим проведення аудіо-, відеоконтролю особи всередині публічно недоступних місць, житла чи іншого володіння особи або негласно отримати зразки для порівняльного дослідження.

Так, Н. Гольдберг проникненням у житло чи інше володіння особи вважає входження чи вторгнення в житло фізично чи з використанням різного роду технічних пристроїв чи інше володіння особи, здійснене всупереч волі особи, що в ньому проживає чи ним користується на законних підставах, а також порушення таємниці її приватного та сімейного життя, листування та телефонних розмов у житлі чи іншому володінні, здійснене поза межами житла чи іншого володіння особи, за відсутності визначених законом підстав чи в порушення встановленого законом порядку [71, с. 51]. З таким визначенням, важко погодитися, оскільки обстеження публічно

недоступних місць, житла чи іншого володіння особи полягає саме в таємному проникненні на законних підставах, а отже не у всіх випадках проникнення є незаконним.

Враховуючи наведене, вважаємо, що в ході обстеження публічно недоступних місць, житла чи іншого володіння особи слідчий, працівники оперативних підрозділів не мають права втручатися у таємницю спілкування, зокрема у особисте листування особи, інші форми спілкування зафіксовані на матеріальних чи електронних носіях, які знаходяться в публічно недоступних місць, житлі чи іншому володіння особи. Така позиція зумовлено змістом даної НСРД, яка в основному носить організаційно-допоміжний характер.

Розглянемо процесуальний порядок отримання дозволу для обмеження таємниці спілкування. У випадку необхідності проведення НСРД спрямованих на обмеження таємниці спілкування (аудіо-, відеоконтролю особи, накладення арешту на кореспонденцію, огляду і виїмки кореспонденції, зняття інформації з транспортних телекомунікаційних мереж, зняття інформації з електронних інформаційних систем, обстеження публічно недоступних місць, житла чи іншого володіння особи, спостереження за особою, аудіо-, відеоконтролю місця) слідчий за погодженням з прокурором або прокурор звертаються з клопотанням до слідчого судді про надання дозволу на проведення зазначених НСРД.

Клопотання слідчого, прокурора слідчому судді про дозвіл на проведення НСРД повинне відповідати вимогам, зазначеним у ст. 248 КПК України, та матеріалам кримінального провадження, які надаються лише на вимогу слідчого судді для підтвердження необхідності проведення НСРД. Зокрема, відповідно до ст. 248 КПК у клопотанні зазначаються: 1) найменування кримінального провадження та його реєстраційний номер; 2) короткий виклад обставин кримінального правопорушення, у зв’язку з розслідуванням якого подається клопотання; 3) правова кваліфікація кримінального правопорушення із зазначенням статті (частини статті) КК; 4) відомості про особу (осіб), місце або річ, щодо яких необхідно провести

НСРД; 5) обставини, що дають підстави підозрювати особу у вчиненні кримінального правопорушення; 6) вид НСРД та обґрунтування строку її проведення; 7) обґрунтування неможливості отримання відомостей про злочин та особу, яка його вчинила, в інший спосіб; 8) відомості залежно від виду НСРД про ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, телекомунікаційну мережу, кінцеве обладнання тощо; 9) обґрунтування можливості отримання під час проведення НСРД доказів, які самостійно або в сукупності з іншими доказами можуть мати суттєве значення для з'ясування обставин кримінального правопорушення або встановлення осіб, які його вчинили.

До клопотання слідчого, прокурора додається витяг з ЄРДР щодо кримінального провадження, у рамках якого подається клопотання. У клопотанні слідчого, прокурора, не зазначається уповноважений оперативний підрозділ, який має виконувати НСРД. У разі прийняття рішення про проведення НСРД, у ході якої необхідно провести іншу НСРД, яка вимагає постановлення ухвали слідчого судді, слідчий, прокурор звертається до нього з клопотанням у загальному порядку, передбаченому ст.248 КПК.

Розгляд та погодження прокурором клопотання слідчого про надання дозволу на проведення НСРД здійснюється невідкладно з моменту надходження. Прокурором вивчаються матеріали кримінального провадження, які є підставою для прийняття рішення про погодження клопотання. Відмова в погодженні клопотання приймається у формі постанови і не виключає повторного звернення слідчого після отримання додаткових доказів або усунення недоліків, вказаних прокурором у рішенні. У випадку відмови прокурора в погодженні клопотання слідчого до слідчого судді про проведення НСРД слідчий має право звернутися до керівника органу досудового розслідування, який після вивчення клопотання, за необхідності, ініціює розгляд питань, порушених у ньому, перед прокурором вищого рівня, який протягом трьох днів погоджує відповідне клопотання або відмовляє в його погодженні (ст. 40 КПК).

За результатами аналізу судової практики розгляду клопотань про дозвіл на проведення НСРД [134] можна виділити такі недоліки щодо змісту клопотання:

1) у більшості клопотань не зазначається номер та дата внесення відомостей про кримінальне провадження до ЄРДР, а також правова кваліфікація із зазначенням частини та статті КК;

2) у клопотанні не міститься достатньої інформації щодо необхідності проведення саме такого виду НСРД. В основному зазначаються загальні підстави, не обґрунтовується неможливість отримання відомостей про злочин та особу, яка його вчинила, в інший спосіб;

3) обставини, що дають підстави підозрювати особу у вчиненні злочину, майже в усіх клопотаннях зазначаються одні і ті ж – рапорт та оперативні матеріали або протокол допиту потерпілого;

4) у клопотанні зазначені неповні відомості про особу (осіб), місце або річ, щодо яких необхідно провести НСРД, а також обставини, що дають підстави підозрювати конкретну особу у вчиненні злочину;

5) не надаються відомості про ідентифікаційні ознаки, які дозволяють унікально ідентифікувати абонента спостереження, телекомунікаційну мережу, кінцеве обладнання;

6) відсутні обґрунтування можливості отримання під час проведення НСРД доказів, які самостійно або у сукупності з іншими доказами можуть мати суттєве значення для з’ясування обставин злочину або встановлення осіб, які його вчинили;

7) у більшості клопотань суб’єктами звернення не обґрунтовується строк проведення НСРД, інколи строк зазначається поза межами, визначеними КПК.

Рішення про надання дозволу на проведення НСРД надає слідчий суддя. Потенціал слідчого судді зумовлюється такими чинниками: 1) організаційною, матеріальною та процесуальною самостійністю від інших органів державної влади, від сторін провадження, відтак він не відповідає за

стан боротьби зі злочинністю; 2) він здійснює свої повноваженні постійно, адже обирається на тривалий строк (згідно ч.5 ст.21 Закону України «Про судоустрій і статус суддів» – на строк не більше трьох років з можливістю повторного переобрання), чим забезпечується його висока фаховість та значний досвід здійснення судового контролю; 3) здійснення ним повноважень із судового контролю враховується при розподілі судових справ та має пріоритетне значення (ч.5 ст.21 Закону України «Про судоустрій і статус суддів»), а тому він володіє також і часовим ресурсом, що позитивно впливає на якість судового контролю; 4) згідно ч.1 ст.76 КПК, якщо він брав участь у кримінальному провадженні під час досудового розслідування, він не має права брати участі у цьому ж провадженні у суді будь-якої інстанції, а тому у майбутньому не буде у будь-який спосіб зобов'язаний власними рішеннями, що робить його незалежнішим та дозволяє якомога якісніше здійснювати свої повноваження; 5) саме суд є авторитетом, покликаним вирішувати різноманітні правові спори, тому його остаточне рішення, як нейтрального арбітра, повинно задовольнити як органи держави [187, с. 255 - 256].

Слідчий суддя постановляє ухвалу про дозвіл на проведення НСРД, якщо прокурор, слідчий доведе наявність достатніх підстав вважати, що: 1) вчинений кримінальне правопорушення відповідної тяжкості; 2) під час проведення НСРД можуть бути отримані докази, які самостійно або в сукупності з іншими доказами можуть мати суттєве значення для з'ясування обставин злочину або встановлення осіб, які вчинили кримінальне правопорушення.

Як вірно зазначає О.Г. Шило, правове значення цих положень закону полягає в тому, що вони визначають межі здійснення дискреційних повноважень за колом осіб та у часі, що є суттєвою гарантією забезпечення конституційних прав як самого підозрюваного, обвинуваченого, так і інших осіб, які, спілкуючись з ним у той чи інший спосіб, обґрунтовано розраховують на приватність такого спілкування [183, с. 445].

Ухвала слідчого судді про дозвіл на проведення НСРД повинна відповідати загальним вимогам до судових рішень, передбачених КПК (зокрема, ст. 372), а також містити відомості про: 1) прокурора, слідчого, який звернувся з клопотанням; 2) кримінальне правопорушення, у зв'язку із досудовим розслідуванням якого постановляється ухвала; 3) особу (осіб), місце або річ, щодо яких необхідно провести НСРД; 4) вид НСРД та відомості залежно від виду негласної слідчої дії про ідентифікаційні ознаки, які дозволять унікальне ідентифікувати абонента спостереження, телекомунікаційну мережу, кінцеве обладнання тощо; 5) строк дії ухвали.

Як зазначає В.М. Юрчишин крім основного призначення судового контролю – захисту прав, свобод і законних інтересів людини та громадянина, він також сприяє ефективному розслідуванню кримінальних правопорушень і забезпеченню оптимальних умов для відправлення правосуддя. Остання мета найбільше характеризує основне призначення і сутність судового контролю у досудовому розслідуванні. Дане концептуальне положення не тільки вказує на контрольний характер судової діяльності у досудовому розслідуванні, але й на взаємозв'язок останньої з подальшим судовим розглядом [188, с. 244].

Ухвала слідчого судді щодо відмови в наданні дозволу на проведення НСРД не оскаржується. Постановлення слідчим суддею ухвали про відмову в наданні дозволу на проведення НСРД не перешкоджає повторному зверненню з новим клопотанням про надання такого дозволу.

Варто зауважити, що ухвала слідчого суддя про дозвіл на проведення НСРД, які обмежують таємницю спілкування, обов'язково має бути розсекречена та долучена до матеріалів кримінального провадження, оскільки відсутність ухвали слідчого судді про дозвіл на проведення негласних слідчих (розшукових) дій унеможливлює використання їх результатів у доказуванні.

Так, Колегія суддів Касаційного кримінального суду у своїй ухвалі про направлення кримінального провадження на розгляд Великої Палати

Верховного Суду висловила бажання відійти від правового висновку, викладеного у постанові ВСУ від 16 березня 2017 р. [133]. Згідно з цим правовим висновком невідкриття матеріалів сторонами одна одній в порядку ст. 290 КПК після закінчення досудового розслідування, а також додаткових матеріалів, отриманих до або під час судового розгляду, є підставою для визнання судом відомостей, що містяться в них, недопустимими як доказ.

Колегія суддів Касаційного кримінального суду сформулювала свій правовий висновок про те, що процесуальні документи, які стали правовою підставою для проведення негласних слідчих (розшукових) дій (ухвали, постанови, клопотання), що не були відкриті стороні захисту на момент звернення до суду з обвинувальним актом, оскільки вони не були у розпорядженні сторони обвинувачення – за наявності відповідного клопотання, можуть бути відкриті під час судового розгляду у суді першої чи апеляційної інстанції. Таке відкриття на цих стадіях кримінального провадження процесуальних документів, які стали правовою підставою для проведення негласних слідчих (розшукових) дій, не тягне за собою за вказаних обставин визнання відомостей, які містяться у них, та результатів проведення таких дій недопустимими доказами відповідно до ст. 290 КПК.

Велика Палата Верховного Суду вважає, що для доведення допустимості результатів НСРД мають бути відкриті не тільки результати цих дій, а й документи, які стали правовою підставою їх проведення (клопотання слідчого, прокурора, їх постанови, доручення, ухвала слідчого судді), оскільки змістом цих документів сторони можуть перевірити дотримання вимог кримінального процесуального закону стосовно негласних слідчих (розшукових) дій.

Документи, які стали правовою підставою проведення НСРД (зокрема, не розсекречені на момент звернення до суду з обвинувальним актом), не можуть вважатися додатковими матеріалами до результатів проведених негласних слідчих (розшукових) дій, отриманими до або під час судового розгляду, оскільки є їх частиною.

Ці процесуальні рішення виступають правовою підставою проведення НСРД, з огляду на їх функціональне призначення щодо підтвердження допустимості доказової інформації, отриманої за результатами проведення таких дій, і повинні перевірятися та враховуватися судом під час оцінки доказів.

Що стосується процесуальних документів, які мають гриф секретності, то за змістом статей 85, 92, 290 КПК прокурор - процесуальний керівник зобов'язаний під час досудового розслідування заздалегідь ініціювати процедуру їх розсекречення одночасно с результатами НСРД і забезпечити відкриття цих документів на етапі закінчення досудового розслідування.

За наявності відповідного клопотання процесуальні документи, які стали підставою для проведення НСРД (ухвали, постанови, клопотання) і яких не було відкрито стороні захисту в порядку, передбаченому ст. 290 КПК, оскільки їх тоді не було у розпорядженні сторони обвинувачення (процесуальні документи не було розсекречено на момент відкриття стороною обвинувачення матеріалів кримінального провадження), можуть бути відкриті іншій стороні, але суд не має допустити відомості, що містяться в цих матеріалах кримінального провадження, як докази [131].

В іншій справі Велика Палата Верховного Суду зробила висновок, що процесуальні документи, які стали підставою для проведення НСРД (ухвали, постанови, клопотання) та які на стадії досудового розслідування не було відкрито стороні захисту в порядку, передбаченому ст. 290 КПК з тієї причини, що їх не було у розпорядженні сторони обвинувачення (процесуальні документи не були розсекречені на момент відкриття стороною обвинувачення матеріалів кримінального провадження), можуть бути відкриті іншій стороні під час розгляду справи у суді за умови своєчасного вжиття прокурором всіх необхідних заходів для їх отримання. Якщо сторона обвинувачення не вжила необхідних та своєчасних заходів, що спрямовані на розсекречення процесуальних документів, які стали процесуальною підставою для проведення НСРД і яких немає в її

розпорядженні, то в такому випадку має місце порушення норм ст. 290 КПК [130].

Безпосередній порядок проведення негласних слідчих (розшукових) дій закріплений у розділі третьому Інструкції. Право безпосередньо проводити НСРД має слідчий або уповноважений ним оперативний підрозділ. У зв'язку із складністю проведення більшості НСРД, необхідністю використання спеціальної техніки, слідчий як правило не проводить таких дій, а доручає їх проведення відповідним оперативним підрозділам. Інструкцією визначено безпосередній порядок надання таких доручень.

Слідчий, прокурор надсилає доручення керівнику органу, під юрисдикцією якого знаходиться місце вчинення кримінального правопорушення і у складі якого знаходяться орган розслідування та/або оперативні підрозділи, уповноважені на проведення НСРД. Залежно від злочину, який розслідується, та статусу особи, щодо якої проводиться НСРД, інших чинників слідчий, за погодженням з керівником органу досудового розслідування відповідного рівня, може доручати проведення НСРД керівнику іншого правоохоронного органу, у тому числі того, під юрисдикцією якого не знаходиться місце вчинення кримінального правопорушення, з обґрунтуванням такої необхідності.

До доручення слідчого, прокурора додається ухвала слідчого судді про дозвіл на проведення НСРД чи постанова слідчого, прокурора про проведення НСРД. Доручення складається у двох примірниках на офіційному бланку органу досудового розслідування чи прокуратури відповідного рівня. Доручення повинно бути вмотивованим, містити інформацію, яка необхідна для його виконання, чітко поставлене завдання, що підлягає вирішенню, строки його виконання, визначати конкретного прокурора, якому слід направляти матеріали. Оперативний підрозділ не має права передоручати виконання доручення іншим оперативним підрозділам. У дорученні також може визначатись порядок взаємодії між слідчим, прокурором і

уповноваженим оперативним підрозділом, а також терміни складання протоколів про хід і результати проведеної НСРД або її проміжного етапу.

Керівник органу відповідно до відомчих нормативно-правових актів визначає виконавця – оперативний підрозділ (оперативні підрозділи). Прокурор має право заборонити проведення ще не розпочатої НСРД, оформивши своє рішення вмотивованою постановою. Прокурор зобов'язаний припинити подальше проведення НСРД, якщо в цьому відпала необхідність, та з інших підстав, викладених ним у постанові, що негайно надається керівнику органу, який проводить НСРД за дорученням слідчого, прокурора, або слідчому, який проводить зазначені дії безпосередньо.

Уповноважений оперативний підрозділ для виконання доручення слідчого, прокурора з урахуванням необхідності забезпечення умов для проведення НСРД залучає на підставі свого завдання відповідні оперативні та оперативно-технічні підрозділи. Уповноважені оперативні підрозділи не мають права виходити за межі доручень слідчого, прокурора. Вони зобов'язані повідомляти їх про виявлення обставин, які мають значення для кримінального провадження або вимагають нових процесуальних рішень слідчого, прокурора.

Керівник органу, якому доручено виконання НСРД, повинен негайно повідомити прокурора та слідчого про неможливість виконання доручення, його затримку з обґрунтуванням причини і повідомленням про вжиття заходів до подолання перешкод у виконанні доручення. Контроль за дотриманням строків і повноти виконання доручення слідчого, прокурора здійснюється начальником уповноваженого оперативного підрозділу. За результатами виконання доручення оперативний співробітник складає рапорт із зазначенням результатів виконаного доручення, залучених при цьому сил і засобів, а також їх результатів. Керівник уповноваженого оперативного підрозділу приймає рішення шляхом накладення резолюції на рапорті стосовно можливості направлення протоколу та додатків до нього прокурору чи вжиття заходів до належного виконання доручення. Протокол та додатки

до нього не пізніше 24 годин після складання надаються прокурору, зазначеному в дорученні.

Неодноразово у практичній діяльності та науковій літературі виникає питання про можливі порушення прав людини оперативними підрозділами під час проведення НСРД у зв’язку з відсутністю належного судового контролю та прокурорського нагляду в ході їх здійснення.

Виходом з цієї ситуації є залучення особи, яка під час судового розгляду клопотань про НСРД буде забезпечувати дотримання прав осіб щодо яких будуть застосовуватися обмеження. В зв’язку з цим, пропонуємо викласти ч. 1 ст. 261 КПК в наступній редакції «Слідчий суддя зобов'язаний розглянути клопотання про надання дозволу на проведення негласної слідчої (розшукової) дії протягом шести годин з моменту його отримання. Розгляд клопотання здійснюється за участю особи, яка подала клопотання та адвоката делегованого центром безоплатної правової допомоги». Такий адвокат, повинен мати допуск до державної таємниці, а доступ до матеріалів клопотання про надання дозволу на проведення НСРД буде надаватися слідчим суддею перед його судовим розглядом.

Запровадження такого інституту звісно може викликати низку заперечень з боку сторони обвинувачення щодо можливого затягування строку розгляду клопотань. Водночас, запровадження такої гарантії буде спростовувати подальші заперечення щодо порушення прав осіб під час надання дозволу на проведення негласної слідчої (розшукової) дії.

2.2. Обмеження таємниці спілкування в ході проведення тимчасового доступу до речей та документів

Тимчасовий доступ до речей і документів полягає у наданні стороні кримінального провадження особою, у володінні якої знаходяться такі речі і документи, можливості ознайомитися з ними, зробити їх копії та вилучити їх (здійснити їх виїмку).

Як вірно зазначає В. Рогальська, для звернення із клопотанням до слідчого судді, суду про тимчасовий доступ до речей і документів буде достатньо розумної підозри слідчого про можливість змінити або знищити речі чи документи особою, у володінні якої вони перебувають, або інформації, що речі та документи містять відомості, які становлять охоронювану законом таємницю [144, с. 130].

Отримання інформації, що містить таємницю спілкування від операторів телекомунікацій для використання її у цілях кримінального провадження давно широко застосовується у міжнародній практиці. Так, у п. 1.4.-1.5. Резолюції Ради Європейського союзу «Про законне перехоплення телекомунікацій» передбачено, що правоохоронні органи вимагають доступу до інформації про зв'язок, такої як:

- сигнал про стан готовності доступу;
- для вихідного з'єднання - номер сторони, з якою зв'язуються, навіть якщо зв'язок не було встановлено;
- для вхідного з'єднання - номер сторони, яка зв'язується, навіть якщо зв'язок не було встановлено;
- усі сигнали, що були видані об'єктом цілі, включаючи сигнали після з'єднання, видані для активації функцій, таких як конференц-зв'язок та передача зв'язку;
- початок, кінець та тривалість з'єднання;
- фактичне місце призначення та проміжний абонентський номер у разі, якщо зв'язок був переадресований;

- інформацію щодо якомога точнішого географічного місцезнаходження, відомого для мережі для мобільних абонентів [141].

В подальшому аналогічний перелік був дещо уточнений і закріплений у Резолюції Ради Європейського союзу «Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг»(ENFOPOL). Крім того у ній було закріплено право правоохоронних органів вимагати від операторів мережі/постачальників послуг здійснювати перехоплення якомога оперативніше (в термінових випадках протягом декількох годин чи хвилин) [142].

На підставі аналізу ст. 162 КПК України можна виокремити дві групи даних, які можна отримати під час тимчасового доступу до речей та документів, які становлять таємницю спілкування. До них зокрема належать особисте листування особи та інші записи особистого характеру та інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо [157, с. 225].

Щодо першої групи інформації потрібно відзначити юридичну колізію у застосуванні двох інститутів доступу до інформації, що містить таємницю листування. Зокрема доступ до неї можливий або в режимі тимчасового доступу до речей і документів або в режимі негласної слідчої дії – зняття інформації з електронних інформаційних систем. У практичній діяльності органів досудового розслідування можна зустріти домінуючий підхід отримання такої інформації в режимі тимчасового доступу. Так, ухвалою слідчого судді Галицького районного суду м. Львова було надано тимчасовий доступ до інформації та відомостей, які знаходяться на персональному комп'ютері (ноутбуку) та мобільному телефоні Samsung *(вказані телефон і комп'ютер вилучені слідчим під час обшуку)*, а саме: особистої переписки (листування) через відповідні програми та застосунки, спілкування через

відповідні застосунки, фото та відеозаписів які використовувались Г. під час здійснення переписки (листування) у відповідних програмах та застосунках, що можуть підтвердити або спростувати факт його спілкування із відправником поштового відправлення CV350548950CA або іншими особами, яким відомі або можуть бути відомі обставини вчинення вищевказаного кримінального правопорушення, із можливістю ознайомитися з інформацією та зробити її копії [170].

Аналогічне рішення прийнято у справі № 461/5038/19, у якій слідчий суддя надав дозвіл на тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю та знаходяться у володінні СУ ГУНП у Львівській області при матеріалах кримінального провадження № 12018140000000280 від 23.05.2018 р., за ознаками кримінального правопорушення, передбаченого ч.2 ст.364 КК України, а саме до особистого листування особи та інших засобів особистого характеру, які можуть бути використані як доказ у кримінальному провадженні та знаходяться у додатках, телефонній книзі та пам'яті електронних носіїв інформації у мобільному телефоні (смартфоні), марки «iPhone», які належать Ч. для огляду з метою виявлення, вилучення та фіксації відомостей щодо обставин вчинення кримінального правопорушення, зокрема листувань у додатках, програмах, месенджерах «Viber», «Telegram», «WhatsApp», у яких наявні листування із абонентами [171]. Такі ж рішення приймалися і у інших справа судів м. Львова [170;172;173].

У інших справах суди уточнюють, яку саме інформацію може отримати слідчий під час тимчасового доступу. Так, у справі №199/677/18 слідчому було надано, тимчасовий доступ до речі, яка містить охоронювану законом таємницю (відомості про особисте листування та інші записи особистого характеру), які зберігаються в мобільних телефонах - марки «Iphon 6» та марки «Iphon 5s», вилучених 30.01.2018 у ході обшуку службового кабінету начальника відділу Індустріального районного відділу у м. Дніпро ГУ ДМС України в Дніпропетровській області, з можливістю ознайомлення з ними та

зняти їх копії, а саме:

- відомостей щодо телефонного довідника (довідника контактів), вхідних та вихідних дзвінків, вхідних та вихідних повідомлень, які охоплюють період з 14 грудня 2017 року по 30 січня 2018 року включно і стосуються зв’язків та/або листування між К. та Б.
- листування з використанням електронної пошти за період з 14 грудня 2017 року по 30 січня 2018 року включно і стосуються зв’язків та/або листування між К. та Б.;
- змісту спілкування (листування) в програмному забезпеченні, що встановлене (було встановлене) в телефоні та забезпечує (забезпечувало) можливість передачі даних (Skype, Viber, WhatsApp, Telegram та інші) за період з 14 грудня 2017 року по 30 січня 2018 року включно і стосуються зв’язків та/або листування між К. та Б .[169].

Таким чином, органи досудового розслідування отримують інформацію про таємницю спілкування осіб, яка знаходиться в електронній інформаційній системі (телефоні, комп’ютері, планшеті) шляхом тимчасового доступу до речей. Варто зауважити, що тимчасовий доступ до речей і документів полягає у наданні стороні кримінального провадження *особою, у володінні якої знаходяться такі речі і документи*, можливості ознайомитися з ними, зробити їх копії та вилучити їх (здійснити їх виїмку). Однак, у всіх наведених випадках особою, у володінні якої знаходяться речі був сам слідчий, який звертався з клопотанням про тимчасовий доступ. Водночас відповідно до ч. 3 ст. 258 КПК 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. Згідно ч. 4 цієї статті втручанням у приватне спілкування є доступ до змісту спілкування за умов, якщо учасники

спілкування мають достатні підстави вважати, що спілкування є приватним.

Категоричною є вимога ч. 1 ст. 264 КПК згідно якої пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або їх частинах, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача може здійснюватися на підставі ухвали слідчого судді, якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування.

Таким чином, виходячи із системного тлумачення вказаних норм, можна зробити висновок, що доступ до таємниці листування та інших записів особистого характеру, які знаходяться в електронній інформаційній системі можливий виключно в режимі НСРД – зняття інформації з електронних інформаційних систем. Однак, варто зауважити, що Верховним судом сформована практика отримання такої інформації під час проведення огляду речового доказу. Так, у постанові від 09 квітня 2020 року Верховний суд зазначив, що інформація, яка була наявна в мобільному телефоні Г. була досліджена шляхом включення телефону та огляду текстових повідомлень, які в ньому знаходились та доступ до яких не був пов`язаний із наданням володільцем відповідного серверу (оператором мобільного зв`язку) доступу до електронних інформаційних систем. В даному випадку орган досудового розслідування провів огляд предмета - телефону та оформив його відповідним протоколом, який складений з дотриманням вимог кримінального процесуального закону [132]. З таким підходом, важко погодитися оскільки втручання у таємницю спілкування в такий спосіб здійснюється без додержання жодних процесуальних гарантій прав особи. Крім того, такий огляд проводиться, зважаючи на необхідність використання спеціальних знань, із залученням спеціаліста, завдання якого полягає у тому, щоб виявити інформацію в електронному пристрої, що досить часто вимагає застосування спеціального програмного забезпечення (використовуються програми «UFED Physical Analyzer», «Мобільний криміналіст» та інші) [181,

с. 76].

В цьому контексті правильно зазначає А.Шило, що інформація, яка міститься на вилучених у ході процесуальних дій (обшуків, затримань) електронних пристроях (персональних комп'ютерах, ноутбуках, смартфонах, телефонах тощо), не може ототожнюватися із самим електронним пристроєм як її фізичним носієм. Така інформація є окремим об'єктом права власності й об'єктом охорони таємниці приватного життя, а отже, її вилучення/копіювання має відбуватися на підставі судового рішення, проте не в режимі застосування НСРД [182, с. 177].

В зв'язку з цим, вважаємо, що потрібно закріпити окрему слідчу дію, як різновид слідчого огляду – огляд електронної інформаційної системи. Такий огляд проводиться щодо електронних інформаційних систем, які вилучені в ході інших слідчих дій та здійснюється на підставі ухвали слідчого судді місцевого суду.

Варто зауважити, що чинне законодавство не містить визначення «електронної інформаційної системи». Відповідно до п. 1.11.6. Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні - зняття інформації з електронних інформаційних систем включає в себе отримання даних з електронно-обчислювальних машин (комп'ютерів), автоматичних систем, комп'ютерних мереж.

Як вірно зазначає В.Луцик з таким визначенням можна погодитись лише частково, оскільки одержання інформації, що міститься в комп'ютерній мережі за загальним правилом повинно охоплюватись такою НСРД, як зняття інформації з транспортних телекомунікаційних мереж. Отримання такої інформації в межах зняття інформації з електронних інформаційних систем можливе лише в тому випадку, коли жоден з елементів локальної мережі не під'єднаний до глобальної мережі [111, с. 222].

Таким чином, об'єктом слідчої (розшукової) дії *огляд електронної інформаційної системи* будуть:

- електронно-обчислювальні машини (комп'ютери, мобільні телефони, планшети, смарт-годиники, сервери);
- автоматичні системи - організаційно-технічні системи, в яких реалізується технологія обробки інформації з використанням технічних і програмних засобів [137].
- локальні комп'ютерні мережі.

Щодо другої групи інформації варто зауважити, що інформація, що зберігається в операторів та провайдерів телекомунікацій, – це відомості, що виникають під час експлуатації систем мобільного зв'язку як безпосередньо користувачем, а також в операційно-інформаційних системах і центрах комутації операторів мобільного зв'язку. Залежно від місця концентрації, інформація, що зосереджена у засобах систем мобільного зв'язку, міститься: у призначеному для користувача устаткуванні (абонентській станції, абонентському пристрої); різних файлах: текстових, звукових, фото-, відео-; в операційно-інформаційних системах і центрах комутації оператора стільникового (мобільного) зв'язку (безпосередньо в операторів) [147, с. 38].

Увесь масив інформації про абонента, що зберігається в операторів і провайдерів телекомунікацій, можна поділити на дві групи: перша – відомості стосовно наданих телекомунікаційних послуг; друга – відомості про споживача, одержані при укладанні договору. До першої групи слід віднести, зокрема: дані про з'єднання терміналів абонентів операторів мобільного зв'язку у певний час («трафіки»), з'єднання певних абонентських номерів або терміналів за певний період часу («звіти»), з'єднання невизначеного кола абонентських номерів (із зазначенням IMEI-терміналу), що відбулись у межах дії певної базової станції за певний період часу («моніторинги») тощо. Відомості про споживача, одержані при укладанні договору – це особисті дані про абонента (копія паспорта, посвідчення водія, службового посвідчення працівника органів державної влади або місцевого самоврядування тощо); реєстраційні дані документів, ідентифікаційний код; відомості стосовно адреси реєстрації, фактичного місця проживання,

контактного телефону, адреси електронної пошти тощо [63, с. 15].

С.Р.Тагієв вірно зазначає, що найчастіше, під час розслідування кримінальних правопорушень викликають інтерес такі дані, що зберігаються в операторів:

— факт отримання послуг, їхня тривалість, зміст, маршрути передавання тощо;

— за відомим номером абонента встановлення *IMEI* коду терміналу (мобільного телефону, інших пристроїв), або *IMEI* кодів всіх терміналів, якими користувався цей абонент у зазначений період часу;

— за відомим *IMEI* кодом терміналу встановлення номера абонента або всіх номерів абонентів, які користувалися цим терміналом у зазначений період часу;

— вибірка вхідних/вихідних дзвінків, *SMS, MMS* та інших повідомлень конкретного абонента у зазначений період часу;

— встановлення місця перебування (в межах соти) конкретного терміналу з прив’язкою до часу, категорії самих станцій, порядок естафетної передачі, режиму роумінгу та ін.;

— встановлення номерів ваучерів поповнення балансу абонента з метою встановлення місця придбання;

— вибірка всіх активних терміналів, які знаходилися в певному квадраті місцевості у певний час;

— встановлення номера абонента користувача Інтернету за допомогою мобільного терміналу за протоколом *gprs/edge/cdma* в разі, якщо відома його *IP* адреса і час виходу в Інтернет під нею;

— постановка на облік певного номера абонента або *IMEI* номера терміналу з подальшим повідомленням замовника у разі появи абонентів або терміналів у мережі (таймер відсутності);

— характеристика та індекс закритих груп користувачів.

Крім цього, в мережах Інтернет у провайдерів зберігаються такі дані, які становлять інтерес для слідства:

— хостинг — розміщення інформації на сервері, що постійно знаходиться у мережі;

— адреса електронної пошти (*e-mail*) — сховище, де зберігаються копії відправлених листів (поштова скринька);

— спам — інформація, отримана без бажання або всупереч бажанням власника електронної пошти;

— *UIN* — універсальний ідентифікаційний номер у парі з паролем конкретної особи для *ICQ* — служби миттєвого обміну повідомленнями в мережі Інтернет;

— сайт — *website* (місце у мережі Інтернет, сукупність електронних документів (файлів) особи (фізичної або юридичної) у мережі, що об'єднані під одними ім'ям або *IP*-адресою;

— доменне ім'я — імена різних рівнів напрямків (наприклад, *ua.svoboda.org.*);

— *IP*-адреса — мережева адреса вузла у мережі (позначається числами, наприклад, 192.186.5.112) [154, с. 103].

Звісно наведений перелік інформації є невичерпним, і в ході розслідування конкретних правопорушень може виникати потреба отримання іншої інформації.

Варто погодитися з думкою О.М. Гуміна, що для отримання доступу до інформації про зв'язок, абонента, надання телекомунікаційних послуг можливе лише за наявності закріплених у законодавстві підстав.

Вказані підстави умовно можуть бути класифіковані на:

а) загальні підстави застосування заходів забезпечення кримінального провадження (такі як: наявність обґрунтованої підозри щодо вчинення кримінального правопорушення такого ступеня тяжкості, що може бути підставою для застосування заходів забезпечення кримінального провадження; виправданість ступеню втручання у права і свободи особи потребами досудового розслідування; можливість виконання визначеного завдання);

б) спеціальні підстави застосування тимчасового доступу до речей і документів (обґрунтована підозра, що речі або документи: перебувають або можуть перебувати у володінні відповідної фізичної або юридичної особи; вказані речі або документи самі по собі або в сукупності з іншими речами і документами кримінального провадження, мають суттєве значення для встановлення важливих обставин у кримінальному провадженні);

в) додаткові підстави надання тимчасового доступу до речей і документів, які містять охоронювану законом таємницю (доведена стороною кримінального провадження можливість використання як доказів відомостей, що містяться в цих речах і документах, та неможливість іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів) [75, с. 55].

І.В.Гловюк вірно зазначає, формулювання ч.2 ст.163 КПК вимагає наявності доказів того, що є реальна загроза зміни або знищення речей чи документів; при цьому реальність загрози є оцінною категорією, що ускладнює застосування цієї норми на практиці. Як уявляється, у даній нормі закладено надто високий стандарт доказування при вирішенні питання про тимчасовий доступ до речей та документів. В зв’язку з цим, ми підтримуємо її думку, що доцільніше було б закріпити інший стандарт доказування для прийняття цього рішення – розумної підозри про можливість зміни або знищення речей чи документів, що дозволяло б приймати рішення про розгляд клопотання без виклику особи, у володінні якої знаходяться такі речі і документи, аналізуючи її статус у кримінальному провадженні або взаємовідносини із суб’єктами кримінального провадження, і не зобов’язувало б суб’єкта подання клопотання надавати достатню сукупність доказів про наявність реальної загрози [67, с. 53 -54].

До клопотання слідчий або прокурор повинен також додати:

– відомості (копії довідки оператора, провайдера, протокол допиту, слідчих дій і тощо) про ознаки, які дозволять ідентифікувати абонента шляхом уніфікації мереж (№ *SIM* карти, *IMEI*, *e-mail* тощо);

- копії інших матеріалів, які мають вагоме значення при розгляді клопотання — слідчий суддя, суд при постановленні ухвали в резолютивній частині повинен зазначати повні дані про особу, щодо якої отримується інформація (прізвище, ім'я, по батькові, місце роботи та ін.);
- повний номер *IMEI*, назву оператора, провайдера, номери мобільних станцій, № *SIM* карти, телефону з зазначенням коду держави України +38. (Наприклад +38 № *SIM*-карти телефону; точної електронної адреси на мові оригіналу, із зазначенням знаків розділу; адреси ІА; паролів *SIM*-карти;
  - номера *ICQ*; оригінальні назви сайтів; *IP*-адреси, тощо) [155, с. 21].

Проблемним на практиці є реалізація положень ч. 4 ст. 163 КПК, згідно якої слідчий суддя, суд розглядає клопотання за участю сторони кримінального провадження, яка подала клопотання, та особи, у володінні якої знаходяться речі і документи. Як слушно зауважують С. С. Чернявський, В. О. Фінагеєв зазвичай фізично неможливо виконати вимоги ст. 163 КПК України щодо судового виклику за повісткою до слідчого судді особи, у володінні якої перебувають речі та документи (представника оператора мобільного зв'язку), з огляду на відсутність у більшості регіонів держави таких представників [179, с. 182].

Також, правильною видається практика долучення до клопотання матеріалів радіотехнічної розвідки, які дозволяють додатково ідентифікувати базові станції через які здійснювали спілкування підозрювані, а отже обмежити порушення таємниці спілкування невизначеної кількості абонентів. Так, у справі № 426/14319/19 з метою встановлення координат базових станцій, які покривають місце злочину, оперативним підрозділом було проведено радіорозвідку та встановлено, що місце вчинення кримінального правопорушення покривають наступні базові станції операторів мобільного зв'язку: ПрАТ «ВФ Україна» - LAC 61171, CelliD

45323,2546; ПрАТ «ВФ Україна» - LAC 11763, CelliD 61461,61465; ПрАТ «Київстар» - LAC 62499, CelliD 4283; ТОВ «Лайфселл»: LAC 23309, CelliD 23801, 23802, 23803, 6312, 6316. На підставі оцінки наданих доказів слідчий суддя надав дозвіл на проведення тимчасового доступу та вилучення інформації у письмовому та електронному вигляді про з'єднання мобільного зв'язку за абонентами "А " та «Б» з вказівкою адрес базових станцій і азимутів прийому, використовуваних Sim-карт та № IMEI мобільних терміналів, яка знаходиться в операторів провайдерів телекомунікацій з прив'язкою до базових станцій у термін часу з 00-01 години 14 вересня 2019 року до 15-00 годину 17 вересня 2019 року, які виходили на зв'язок в зоні дії вказаних базових станцій [174].

У разі задоволення клопотання ухвала слідчого судді про надання тимчасового доступу до речей і/або документів повинна містити чітку вказівку на те:

- *хто повинен* надати тимчасовий доступ до речей і документів (із зазначенням повної та точної назви юридичної особи її юридичної адреси;

- якщо вказаний обов'язок покладено на фізичну особу, то зазначається її прізвище, ім'я та по батькові);

- *кому повинно* бути надано тимчасовий доступ до речей і документів (із зазначенням прізвища, імені, по батькові, а також посади уповноваженої особи);

- *які саме* необхідно надати документи для ознайомлення, отримання їх копій чи здійснення виїмки;

- *який строк* встановлено для застосування вказаного заходу [152, с. 512].

Варто згадати, що листом Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ № 223-559/0/4-13 від 05.04.2013 «Про деякі питання здійснення слідчим суддею суду першої інстанції судового контролю за дотриманням прав, свобод та інтересів осіб під час застосування заходів забезпечення кримінального провадження» було

закладено у практичній діяльності підхід щодо уніфікації в одній ухвалі отримання інформації про невизначену кількість абонентів. Зокрема, у цьому листі зазначено, що однорідні питання, які потрібно з'ясувати в рамках одного кримінального провадження шляхом застосування одного або різних видів заходів забезпечення, пов'язаних між собою (при цьому необхідність з'ясування таких питань обґрунтовується однаковими обставинами), можуть ініціюватися слідчим (прокурором) у рамках одного клопотання та вирішуватися слідчим суддею в одній ухвалі. Такий підхід доцільно застосовувати для розгляду клопотань про надання тимчасового доступу до документів, які знаходяться в операторів і провайдерів телекомунікацій та містять інформацію про зв`язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалість, зміст, маршрути передавання тощо

Зокрема, у разі необхідності отримання інформації у рамках одного кримінального провадження з однаковим обґрунтуванням такої потреби вважаємо доцільним об'єднання в межах одного клопотань, які стосуються отримання тимчасового доступу (можливості ознайомитися та зробити копії) до документів, що знаходяться в оператора (провайдера), за умови реальної технічної можливості операторів (провайдерів) телекомунікацій надати таку інформацію, та які містять:

1) інформацію про ідентифікаційні ознаки кінцевого обладнання телекомунікацій (абонентський номер SIM-картки, IMEI, MAC-адреса, IP-адреса тощо), яке перебувало у зоні дії певних базових станцій у певний час;

2) інформацію про прізвища, імена, по батькові та інші відомості про споживача телекомунікаційних послуг та абонентів зазначеного кінцевого обладнання телекомунікацій (за наявності таких відомостей);

3) інформацію про типи з'єднань зазначеного кінцевого обладнання телекомунікацій (вхідні та вихідні з'єднання) за певний період часу включно із зазначенням дати і часу, тривалості таких з'єднань, маршрутів передавання даних (при цьому зазначений період часу може завершуватися після

пред'явлення ухвали до виконання, тобто передбачати надання доступу - можливості постфактум ознайомитися та зробити копії - до інформації щодо з'єднань, які відбудуться у майбутньому);

4) зазначену в пунктах 1, 2, 3 інформацію щодо кінцевого обладнання телекомунікацій, з якими з'єднувалося кінцеве обладнання телекомунікацій, що перебувало у зоні дії певних базових станцій у певний час, та щодо їх наступних з'єднань;

5) іншу інформацію про телекомунікації.

З таким підходом, можна погодитися виходячи із вимог оперативності розслідування кримінальних правопорушень, але не в повній мірі в частині забезпечення прав учасників процесу. Це зумовлено тим, що отримання інформації про невизначену кількість абонентів не дає можливість викликати їх у судове засідання для захисту своїх прав.

Ураховуючи специфіку формату зберігання інформації, що передбачена п. 7 ч. 1 ст. 162 КПК України і знаходиться в операторів (провайдерів) телекомунікацій, надання доступу до відповідних документів (тобто надання можливості ознайомитися з ними та зробити з них копії), може здійснюватися як безпосередньо в оператора (провайдера), так і шляхом надану доступу до відповідних документів уповноваженому на зняття інформації з транспортних телекомунікаційних мереж підрозділу правоохоронного органу через відповідні інформаційні системи відповідно до встановленого порядку з обов’язковим наданням копії ухвали слідчого судді відповідному оператору (провайдеру) [48, с. 64].

Одержання (вилучення) інформації безпосередньо в операторів і провайдерів телекомунікацій вимагає забезпечення участі у проведенні цього заходу спеціалістів, передусім фахівців у галузі комп’ютерних технологій, засобів зв’язку або обслуговування мережі. Вилучення телекомунікаційних повідомлень здійснюється у присутності представника оператора мобільного зв’язку, понятих (бажано з числа працівників фірми-оператора). Залежно від змісту повідомлень, вони можуть бути вилучені шляхом копіювання вмісту

на магнітні носії комп’ютерної інформації (у цьому разі ще на підготовчій стадії вилучення необхідно підготувати апаратно-технічні засоби для зчитування і збереження інформації, що вилучається, перелік яких слід попередньо узгодити із спеціалістом, а також переносні накопичувальні пристрої [179, с. 183].

Таким чином, вважаємо, що шляхом тимчасового доступу до речей документів які знаходяться в операторів та провайдерів телекомунікацій може отримуватися лише інформація про зв’язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання, яка за своїм змістом охороняється таємницею спілкування.

2.3. Обмеження таємниці спілкування в ході проведення аудіо-, відеоконтролю особи та місця.

Особисте спілкування осіб, в тому числі, не тільки підозрюваних, але й інших осіб, які часто не є учасниками кримінального провадження, дуже часто стає предметом негласної слідчої (розшукової) дії - аудіо-, відеоконтролю особи. За своїм змістом дана НСРД є різновидом втручання у приватне спілкування, яке проводиться без відома особи на підставі ухвали слідчого судді, якщо є достатні підстави вважати, що розмови цієї особи або інші звуки, рухи, дії, пов’язані з її діяльністю або місцем перебування тощо, можуть містити відомості, які мають значення для досудового розслідування.

Відповідно до п. 1.11.2. Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні - аудіо-, відеоконтроль особи полягає в негласній (без відома особи) фіксації та обробці із використанням технічних засобів розмови цієї особи або інших звуків, рухів, дій, пов'язаних з її діяльністю або місцем перебування тощо.

Негласні слідчі дії з аудіоконтролю проводяться за допомогою спеціальних технічних засобів фіксації інформації. Однією з особливостей аудіоконтролю є те, що він може бути епізодичним, тобто на необхідний проміжок часу, однак, як правило, аудіоконтроль особи здійснюється цілодобово, тому що особа, яка може бути причетна до протиправних дій, може в будь-який момент часу надати чи спробувати передати іншим особам інформацію, яка може мати значення для кримінального провадження.

Метою відеоконтролю є візуальне негласне спостереження за діями особи (шляхом відеозапису та аудіофіксації) у будь-якому місці його перебування для отримання інформації, яка має значення для досудового розслідування. Відеоконтроль проводиться шляхом негласного візуального спостереження за діями особи, його розмовами, поведінкою спеціальними підрозділами за допомогою спеціальних технічних засобів. Відеоконтроль може здійснюватися в будь-якому місці перебування особи, зокрема в житлі

або в іншому володінні особи, у приміщеннях, транспортних засобах та інших місцях. Відеозапис дозволяє більш детально зібрати необхідну інформацію, ретельно вивчити дії заінтересованих осіб, отримати повну інформацію, що стосується діяльності підозрюваної або обвинуваченої особи у вчиненні кримінального правопорушення [109, с. 337].

Як вірно зазначає М.Л. Грібов відповідна НСРД передбачає фіксацію (за допомогою аудіо- та/або відеотехніки) дій особи незалежно від її місця перебування: у квартирі, офісі, особистому чи громадському транспорті, на вулиці. Водночас технічно досягти цього неможливо. Аудіо-, відеоконтроль особи можливий лише в конкретному приміщенні або транспортному засобі, де ймовірно буде перебувати особа, щодо якої проводять НСРД. Аудіо-, відеоконтроль у приміщенні проводять не лише тоді, коли особа, яка є об'єктом НСРД, перебуває там сама, а й коли до неї долучаються інші особи чи коли вона відсутня, а в приміщенні (транспортному засобі) перебувають люди, які не є об'єктами НСРД [74, с. 239].

Цікавим у практичній діяльності був наступний випадок. Слідчим управлінням ГУНП у Львівській області проводилося досудове розслідування у кримінальному провадженні за фактами надання, вимагання та одержання неправомірної вигоди за ч. 3 ст. 368, ч. 3 ст. 369 КК України.

З матеріалів, які стали підставою для початку досудового розслідування вбачалося, що керівник одного із комунальних підприємств Львівської області вимагав у представника комерційної структури неправомірну вигоду за надання переваг під час проведення комунальним підприємством тендерної закупівлі техніки та подальшого укладення договору її поставки, на що представник комерційної структури погодився, із заявою про вчинення злочину не звертався.

Під час проведення досудового розслідування проводився великий обсяг негласних слідчих (розшукових) дій, а саме, передбачених ст.ст. 260, 263, 267, 269 КПК України. В тому числі було встановлено техніку для проведення аудіо-, відео-контролю особи (чотири стаціонари) в службових

кабінетах комунального підприємства, а також комерційної структури. Документувалися неправомірні дії як керівника комунального підприємства, який вимагав неправомірну вигоду так і двох працівників комерційної структури, які погодилися її надати.

В подальшому, під час проведення обшуку грошових коштів, які надавались в якості неправомірної вигоди відшукано та вилучено не було, відтак не було повідомлено про підозри особам за ст. 368, 369 КК України.

Однак завдяки проведеним НСРД було задокументовано факт домовленості між керівником комунального підприємства та представниками комерційних структур, яка полягала у свідомому створенні тендерних умов під учасника тендеру (фірми підконтрольної фігурантам кримінального провадження), штучному завищенні вартості одиниць техніки, при чому було проговорено суми завищення вартості кожної із поставлених одиниць техніки. Вилученими документами вказані обставини були підтверджені, а також було встановлено матеріальну шкоду, завдану внаслідок завищення поставленої техніки на суму понад 1,5 млн. грн., яка була підтверджена проведеними судовими експертизами.

Відтак було розпочато досудове розслідування за фактом розтрати бюджетних коштів в особливо великих розмірах, вчинених організованою групою за ч. 5 ст. 191 КК України.

В рамках досудового розслідування, з метою використання результатів проведення негласних слідчих (розшукових) дій у кримінальному провадженні розпочатому за ч. 5 ст. 191 КК України, прокурор в порядку ст. 257 КПК України звернувся до слідчого судді апеляційного суду із клопотанням про надання такого дозволу, яке слідчим суддею було задоволено.

За результатами досудового розслідування, яке тривало 8 місяців до суду було скеровано обвинувальний акт відносно 4 осіб про вчинення кримінальних правопорушень, передбачених ч. 5 ст. 191 КК України (розтрата бюджетних коштів в особливо великих розмірах, вчинена

організованою групою) та ч. 1 ст. 366 КК України (службове підроблення) [100].

Проведенню аудіо-, відеоконтролю особи в середині публічно недоступних місць, житла чи іншого володіння особи передує їх обстеження, в результаті таємного проникнення до яких встановлюються технічні засоби аудіо-, відеоконтролю (п. 5 ч. 1 ст. 267 КПК). Тому в разі отримання слідчим, прокурором фактичних даних, що розмови конкретної особи або інші звуки, рухи, дії, пов'язані з її діяльністю та перебуванням в середині публічно недоступних місць, житла чи іншого володіння особи, можуть містити відомості, які мають значення для досудового розслідування, та за неможливості отримати ці відомості іншим шляхом окрім як проведенням даної негласної слідчої (розшукової) дії, слідчий (прокурор) складає окремі клопотання, узгодженні з прокурором, до слідчого судді про дозвіл на проведення обстеження публічно недоступних місць, житла чи іншого володіння особи для встановлення технічних засобів аудіо-, відеоконтролю особи та про дозвіл на проведення аудіо-, відеоконтролю особи в середині цих місць [122, с. 37].

В зв'язку з цим, не можна погодитися з думкою В.А. Колесника, який вважає, що якщо негласну слідчу (розшукову) дію, передбачену ст. 267 КПК, проводять для встановлення технічних засобів аудіо-, відеоконтролю особи в публічно недоступних місцях, житлі чи іншому її володінні, то отримання окремої ухвали слідчого судді з дозволом на проведення аудіо-, відеоконтролю особи як окремої негласної слідчої (розшукової) дії не потрібне, оскільки встановлення таких спеціальних технічних засобів прямо передбачене метою даної негласної слідчої (розшукової) дії. Варто зауважити, що мета негласного обстеження публічно недоступних місць, житла чи іншого володіння особи та аудіо-відеоконтролю особи є зовсім різними. Якщо перша має розшуково-пошуковий та допоміжний характер, то друга спрямована на отримання доказової інформації, яка міститься в спілкуванні особи.

Суб'єктів аудіо-, відео контролю у процесуальній літературі поділяють на суб'єктів-ініціаторів, суб'єктів-виконавців та контролюючих суб'єктів [80]. Так, ініціювати рішення щодо проведення аудіо-, відеоконтролю особи має право слідчий за погодженням з прокурором, прокурор (ч. 3 ст. 246, ч. 2 ст. 258 КПК). Контролюючим суб'єктом, від дозволу або відмови в дозволі котрого залежить проведення досліджуваної НСРД, є слідчий суддя, повноваження якого реалізуються суддею Апеляційного суду Автономної Республіки Крим, апеляційного суду області, міст Києва та Севастополя (ст. 247 КПК). Безпосередніми виконавцями виступають уповноважені оперативні підрозділи, яким доручається проведення цієї НСРД.

У практичній діяльності органів досудового розслідування трапляється підміна гласних слідчих (розшукових) дій аудіо-відеоконтролем особи. Зокрема, виникає питання чи може охоплюватися даною НСРД спілкування підозрюваного із працівниками правоохоронних органів.

Так, у вироку Печерського районного суду м. Києва суд зазначив, що на підтвердження винуватості П. в інкримінованому йому правопорушенні стороною обвинувачення надано протокол негласної слідчої (розшукової) дії щодо аудіо-, відеоконтролю особи від 15.05.2017. Там зафіксовано, як 16.03.2017 в приміщенні кабінету, розташованого на 4-му поверсі Оболонського УП ГУНП у м. Києві, П. в присутності кількох осіб у цивільному одязі розповідає про обставини вчинення кримінального правопорушення - вбивства. Також надано відеозапис зазначеної НСРД.

Пославшись на положення ст.ст.258 та 260 КПК, суд наголосив, що в даному випадку спілкування не було приватним, оскільки П. перебував під контролем працівників поліції та розумів, що фактично дає показання [65].

Аналогічну позицію щодо такого «приватного спілкування» викладено у вироку Дарницького районного суду м. Києва. Зокрема, судом було встановлено, що обвинувачення К. у вчиненні інкримінованого йому злочину ґрунтується на матеріалах оперативно-розшукових заходів із застосуванням технічних засобів з додатками до них, проведених на підставі

ухвали Апеляційного суду м. Києва. Разом з тим твердження прокурора, що вказана негласна слідча (розшукова) дія є аудіо-, відеоконтролем особи, є безпідставними.

Згідно з п.1 ч.4 ст.258 КПК аудіо-, відеоконтроль особи є різновидом утручання в приватне спілкування, який складається з доступу до змісту спілкування за умов, якщо його учасники мають достатні підстави вважати, що воно є приватним. Ураховуючи наведене, суд приходить дійшов до висновку, що спілкування в умовах відділу поліції К. з оперуповноваженим, який брав участь у розслідуванні злочину, у жодному разі не можна визнати слідчою (розшуковою) дією — аудіо-, відеоконтролем особи. Адже учасники такого спілкування не мали жодних підстав уважати, що спілкування є приватним. Тому воно оцінюється судом як допит, проведений за відсутності захисника, участь якого у справах даної категорії є обов'язковою [64].

В описаній ситуації, не можна жодним чином говорити про таємницю спілкування, оскільки підозрюваний усвідомлює, що він спілкується з офіційними посадовими особами, а отже його спілкування не може бути приватним. Характер спілкування між підозрюваним і працівниками правоохоронних органів унеможливлював умови для приватного спілкування, за яких підозрюваний міг би розраховувати на те, що повідомлена ним інформація буде збережена в таємниці.

Відповідно до ст. 270 КПК аудіо-, відеоконтроль місця як НСРД полягає у здійсненні прихованої фіксації відомостей за допомогою аудіо-, відеозапису всередині публічно доступних місць без відома їх власника, володільця або присутніх у цьому місці осіб, за наявності відомостей про те, що розмови і поведінка осіб у цьому місці, а також інші події, що там відбуваються, можуть містити інформацію, яка має значення для кримінального провадження.

Згідно п. 1.11.9. Інструкції аудіо-, відеоконтроль місця полягає у застосуванні технічного обладнання у публічно доступному місці з метою фіксації відомостей (розмов, поведінки осіб, інших подій), які мають

значення для кримінального провадження, без відома присутніх у ньому осіб.

Об'єктом аудіо-, відеоконтролю місця є приватне спілкування особи у публічно доступному місці у вигляді розмов або інших звуків, рухів, дій, пов'язаних з її діяльністю або місцем перебування, а також інші події, які там відбуваються, зміст яких має значення для досудового розслідування.

Визначаючи особливості аудіо-, відеоконтролю особи, які відрізняють її від спостереження за особою, річчю або місцем, аудіо-, відеоконтролю місця, С. Фомін і С. Гриненко зазначають про те, що вона проводиться щодо конкретної особи як у публічно доступних, так і у публічно недоступних місцях (місцях, до яких неможливо увійти або в яких неможливо перебувати на правових підставах без отримання на це згоди власника, користувача або уповноважених ними осіб (ч. 2 ст. 267 КПК) чи в умовах, коли учасники спілкування мають достатні підстави вважати, що спілкування є приватним (розумно розраховують на приватність) [102, с. 436]. Р. Шехавцов і М. Шумило також вважають, що відмінність аудіо-, відеоконтролю особи від передбачених ст.ст. 269, 270 КПК НСРД полягає у використанні аудіо-, відеозаписуючих пристроїв, встановлених всередині публічно недоступних місць для фіксації поведінки особи [103, с. 574].

Також у літературі зазначається, що якщо для візуального спостереження за особою основним завданням є з'ясування і фіксація відомостей щодо її пересування, місць перебування, фактів зустрічей з іншими особами як із застосуванням технічних засобів, так і без, то аудіо-, відеоконтроль особи – НСРД, яка здійснюється з метою отримання інформації і джерелом якої є особа – об'єкт контролю: дії, рухи, висловлювання та інша аудіовізуальна інформація, при цьому місце її знаходження має факультативне значення. Вона проводиться винятково з використанням технічних засобів фіксації інформації [102, с. 436 - 437].

За своїм характером і аудіо-, відеоконтроль особи і місця мають на меті обмеження таємниці спілкування, та спрямовані на отримання доказової інформації, яка міститься в розмовах, рухах чи діях особи. Однак, якщо під

час аудіо-, відеоконтролю особи нас цікавить конкретна особа, яка підозрюється у вчиненні кримінального правопорушення, то під час аудіо-, відеоконтролю місця коло осіб невизначене, в зв’язку з цим обмежується таємниця спілкування невизначеного кола осіб.

2.3. Обмеження таємниці спілкування в ході проведення огляду і виїмки кореспонденції.

Класичною негласною слідчою (розшуковою) дією є арешт, огляд та виїмка кореспонденції. В контексті обмеження таємниці спілкування ми розглянемо лише огляд та виїмку кореспонденції саме під час яких відбувається втручання в таємницю спілкування.

Обмеження конституційного права окремих громадян на таємницю кореспонденції при його здійсненні обумовлюється наявною необхідністю проведення цієї негласної слідчої (розшукової) дії для забезпечення ефективного розслідування злочинів та необхідністю реалізації конституційних вимог щодо захисту прав усіх громадян від будь-яких злочинних посягань [183, с. 1090].

Варто згадати, що порушення під час накладення арешту на кореспонденцію були предметом розгляду ЄСПЛ. Зокрема, Європейський суд у рамках справи "Волохи проти України" встановив, що під час розслідування кримінальної справи в Україні було винесено постанову про накладення арешту на кореспонденцію, яку після її закриття понад один рік не було скасовано. Такими чином, арешт на кореспонденцію протягом тривалого часу діяв після припинення кримінального провадження незаконно обмежував конституційне право Ольги та Михайла Волохів на таємницю листування, телеграфної та іншої кореспонденції [153].

Арешт на кореспонденцію накладається, якщо під час досудового розслідування є достатні підстави вважати, що поштово-телеграфна кореспонденція певної особи іншим особам або інших осіб їй може містити відомості про обставини, які мають значення для досудового розслідування, або речі і документи, що мають істотне значення для досудового розслідування.

Накладення арешту на кореспонденцію особи без її відома проводиться у виняткових випадках на підставі ухвали слідчого судді. У ч. 1 ст. 261 КПК потрібно встановити спеціальні вимоги до ухвали слідчого судді про надання

дозволу на накладення арешту на кореспонденцію. Зокрема, в ухвалі слідчого судді мають бути вказані: підстави на яких буде проводитись слідча (розшукова) дія, прізвище, ім'я та по батькові особи, кореспонденція якої має затримуватися, точна адреса цієї особи, види кореспонденції, на яку накладається арешт, строк дії ухвали, назва установи зв'язку, на яку покладається обов'язок затримувати кореспонденцію та повідомляти про це слідчого.

Після накладення арешту на кореспонденцію у слідчого виникає право здійснювати огляд і виїмку цієї кореспонденції. Виходячи із тлумачення ч. ч. ст. 261 огляду та виїмці підлягають листи усіх видів, бандеролі, посилки, поштові контейнери, перекази, телеграми, інші матеріальні носії передання інформації між особами. Однак даний перелік не є вичерпним, оскільки ст. 1 ЗУ «Про поштовий зв'язок» та Правила надання послуг поштового зв'язку встановлюють дещо ширший перелік цих об'єктів, зокрема до них належать:

– листи - поштове відправлення у вигляді поштового конверта з вкладенням письмового повідомлення або документа, розміри і масу якого встановлено відповідно до законодавства України;

– поштові картки - поштове відправлення у вигляді стандартного бланка, що містить відкрите письмове повідомлення;

– бандеролі - поштове відправлення з друкованими виданнями, діловими паперами, предметами культурно-побутового та іншого призначення, розміри, маса і порядок упакування якого встановлені відповідно до законодавства України;

– секограми - письмові повідомлення, написані секографічним способом, друковані видання для сліпих, кліше із знаками секографії, що подаються у відкритому вигляді, а також звукові записи та спеціальний папір, призначені виключно для сліпих, за умови, що вони відправляються офіційно визнаними установами для сліпих або на їх адресу;

– дрібні пакети - міжнародне рекомендоване поштове відправлення із зразками товарів, дрібними предметами подарункового та іншого характеру, розміри, маса і порядок упакування якого встановлені відповідно до законодавства України;

– міжнародні відправлення з оголошеною цінністю - міжнародне реєстроване поштове відправлення з вкладенням паперів, документів або інших предметів, оцінка вартості яких визначається відправником;

– посилки - поштове відправлення з предметами культурно-побутового та іншого призначення, не забороненими законодавством до пересилання, розміри, маса і порядок упакування якого встановлені відповідно до законодавства України;

– прямі поштові контейнери - внутрішнє реєстроване поштове відправлення з вкладенням товарів та інших матеріальних цінностей у спрощеній упаковці, пересилання якого здійснюється без розкриття;

– мішок «М» - міжнародне реєстроване поштове відправлення (спеціальний мішок) з вкладенням друкованих видань (книг, газет, журналів тощо), що подається для пересилання одним відправником і адресується одному адресатові;

– відправлення «EMS» - міжнародне реєстроване поштове відправлення з вкладенням документів та/або товарів, що приймається, перевозиться і доставляється найшвидшим способом [135].

Під іншими матеріальними носіями передання інформації між особами, на які може бути накладений арешт, потрібно розуміти інформацію, викладення і передача якої можлива разом з поштовим переказом, а також повідомлення, що приймаються від відправника на паперовому або магнітному носії, для передачі електронним шляхом і які доставляються адресату відтвореними в фізичній або електронній формі. Такі повідомлення

вручаються адресату в запечатаному вигляді, як письмова кореспонденція [156, с. 351].

Згідно п. 1.11.4. Інструкції - огляд і виїмка кореспонденції **п**олягає в негласному відкритті й огляді затриманої кореспонденції, на яку накладено арешт, її виїмці або знятті копії чи отриманні зразків, нанесенні на виявлені речі і документи спеціальних позначок, обладнанні їх технічними засобами контролю, заміні речей і речовин, що становлять загрозу для оточуючих чи заборонені у вільному обігу, на їх безпечні аналоги.

Варто погодитися з думкою, що арешт може накладатися на кореспонденцію адресовану конкретній особі або відправлену цією особою. В зв'язку із розміщенням даної негласної слідчої (розшукової) дії у § 2 Глави 21 КПК «втручання у приватне спілкування», не може накладатися арешт на кореспонденцію, яка надходить на конкретну адресу або відправляється з неї, без зазначення особи, якій адресується кореспонденція [55, с. 142].

Варто звернути увагу на певну юридичну колізію у застосуванні норм ст. 262 КПК. Так, виходячи зі змісту статті 262 КПК України кореспонденція, що надійшла до установи зв'язку (поштове відділення) не вручається адресату у строки, визначені відомчими нормативними актами, а затримується для проведення усіх необхідних процесуальних дій (огляду, зняття копій, отримання зразків, виїмки тощо). Саме такий зміст витікає з частини першої, відповідно до якої, огляд затриманої кореспонденції проводиться в установі зв'язку, якій доручено здійснювати контроль і затримувати кореспонденцію.

Разом з тим, зі змісту частини четвертої цієї статті витікає зовсім інша послідовність дій. Так, в цій частині зазначено: «Про кожен випадок проведення огляду, виїмки або затримання кореспонденції складається протокол згідно з вимогами цього Кодексу. У протоколі обов'язково зазначається, які саме відправлення були оглянуті, що з них вилучено і що має бути доставлено адресату або тимчасово затримано, з яких відправлень

знято копії чи отримано зразки». Виходить, що кореспонденція може бути затримана і після її огляду [90, с. 199].

Огляд затриманої кореспонденції проводиться в установі зв'язку, якій доручено здійснювати контроль і затримувати цю кореспонденцію, за участю представника цієї установи, а за необхідності – за участю спеціаліста. У присутності зазначених осіб слідчий вирішує питання про відкриття і оглядає затриману кореспонденцію.

При цьому є доцільним залучення спеціаліста-криміналіста який може надати допомогу слідчому у відкритті (а в подальшому закритті) упаковки затриманої кореспонденції, без порушення захисних засобів, у огляді кореспонденції на предмет виявлення слідів рук, мікрооб'єктів, слідів біологічного походження, слідів повного або часткового підроблення документів, виявлення тайнопису тощо [56, с. 208].

У разі відсутності речей чи документів, які мають значення для досудового розслідування, слідчий дає вказівку про вручення оглянутої кореспонденції адресату. Така вказівка повинна бути зафіксована у протоколі огляду кореспонденції і під розписку доведена до відома особи, яка відповідальна за доставку кореспонденції.

Підставами для проведення виїмки, затриманої в установі зв'язку кореспонденції, є:

– наявність в ухвалі слідчого судді про накладення арешту на кореспонденцію дозволу на проведення її виїмки при встановленні в ній відомостей про обставини, які мають значення для досудового розслідування, або речей і документів, що мають істотне значення *для* досудового розслідування;

– фактичне встановлення слідчим за результатами проведення огляду затриманої кореспонденції, що конкретне поштово-телеграфне відправлення містить відомості про обставини, які мають значення для досудового розслідування, або речі і документи, що мають істотне значення для досудового розслідування, і що зняття з них

копій або їх фотографування, проведення відеозапису вмісту чи отримання зразків з цих відправлень не може забезпечити встановлення відомостей, які мають значення для досудового розслідування [122, с. 40].

Вірною є думка, що значно утруднюється проведення НСРД із залученням співробітників установ зв'язку, а також операторів (провайдерів) телекомунікаційного зв'язку, конфідентів, інших осіб у зв'язку з доповненням наказом СБУ №470 від 17 жовтня 2012 року Зводу відомостей, що становлять державну таємницю – підпунктами 4.12.4 та 4.12.5. Останніми, відповідно, до відомостей, що мають ступінь секретності «таємно», віднесені відомості про факт або методи проведення НСРД, а також відомості, що дають змогу ідентифікувати особу, місце або річ, щодо якої проводиться чи планується проведення НСРД, розголошення яких створює загрозу національним інтересам і безпеці. Подібне нормативно-правове регулювання вимагає наявності у всіх залучених осіб відповідної форми допуску до державної таємниці [121, с. 507-508].

Враховуючи, значну поширеність послуг приватних операторів поштового зв'язку, зокрема більше 30 підприємств, мають ліцензію на надання послуг у сфері поштового зв'язку, в тому числі фінансові відправлення, однак не мають допуску до державної таємниці, і такий допуск не передбачено ліцензіями, і звісно у їх штаті відсутні особи, які мають допуск до державної таємниці, а отже проведення накладення арешту кореспонденції на поштові перевезення, які ними здійснюється станом на сьогодні є неможливим, а огляд такої кореспонденції може проводитися тільки шляхом обшуку, що звісно ускладнює роботу органів досудового розслідування.

Ще одним проблемним питанням є визначення установи зв'язку, керівнику якої слідчий, прокурор направляють ухвалу слідчого судді про дозвіл на проведення накладення арешту на кореспонденцію для забезпечення її виконання. Вирішення цього проблемного питання ще більше

ускладнюється в умовах великого міста, де можуть функціонувати кілька відділень одного або різних операторів поштового зв'язку. У зв'язку з цим постає питання щодо кількості ухвал слідчого судді (або їх копій), потрібних для забезпечення накладення арешту на кореспонденцію. Якщо ж у матеріалах кримінального провадження містяться достатні підстави вважати, що поштово-телеграфна кореспонденція, яка має значення для досудового розслідування, буде передаватися певною особою через оператора поштового зв'язку, перед проведенням накладення арешту на цю кореспонденцію, з метою встановлення відділення зв'язку, який буде використовуватися особою, потрібно передбачити застосування відеоконтролю за цією особою [128, с. 92].

Вважаємо за доцільне розширити сферу застосування цієї НСРД, і зокрема передбачити в ході її проведення право відшуковувати поштово-телеграфну кореспонденцію, на яку необхідно накладати арешт. Така кореспонденція може відшуковуватися за почерком, за виглядом упаковки, місцем відправки чи одержання тощо.

2.4. Обмеження таємниці спілкування в ході проведення зняття інформації з транспортних телекомунікаційних мереж.

У процесі спілкування, зокрема в телефонних розмовах, передаються почуття, освідчення, мрії та бажання, викладаються міркування, думки, дається оцінка тим чи іншим подіям, вчинкам людей. Під час телефонних розмов зачіпаються інтимні та інші сторони життя людини, інформація про які має конфіденційний характер [106, с. 293]. Таким чином, контроль за телефонними розмовами втручається у сферу особистого та сімейного життя осіб, а отже потребує значного контролю з боку слідчого судді та застосуванню у виключних випадках.

Відповідно до п. 1.11.5. Інструкції зняття інформації з транспортних телекомунікаційних мереж полягає в негласному проведенні із застосуванням відповідних технічних засобів спостереження, відбору та фіксації змісту інформації, яка передається особою, а також одержанні, перетворенні і фіксації різних видів сигналів, що передаються каналами зв'язку (знаки, сигнали, письмовий текст, зображення, звуки, повідомлення будь-якого виду).

В свою чергу, зняття інформації з транспортних телекомунікаційних мереж поділяється на:

- контроль за телефонними розмовами, що полягає в негласному проведенні із застосуванням відповідних технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, спостереження, відбору та фіксації змісту телефонних розмов, іншої інформації та сигналів (SMS, MMS, факсимільний зв'язок, модемний зв'язок тощо), які передаються телефонним каналом зв'язку, що контролюється;

- зняття інформації з каналів зв'язку, що полягає в негласному одержанні, перетворенні і фіксації із застосуванням технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, у відповідній формі різних видів сигналів, які передаються каналами зв'язку мережі Інтернет, інших мереж передачі даних, що контролюються.

Аналіз нормативно-правових актів кримінально-процесуального, оперативно-розшукового та телекомунікаційного законодавства, дозволяє стверджувати, що даній негласній слідчій (розшуковій) дії притаманні такі властивості: пов’язана з тимчасовим обмеженням конституційних прав громадян, а саме втручанням у приватне спілкування громадян; здійснюється щодо тяжких або особливо тяжких злочинів у випадках, якщо іншим шляхом отримати інформацію з метою розслідування злочину неможливо; проводиться за ухвалою слідчого судді після погодження з прокурором; полягає в застосуванні спеціальних технічних засобів негласного отримання інформації; тактика проведення аналогічна тактиці проведення оперативно-розшукових заходів із застосуванням технічних засобів негласного отримання інформації; полягає у спостереженні (контролі), відборі інформації, фіксації змісту інформації, а також одержанні, перетворенні та фіксації сигналів, що передаються каналами зв’язку; безпосереднє проведення покладається на уповноважені оперативні підрозділи; передбачає отримання інформації, що передавалася особою за допомогою технічних засобів телекомунікацій або каналами зв’язку та має значення для розслідування; може бути проведена як у комплексі з іншими негласними слідчими (розшуковими) діями, так і окремо; передбачає отримання даних про взаємоз’єднання телекомунікаційних мереж, що дозволяє одночасно встановити місцезнаходження радіоелектронного засобу; результати цієї дії можуть використовуватися у доказуванні на тих самих підставах, що й результати проведення інших слідчих (розшукових) дій [114, с. 232].

Зняття інформації з транспортних телекомунікаційних мереж завжди повинно передбачати контроль розмов обидвох абонентів, шляхом використання безпосереднього підключення до телефонного каналу або сканування радіоканалу. Прослуховування телефонної розмови тільки одного з абонентів, в тому числі і з використанням технічних засобів, без підключення до мережі зв’язку не вважається зняттям інформації з транспортних телекомунікаційних мереж, а повинно розглядатись, як інша

НСРД пов’язана із втручанням у приватне спілкування (наприклад, аудіо-, відеоконтроль особи) [55, с. 149].

Слушним є міркування, що кримінальне процесуальне законодавство України, дозволяючи слідчому, прокуророві чи за їх дорученням уповноваженим оперативним підрозділам проводити відповідно до ст. 263 КПК України негласні слідчі (розшукові) дії, не визначило порядок співвідношення (ідентифікації) кінцевого обладнання з абонентом, адже користуватися кінцевим обладнанням може не лише сам фігурант, а й члени його сім’ї, які, до речі, також можуть користуватися відповідним обладнанням, призначеним для з’єднання з пунктом закінчення телекомунікаційної мережі з метою забезпечення доступу до телекомунікаційних послуг [54, с. 72].

Відповідно до законодавства України, безпосередній контроль і запис телефонних розмов, що прослуховуються, пов’язані з конспіративним підключенням спеціальних технічних засобів до стаціонарної апаратури зв’язку незалежно від форм власності, фізичних і юридичних осіб. Насправді без дотримання умов конспірації в таких випадках навряд чи можна розраховувати на отримання значущої для кримінального провадження інформації. Причому в таємниці має залишатися не лише факт проведення НСРД, а й факт ухвалення рішення про її проведення. Адже в іншому разі мета проведення НСРД навряд чи буде досягнута [168, с. 123].

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, транспортну телекомунікаційну мережу, кінцеве обладнання, на якому може здійснюватися втручання у приватне спілкування.

До таких ідентифікаційних ознак можна віднести:

– електронний код (ідентифікатор) кінцевого обладнання – код, який присвоюється виробником технічних засобів телекомунікацій для унікальної ідентифікації кінцевого

обладнання (міжнародні серійні коди IMEI, ESN, MEID тощо) [136]. IMEI (International Mobile Equipment Identifier - міжнародний ідентифікатор мобільного обладнання) - унікальний номер мобільного телефону. Номер включає в себе 15 цифр. Він присвоюється апарату під час виготовлення і призначений для ідентифікації телефону в мережі GSM [34];

- ідентифікаційна телекомунікаційна картка – засіб, який використовується для позначення (ідентифікації) кінцевого обладнання абонента в телекомунікаційній мережі (SIM-картка, USIM-картка, R-UIM-картка тощо);
- мережевий ідентифікатор споживача – індивідуальний набір цифр та/або символів, присвоєний кінцевому обладнанню абонента та/або споживачеві в телекомунікаційній мережі чи Інтернеті. Під ним потрібно розуміти або номер абонента в мережах GSM, CDMA або IP-адресу електронної інформаційної системи. IP-адреса (Internet Protocol Address) – це унікальний числовий ідентифікатор конкретного пристрою в складі комп'ютерної мережі, побудованої на основі протоколу TCP / IP. Кожна онлайн-дія включає обмін IP-адресами, тобто кожен пристрій дізнається IP-адресу іншого, з ким він з'єднується, так як для роботи в Інтернеті потрібна унікальність його кожного пристрою. IP-адреси поділяються на статичні і динамічні. Статичні IP-адреси є незмінними (постійними). Вони присвоюються пристрою автоматично в момент його приєднання до комп'ютерної мережі або прописуються користувачем вручну. Статичні адреси доступні для використання необмежений час. Вони можуть виконувати функцію ідентифікатора тільки для одного мережевого вузла.

  Динамічні IP-адреси присвоюються пристрою на певний час. Вони автоматично присвоюються в момент підключення до

мережі і мають обмежений термін дії (від початку сесії до її завершення). Динамічні IP-адреси - своєрідний спосіб маскування. Відстежити людину, що виходить в Інтернет за допомогою такої адреси, складно технічно, в цьому випадку не обійтися без професійних інструментів;

– MAC-адреса – це унікальний ідентифікатор мережевого інтерфейсу (зазвичай мережевої карти) для реалізації комунікації пристроїв в мережі на фізичному рівні. В той час як IP-адреса є логічною і може змінюватися адміністратором мережі, MAC-адреса є апаратною і постійною. Саме вона використовується при обміні інформацією між комп'ютерами через локальну мережу. Перед тим як відправити пакет з даними за певною IP-адресою, комп'ютер повинен дізнатися фізичну адресу одержувача. Кожен комп'ютер зберігає фізичні адреси мережевих пристроїв своєї локальної мережі в спеціальній ARP-таблиці і отримує MAC-адресу з неї. Для кожного мережевого інтерфейсу існує окрема ARP-таблиця.

Оперативні підрозділи, здійснюючи зняття інформації з транспортних телекомунікаційних мереж, можуть встановити: факт передавання інформації в режимі реального часу з фіксацією змісту відомостей, що передаються, установленням їх отримувача, кінцевого обладнання тощо; дані про початок, кінець, тривалість і зміст з’єднання, що передаються в режимі реального часу; зміст електронної пошти або SMS, MMS повідомлень, (як відкритих й прочитаних абонентом, так і невідкритих й непрочитаних); зміст телефонних розмов підозрюваного або іншої особи [87, с.36].

Можна навести наступний приклад. Слідчим управлінням ГУНП у Львівській області проводилося досудове розслідування у кримінальному провадженні за фактом умисного вбивства, вчиненого з корисливих мотивів, за попередньою змовою групою осіб та розбою, поєднаного із проникненням в житло і заподіянням тяжких тілесних ушкоджень за ч. 4 ст. 187, п.п. 6, 12 ч.

2 ст. 115 КК України.

З матеріалів, які стали підставою для початку досудового розслідування вбачалося, невстановлені особи на автомобілі прибули у одне із сіл Львівської області, маючи із собою заздалегідь заготовлені для уникнення викриття маски та дезінфікуючі засоби, шляхом розбиття склопакета вікна проникли у приватний будинок, де з метою подолання опору подружжя потерпілих літнього віку та їх знерухомлення за допомогою липкої стрічки та отримання відомостей про місце схову цінних речей у домі, нанісши власнику тяжкі тілесні ушкодження, які призвели до його смерті, заволоділи ювелірними виробами та грошовими коштами останнього, після чого з викраденим майном з місця події втекли.

Під час проведення досудового розслідування проводився великий обсяг негласних слідчих (розшукових) дій, а саме, передбачених ст.ст. 260, 263, 269 КПК України.

В ході проведення вказаних НСРД було здобуто фактичні дані про причетність 3 осіб до вказаного кримінального правопорушення, а також інших нерозкритих кримінальних правопорушень, що були вчинені на території різних областей України, зокрема крадіжок і розбійних нападів, поєднаних з проникненням у житло.

Відтак за результатами проведених НСРД 2 особам додатково повідомлено про підозру у вчиненні кримінальних правопорушень, передбачених ч. 3 ст. 187, ч. 3 ст. 185, ч. 2 ст. 262 КК України, які були вчинені впродовж 2017 – 2020 років [101].

В літературі зазначається, що слідчий ознайомлюється з інформацією, здобутою під час зняття інформації з транспортних телекомунікаційних мереж тільки після завершення негласної слідчої (розшукової) дії [55, с. 149]. Практика виробила іншу процедуру, яка не суперечить закону, але оптимізує проведення слідчої (розшукової) дії. В дорученні вказується про надання можливості періодично ознайомлюватися слідчому або іншій зазначеній особі з інформацією, яка отримується протягом строку дії дозволу на

проведення негласної слідчої (розшукової) дії. Використання вказаного прийому має позитивні наслідки.

По-перше, оскільки лише слідчий (працівник оперативного підрозділу), обізнаний у матеріалах кримінального провадження, розуміє справжній зміст розмов або інших повідомлень між кореспондентами, то регулярне ознайомлення з інформацією дозволяє вибирати із загального потоку лише ті відомості, які мають значення для розслідування. Накопичена протягом строку проведення негласної слідчої (розшукової) дії корисна інформація в компактному викладі в подальшому викладається в протоколі. Отже, до протоколу даної дії будуть внесені лише ті фрагменти спілкування, які містять важливі для кримінального провадження дані.

По-друге, своєчасне отримання інформації ще до моменту остаточного складання протоколу дає можливість слідчому негайно прийняти заходи з протидії злочину, який вчинюється або готується, провести інші гласні або негласні слідчі (розшукові) дії. Крім того, попередній аналіз інформації дає можливість отримати відомості про можливі носії доказової інформації та їх місцезнаходження (схованки, місця поховання трупа, особи, які мають необхідні відомості тощо); а також про характерні риси цих носіїв інформації (наприклад, про зв’язки підозрюваних, їх взаємовідношення з іншими особами і т.п.); про можливу поведінку учасників процесу на допитах; про ті дані, які можуть бути отримані шляхом дослідження тих чи інших носіїв. Такі відомості сприяють правильному вибору тактичних і технічних заходів пошуку та дослідження нових доказів, а також сприяють оцінці вже отриманих даних. На відміну від доказової, така попередня інформація має орієнтуючий характер [185, с. 157 - 158].

Під час проведення цієї НСРД здійснюється накопичення значного обсягу інформації, яка стосується особистого життя громадян. В зв’язку з цим, відомості, речі та документи, отримані в результаті проведення негласних слідчих (розшукових) дій, які прокурор не визнає необхідними для подальшого проведення досудового розслідування, повинні бути невідкладно

знищені на підставі його рішення у порядку ст. 255 КПК.

Варто погодитися із думкою тих дослідників, які вважають, що використанню для доказування матеріалів звукозапису телефонних розмов має передувати експертиза матеріалів і засобів звукозапису, яка може дати відповіді на такі питання: кому з числа перерахованих осіб належать окремі вислови, що містяться на фонограмі; чи є голос, зафіксований на фонограмі, голосом конкретної особи; чи зазнавала змін ця фонограма; чи мають місце ознаки монтажу фонограми; які є ознаки механічного й електронного монтажу фонограми; чи велася зафіксована на фонограмі розмова телефоном тощо. При цьому в науковій юридичній літературі зазначається, що труднощі виникають із матеріалами звукозапису, виготовлених із використанням цифрової техніки. Експерти досі не мають технічної можливості встановити наявність або відсутність ознак монтажу. Якщо експерти роблять висновок про те, що встановити наявність або відсутність ознак монтажу неможливо, зафіксовані на відповідному носії дані стають сумнівними. Усі сумніви мають тлумачитися на користь обвинуваченого. А отже, матеріали технічного документування, щодо яких виникають сумніви щодо їх допустимості у справі і достовірності, використанню для доказування не підлягають [164, 123].

2.5. Обмеження таємниці спілкування в ході проведення зняття інформації з електронних інформаційних систем.

Згідно п. 1.11.6. Інструкції зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача полягає в одержані інформації, у тому числі із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютер), автоматичних системах, комп'ютерній мережі.

Під електронною інформаційною системою слід розуміти взаємозв’язок технічних засобів (комп’ютерів, серверів, апаратно-програмних комплексів, зовнішніх накопичувачів інформації, локальних комп’ютерних мереж та/або інших технічних засобів) з інформаційними технологіями, що реалізують інформаційні процеси та призначені для збору, зберігання, обробки, пошуку, розповсюдження, передачі та надання впорядкованої інформації (даних) в електронному вигляді. В той же час, під частинами електронних інформаційних систем слід вважати бази даних, системи управління базами даних, клієнтське програмне забезпечення, доступ до яких обмежується їх власником, володільцем або утримувачем, зокрема застосуванням системи логічного захисту [69, с. 72].

Зняття інформації з електронних інформаційних систем або їх частин може здійснюватися, як шляхом безпосереднього фізичного доступу до них фахівцями уповноважених підрозділів правоохоронних органів, так і шляхом програмного проникнення. Негласне зняття інформації з засобів електронно-обчислювальної техніки полягає у застосуванні технічних засобів із великими ресурсами оперативної та довгочасної пам’яті, яка забезпечує повне копіювання інформації із жорсткого диску (дисків) та інших електронних носіїв інформації підозрюваного, обвинуваченого.

Програмне проникнення до електронних інформаційних систем (їх частин) здійснюється шляхом застосування спеціальних програмних продуктів, які забезпечують подолання системи захисту і копіювання інформації, що обробляється в зазначених системах (їх частинах), на

віддалений комп’ютер, що перебуває у користуванні уповноваженого органу, який проводить цю НСРД.

Сукупність таких технічних та програмних засобів для проведення зазначеної НСРД складає окремий вид спеціальних технічних засобів для зняття інформації з каналів зв’язку та інших технічних засобів негласного отримання інформації [69, с. 71].

Враховуючи функціональні особливості та методи отримання інформації з електронних інформаційних систем, виділяють наступні типи СТЗ:

1) засоби для зняття (шляхом фізичного/технічного доступу) інформації з електронних інформаційних систем або з їх частин;

2) спеціалізовані програми для зняття (шляхом програмного проникнення), порушення цілісності, знищення, блокування та/або копіювання інформації з електронних інформаційних систем або з їх частин;

3) закладні пристрої, що розміщують безпосередньо в засобах обчислювальної техніки (USB-портах, системних платах, клавіатурах тощо) або в периферійному обладнанні (модемах, принтерах та інших пристроях);

4) засоби зняття, фіксації та аналізу побічних електромагнітних випромінювань від електронних інформаційних систем;

5) спеціальні засоби для експрес копіювання, руйнування (знищення) інформації з технічних носіїв [69, с. 72].

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 НСРД; 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 електронної інформаційної системи; обґрунтування можливості отримання під час проведення даної НСРД 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 ЄРДР щодо кримінального провадження, у рамках якого подається клопотання.

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:

− IP-адреса (IP − 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 ЕОМ.

Важливо підкреслити, що у протоколі негласної слідчої (розшукової) дії підлягають відображенню такі відомості:

- в пам'яті якого пристрою виявлено віртуальні сліди;

- кому належить пристрій; чи має пристрій вихід в мережу Інтернет, інші телекомунікаційні або локальні мережі;

- яка оперативна система функціонує на пристрої (Windows, Linux – на комп'ютері, Windows mobile, Android, Symbian – на мобільному телефоні, комунікаторі, планшеті і т.п.);

- в яких файлах виявлені сліди втручання, які саме;

- коли файл був створений, змінений, відкривався востаннє [125, с. 239].

Висновки до Розділу 2

1. Можна виокремити наступну систему процесуальних дій, спрямованих на обмеження таємниці спілкування.

Зокрема, на підставі ухвали слідчого судді суду першої інстанції проводяться наступні процесуальні дії спрямовані на обмеження таємниці спілкування:

- тимчасовий доступ до речей та документів;
- обшук.

На підставі ухвали слідчого судді апеляційного суду, слідчого судді Вищого антикорупційного суду проводяться такі негласні слідчі (розшукові) дії:

– аудіо-, відеоконтроль особи;
- накладення арешту на кореспонденцію, огляд і виїмка кореспонденції;
- зняття інформації з транспортних телекомунікаційних мереж;
- зняття інформації з електронних інформаційних систем;
- спостереження за особою;
- аудіо-, відеоконтроль місця.

2. В ході обстеження публічно недоступних місць, житла чи іншого володіння особи слідчий, працівники оперативних підрозділів не мають права втручатися у таємницю спілкування, зокрема у особисте листування особи, інші форми спілкування зафіксовані на матеріальних чи електронних носіях, які знаходяться в публічно недоступних місць, житлі чи іншому володіння особи. Така позиція зумовлено змістом даної НСРД, яка в основному носить організаційно-допоміжний характер.

3. Ухвала слідчого суддя про дозвіл на проведення НСРД, які обмежують таємницю спілкування, обов’язково має бути розсекречена та долучена до матеріалів кримінального провадження, оскільки відсутність ухвали слідчого судді про дозвіл на проведення негласних слідчих (розшукових) дій унеможливлює використання їх результатів у доказуванні.

4. З метою вирішення питання про можливі порушення прав людини оперативними підрозділами під час проведення НСРД у зв’язку з відсутністю належного судового контролю та прокурорського нагляду в ході їх здійснення пропонується запровадження інституту залучення особи, яка під час судового розгляду клопотань про НСРД буде забезпечувати дотримання прав осіб щодо яких будуть застосовуватися обмеження. В зв’язку з цим, пропонуємо викласти ч. 1 ст. 261 КПК в наступній редакції «Слідчий суддя зобов'язаний розглянути клопотання про надання дозволу на проведення негласної слідчої (розшукової) дії протягом шести годин з моменту його отримання. Розгляд клопотання здійснюється за участю особи, яка подала клопотання та адвоката делегованого центром безоплатної правової допомоги». Такий адвокат, повинен мати допуск до державної таємниці, а доступ до матеріалів клопотання про надання дозволу на проведення НСРД буде надаватися слідчим суддею перед його судовим розглядом.

5. На підставі аналізу ст. 162 КПК України можна виокремити дві групи даних, які можна отримати під час тимчасового доступу до речей та документів, які становлять таємницю спілкування. До них зокрема належать особисте листування особи та інші записи особистого характеру та інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв’язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

6. У зв’язку з неоднозначністю застосування норм КПК щодо отримання інформації, яка містить таємницю спілкування та знаходиться в електронних інформаційних системах потрібно закріпити окрему слідчу (розшукову) дію, як різновид слідчого огляду – огляд електронної інформаційної системи. Такий огляд проводиться щодо електронних інформаційних систем, які вилучені в ході інших слідчих (розшукових) дій та здійснюється на підставі ухвали слідчого судді місцевого суду.

7. Доцільним є долучення до клопотання про тимчасовий доступ до речей та документів, що знаходяться в операторів та провайдерів

телекомунікацій, матеріалів радіотехнічної розвідки, які дозволяють додатково ідентифікувати базові станції через які здійснювали спілкування підозрювані, а отже обмежити порушення таємниці спілкування невизначеної кількості абонентів.

8. Шляхом тимчасового доступу до речей документів які знаходяться в операторів та провайдерів телекомунікацій може отримуватися лише інформація про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання, яка за своїм змістом охороняється таємницею спілкування.

9. У практичній діяльності органів досудового розслідування трапляється підміна гласних слідчих дій аудіо-відеоконтролем особи. Зокрема, виникає питання чи може охоплюватися даною НСРД спілкування підозрюваного із працівниками правоохоронних органів. В описаній ситуації, не можна жодним чином говорити про таємницю спілкування, оскільки підозрюваний усвідомлює, що він спілкується з офіційними посадовими особами, а отже його спілкування не може бути приватним. Характер спілкування між підозрюваним і працівниками правоохоронних органів унеможливлює умови для приватного спілкування, за яких підозрюваний міг би розраховувати на те, що повідомлена ним інформація буде збережена в таємниці.

10. За своїм характером і аудіо-, відеоконтроль особи і місця мають на меті обмеження таємниці спілкування, та спрямовані на отримання доказової інформації, яка міститься в розмовах, рухах чи діях особи. Однак, якщо під час аудіо-, відеоконтролю особи нас цікавить конкретна особа, яка підозрюється у вчиненні кримінального правопорушення, то під час аудіо-, відеоконтролю місця коло осіб невизначене, в зв'язку з цим обмежується таємниця спілкування невизначеного кола осіб.

11. Вважаємо за доцільне розширити сферу НСРД - арешт, огляд і виїмка кореспонденції і зокрема передбачити в ході її проведення право відшуковувати поштово-телеграфну кореспонденцію, на яку необхідно

накладати арешт. Така кореспонденція може відшуковуватися за почерком, за виглядом упаковки, місцем відправки чи одержання тощо.

12. У ч. 1 ст. 261 КПК потрібно встановити спеціальні вимоги до ухвали слідчого судді про надання дозволу на накладення арешту на кореспонденцію. Зокрема, в ухвалі слідчого судді мають бути вказані: підстави на яких буде проводитись слідча (розшукова) дія, прізвище, ім’я та по батькові особи, кореспонденція якої має затримуватися, точна адреса цієї особи, види кореспонденції, на яку накладається арешт, строк дії ухвали, назва установи зв’язку, на яку покладається обов’язок затримувати кореспонденцію та повідомляти про це слідчого.

РОЗДІЛ 3
ВИКОРИСТАННЯ В ДОКАЗУВАННІ РЕЗУЛЬТАТІВ ПРОЦЕСУАЛЬНИХ ДІЙ СПРЯМОВАНИХ НА ОБМЕЖЕННЯ ТАЄМНИЦІ СПІЛКУВАННЯ

Питання ефективності використання доказів, які отримуються в ході НСРД, зокрема і спрямованих на обмеження таємниці спілкування, неодноразово постає у науці та практичній діяльності.

На думку Д.Б. Сергеєвої лише до 5% результатів НСРД визнаються доказами національними судами, що безумовно актуалізує дослідження причин такого низького використання результатів НСРД для отримання доказів у кримінальному провадженні [149, с. 82].

Більш оптимістично до використання результатів НСРД підходить В.М. Трепак. На його думку, про ефективність НСРД свідчить, зокрема, те, що у кримінальному провадженні використовують лише від 22,6 % до 30,5 % результатів НСРД, які проводяться на підставі ухвал слідчих суддів, та від 35,6 % до 50,8 % результатів НСРД, які проводяться за рішеннями прокурорів (контроль за вчиненням злочину, виконання спеціального завдання). Враховуючи істотне обмеження прав людини під час їхнього проведення, результативність НСРД не можна визнати високою. Відтак, крім питання ефективності НСРД виникає питання обґрунтованості їхнього проведення. Адже якщо у кримінальному процесі використовуються результати лише третьої чи навіть п’ятої частини проведених слідчих (розшукових) дій, то закономірно постає питання про те, на яких підставах і з якою метою проводились інші НСРД [161, с. 295].

Така ситуація із використанням результатів НСРД зумовлена нехтуванням працівниками оперативних підрозділів та органів досудового розслідування вимогами кримінального процесуального законодавства, а також неврахування специфіки отриманої доказової інформації.

Варто погодитися з думкою, що результати НСРД розглядаються лише як різновиди матеріально фіксованих джерел, що виникають у процесі

проведення НСРД та містять певну інформацію, відомості, тобто у вузькому значенні цього терміну. Результати НСРД для їх подальшого використання, в тому числі й у кримінальному процесуальному доказуванні, мають бути трансформовані в передбачену матеріальну форму – відповідні матеріали НСРД. Сама лише змістовна складова результатів їх проведення – інформація, що отримується в результаті їх проведення, не дозволяє її використовувати у кримінальному процесуальному доказуванні [149, с. 86].

Ще одним проблемним питанням є фіксація ходу та результатів НСРД. Відповідно до ч.1 ст. 110 КПК України, процесуальними рішеннями є всі рішення органів досудового розслідування, прокурора, слідчого судді, суду. Відповідно до ч.3 ст. 110 КПК України, рішення слідчого, прокурора приймається у формі постанови. Постанова виноситься у випадках, передбачених цим Кодексом, а також коли слідчий, прокурор визнає це за необхідне. Відповідно до ч.1 ст. 107 КПК України, рішення про фіксацію процесуальної дії за допомогою технічних засобів під час досудового розслідування приймає особа, яка проводить відповідну процесуальну дію.

Таким чином, оскільки положеннями КПК України прямо передбачено, що рішення про фіксацію процесуальної дії за допомогою технічних засобів приймається особою, яка проводить відповідну процесуальну дію, то відповідно до ч.3 ст. 110 КПК України, особа, яка проводить негласну слідчу (розшукову) дію (наприклад аудіо- відео контроль особи), повинна винести відповідну постанову про фіксацію процесуальної дії за допомогою технічних засобів. При цьому, слідчий (оперативний працівник) повинні вказати у цій постанові ідентифікаційні ознаки технічних засобів, які будуть використані під час проведення процесуальної дії. Посилання прокурора на ту обставину, що ухвалою слідчого судді, який надав дозвіл на проведення негласних слідчих (розшукових) дій вже надано дозвіл на проведення аудіо-відеоспостереження і винесення постанови відповідно до ч.1 ст. 107 КПК України недоцільне, не може прийматися до уваги, оскільки ухвала слідчого судді лише надає дозвіл слідчому та/або прокурору на проведення аудіо-

відео контролю.

Проте, дане рішення слідчого судді є пасивним. Реалізація цього рішення залежить від волі слідчого чи прокурора і не носить для них обов'язкового характеру. Отримавши такий дозвіл від слідчого судді, прокурор в залежності від обставин кримінального провадження, може не проводити відповідну негласну процесуальну дію. Крім того, в ухвалі слідчого судді не відображаються технічні засоби, які будуть використані для проведення НСРД, оскільки такої інформації у слідчого судді не має і не може бути на момент прийняття ним такого рішення. Не винесення відповідної постанови про фіксацію процесуальної дії за допомогою технічних засобів є істотним порушенням ч.1 ст. 107 КПК України, що тягне за собою недопустимість даного доказу, оскільки даний доказ отриманий не в порядку передбаченому Кримінальним процесуальним кодексом України.

Особливу важливість наявність відповідної постанови має для такої негласної слідчої (розшукової) дії, як аудіо- відеоконтроль особи, аудіо- відео контроль місця.

Адже перевірити достовірність зробленого відеозапису під час проведення даних негласних слідчих (розшукових) дій, можливо лише за допомогою відповідної експертизи, призначення та проведення якої можливе лише за наявності конкретних технічних засобів, які використовувалися під час проведення аудіо- відео фіксування процесуальної дії. Встановити ж якими саме технічними засобами здійснювалося аудіо- відеоспостереження, без відображення цих даних в матеріалах кримінального провадження неможливо, що ставить отримані таким чином докази під сумнів.

Під час проведення процесуальних дій спрямованих на обмеження таємниці спілкування органи досудового розслідування отримують різноманітні джерела доказів, однак враховуючи специфіку процесуальних дій, які у більшості випадків пов'язані із отриманням інформації із транспортних телекомунікаційних мереж та електронних інформаційних систем, слідчому доводиться мати справу із великим обсягом інформації

розміщеної на матеріальних носіях інформації.

За своєю правовою природою така інформація згідно з п. 1 ч. 2 ст. 99 КПК визнається документом. Чинний КПК не встановлює спеціальних вимог до форми, змісту та процесуального порядку долучення електронних документів. Водночас, у більшості країн світу давно розробляється концепція використання цифрових (електронних) доказів.

Так, міжнародною організацією по цифрових доказах (International Organization on Digital Evidence (IOCE)) визначені наступні принципи операцій з цифровою інформацією, що є доказом:

1) при роботі з доказовою інформацією, що міститься на цифровому носії, повинні дотримуватися процесуальні і криміналістичні вимоги;

2) при операціях з доказовою інформацією на цифрових носіях неприпустимо внесення змін до цієї інформації;

3) всі операції з виявлення, вилучення, зберігання і переміщення доказової інформації на цифрових носіях повинні бути зафіксовані в документальній формі, захищені від несанкціонованої зміни і придатні для дослідження;

4) особа, яка здійснює операції з доказової інформацією на цифрових носіях, несе відповідальність за її збереження, поки має доступ до цієї інформації;

5) будь-яка організація, що здійснює виявлення, вилучення, зберігання і переміщення доказової інформації на цифрових носіях, повинна дотримуватися вказаних принципів [26].

Аналізуючи норми КПК можна зауважити, що не всі із вказаних вимог враховані під час використання результатів НСРД та тимчасового доступу до речей і документів, які містять таємницю спілкування.

Основним при формулюванні ознак отриманої інформації має бути вказівка на важливу для кримінального провадження складову таких джерел доказів, а не на їх технічні властивості. Специфічні особливості цифрових даних полягають у тому, що:

– доказове значення мають не фізичні або технічні параметри носія, а електронна інформація яка на ньому міститься або факт її перебування на даному носії;

– ця інформація створена не в процесі розслідування кримінального провадження та не є загальнодоступною;

– сприйняття цієї інформації можливе тільки із застосуванням спеціальних пристроїв;

– сучасні технічні можливості дозволяють вносити зміни в зміст зазначеної інформації, в тому числі і без безпосереднього впливу на носій;

– зміна інформації, наявної на носії, може бути здійснена без відображення у вигляді матеріальних слідів [73, с. 3].

Варто погодитися з думкою, що основні принципи роботи з електронними доказами полягають у такому: 1) необхідно забезпечити цілісність відібраного матеріалу та збереження історії його передачі шляхом безперервного інструментального контролю за вилучення даних; 2) необхідно документувати будь-які дії, які виконуються щодо цифрових (електронних) доказів, щоби незалежна третя сторона могла, повторивши ці дії, отримати аналогічний результат; 3) необхідна підтримка спеціалістів, які повинні мати: спеціальні знання і досвід у відповідній сфері; досвід і навички поводження із цифровими джерелами інформації; розуміння досліджуваного питання; необхідні правові знання; відповідні комунікаційні навички (що дозволяють їм давати усні та письмові пояснення); достатні і необхідні мовні навички; правові підстави для залучення у процесуальні дії; 4) якщо під час огляду не присутні спеціалісти із цифрових джерел інформації, то особи, які виконують слідчі дії на місці огляду/обшуку, повинні володіти необхідними знаннями для виявлення і збору доказів; 5) органи і особи, які ведуть розслідування, зобов’язані дотримуватися законодавства, загальних криміналістичних і процесуальних принципів. Для того, щоби розумно задокументувати відомості з цифрових джерел, потрібно враховувати

функціональні особливості технологій, з використанням яких їх було створено, збережено, передано тощо [59, с. 121 -122].

Запровадження в кримінальному процесуальному законі новітньої категорії «електронні носії інформації» зумовлено практичною потребою визнати ці об'єкти джерелом доказів у кримінальному провадженні. Буквальне тлумачення тексту ст. 99 КПК дає підстави для висновку, що «електронні носії інформації» потрібно трактувати як будь-які електронні носії. Такі носії можуть бути вбудовані в комп'ютерні пристрої, підключені до інформаційної мережі. Вони можуть містити матеріали в будь-якій формі (письмовій, графічній, фотографічній, відео- чи звукозапису тощо) [126, с. 14]. Однак, потрібно розмежовувати поняття «електронні носії інформації» та «електронні докази», оскільки один електронний носій інформації може містити у собі декілька електронних доказів.

В юридичній літературі англійський термін «digital evidence» трактується по різному, одні автори перекладають його як «електронні докази», інші як «цифрові докази» вкладаючи різний зміст у це поняття, або ототожнюючи дані терміни. Вважаємо за більш доцільне використовувати термін «цифрові докази», який відображає природу створення даних доказів.

У зарубіжній літературі під поняттям «цифрові або електронні докази» розуміється будь-яка доказова інформація, що зберігається або передається в цифровій формі, яку сторона судової справи може використовувати в судовому розгляді. Цифрові докази – це вся інформація в цифровій формі, яка може використовуватися як доказ у кримінальному провадженні [22, с. 7].

Цифрова інформація може бути розподілена на сам контент (наприклад, текстовий документ, малюнок або фотографія, база даних і т.д.) та інформацію про цей контент (метадані). Часто неможливо обробляти цифрову інформацію, не отримуючи інформацію з метаданих [2].

Так, Д.М. Цехан під «цифровим доказом» розуміє фактичні дані, представлені у цифровій (дискретній) формі та зафіксовані на будь-якому

типі носія, що стають доступними для сприйняття людиною після обробки ЕОМ та на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню [178, с. 259].

Під цифровим доказом слід розуміти будь-яку інформацію, на підставі якої слідчий, прокурор, слідчий суддя та суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження, дослідження якої може бути здійснено за допомогою спеціальних програмно-технічних засобів [185, с. 148].

І. О. Крицька виокремлює характерні властивості цифрових джерел доказової інформації, які обґрунтовують їх особливий процесуальний статус: а) неречовий характер, який пов’язаний з відсутністю твердого зв’язку з матеріальним носієм; б) неможливість безпосереднього сприйняття та подальшого дослідження цифрової інформації, тобто, вона повинна бути інтерпретована та перекодована за допомогою спеціальних технічних засобів і програмного забезпечення; в) існування можливості дистанційного внесення змін до неї та її знищення; г) специфічний порядок збирання, перевірки й оцінки цифрових джерел доказової інформації [105, с. 304].

Досить повна і розгорнута класифікація цифрових доказів проведена групою авторів, які виокремлюють наступні види цих доказів:

1) файл;

2) мережева адреса;

3) доменне ім'я;

4) електронне повідомлення;

5) електронний документ;

6) інформаційна система;

7) сайт в мережі Інтернет;

8) сторінка сайту в мережі Інтернет;

9) електронний підпис;

10) комп'ютерна програма;

11) база даних;

12) електронний журнал;

13) електронні грошові кошти [140, с. 68].

Інформаційна сутність фіксації доказів, що знаходяться в електронній формі, полягає в наступному.

1. Проводиться перекодування доказової комп'ютерної інформації, що знаходиться на оригінальному матеріальному носії, в форму, доступну для сприйняття її людиною, наприклад, вона відображається на екрані (моніторі) комп'ютерного пристрою або прослуховується як фонограма.

2. Комп'ютерна інформація вилучається разом з її матеріальним носієм або копіюється на відмінний від оригіналу матеріальний носій, коли його вилучення неможливо або недоцільно.

3. Забезпечується збереження доказової комп'ютерної інформації для неодноразового її використання в процесі доказування, наприклад, в процесі судово-експертного дослідження, пред'явлення як доказу в ході допиту.

4. Завдяки збереженню зафіксованої «порції» комп'ютерної інформації забезпечується можливість її накопичення до необхідного обсягу, тобто до моменту доведення всіх обставин, що підлягають доказуванню. Наприклад, за реквізитами файлу електронного повідомлення, відправленого підозрюваним адресу потерпілого, встановлюють приблизну дату і час вчинення злочину, електронну адресу підозрюваного, ідентифікатор його комп'ютерного передавального пристрою, абонентський номер цього пристрою в мережі оператора зв'язку, фізичну адресу знаходження комп'ютерного пристрою, з якого було відправлено повідомлення, можливі сліди підготовки зазначеного повідомлення на даному технічному пристрої.

5. Забезпечується можливість відбору інформації про подію злочину: фіксується не вся комп'ютерна інформація, а лише та яка стосується предмету доказування.

6. Фіксується не тільки сама доказова комп'ютерна інформація, але

також інформація про шляхи, способи її отримання, як необхідна умова визнання її допустимості у кримінальному провадженні [62, с. 48].

Можна виокремити загальні особливості слідчих та інших процесуальних дій, проведення яких має на меті збирання і перевірку електронної доказової інформації:

1. Процесуальна коректність фіксації: вміст і реквізити цифрової інформації підлягають обов'язковому опису в протоколі слідчої дії або експертному висновку. Однак найчастіше виключно документально-текстова фіксація є недостатньою, тому рекомендується вносити в текст процесуального документу або додавати до нього скріншоти, роздруківки логів, витяги з зовнішньої аналітики і статистики по сайту і т.п. У разі копіювання цифрової інформації, повинен бути долучений оригінальний носій з якого здійснювалося копіювання. Крім того, до участі в слідчому огляді рекомендується залучати понятих, яким варто послідовно роз'яснювати сутність всіх дій слідчого і спеціаліста.

2. Точний опис проведених операцій щодо виявлення інформації, в тому числі із зазначенням використаних технічних засобів, програмного забезпечення (включаючи точну версію). Специфіка подібної вимоги полягає в тому, що на відміну від багатьох інших слідів, цифрова інформація, особливо розміщена в Інтернеті, після її вивчення суб'єктом розслідування може залишитися незмінною. Відповідно, комплекс операцій по її виявленню і фіксації повинен становити собою формалізований алгоритм, який при необхідності може бути у точності відтворений згодом [99, с.78].

Відмінність електронних носіїв інформації від «традиційних» речових доказів та інших документів призводить до необхідності використовувати різні прийоми і засоби роботи з зазначеними доказами. «Предметні» речові докази містять в якості доказової інформації сліди матеріального світу. Зміна цієї інформації неможлива без безпосереднього впливу на сам предмет. Тому для гарантування їх достовірності цілком достатньо традиційної упаковки, що забезпечує відсутність механічного впливу. Стверджувати це ж щодо

електронних носіїв інформації неможливо. Тому вимога застосування спеціальних засобів, що виключають дистанційний вплив на них, є обов'язковою вимогою під час їх огляду та вилучення.

В окремих ситуаціях доказове значення можуть мати логи - системні записи, в яких відображаються дії користувача. І хоча у спеціальній літературі можна зустріти думку про доцільність роздрукування логів, такий підхід видається непрактичним, оскільки їх довжина може налічувати сотні тисяч сторінок, відповідно, більш коректним видається їх копіювання за допомогою спеціаліста. Оскільки, як правило, доступ до логів можливий лише із застосуванням спеціальних знань, для їх отримання потрібна допомога спеціаліста. Також варто документувати не тільки самі логи, але і програми, що їх створюють, їх налаштування. Крім того, потрібно з’ясувати в спеціаліста або експерта думку щодо інтерпретації логів на підставі вищевказаної інформації [175, с. 208].

Встановлення наявності адреси електронної пошти і навіть її змісту саме по собі не може бути доказом того, що ця адреса електронної пошти належить конкретній особі. Після встановлення скриньки електронної пошти, прив'язаної до адреси електронної пошти, необхідно встановити, хто користувався цією скринькою і, отже, є власником адреси електронної пошти. Відомості такого роду можуть бути отримані в ході тимчасового доступу до речей і документів, обшуків, зняття інформації з транспортних телекомунікаційних мереж і електронних інформаційних систем можуть включати в себе наступні факти:

- наявність на комп'ютерних пристроях, що належать конкретній особі, додатків з налаштованим доступом до поштової скриньки або збережених в браузері вкладок, закладок, пар «логін-пароль», що забезпечують доступ до онлайн-сервісів електронної пошти;

- наявність на поштовому сервері, який обробляє передані повідомлення електронної пошти, логів (записів) про те, що користувач поштової скриньки успішно авторизувався на сервері і використовував

електронну пошту;

- наявність на комп'ютерних пристроях, що належать особі, отриманих і збережених повідомлень електронної пошти в яких відобразилася службова інформація про те, що повідомлення було отримано на конкретну адресу електронної пошти;

- наявність на комп'ютерних пристроях, що належать особі, чернеток повідомлень електронної пошти, документів, файлів, переданих по електронній пошті іншим особам.

- наявність на комп'ютерних пристроях інших осіб повідомлень від особи, в яких відобразилася службова інформація про електронну поштову скриньку, з якої було відправлено повідомлення або повідомлень, написаних у відповідь на повідомлення особи (при цьому часто повністю зберігається зміст вихідного повідомлення (безпосередньо або у формі посилань) і службова інформація).

Варто, особливу увагу звернути на особливості опису у протоколі НСРД вмісту електронного листування, яке становить таємницю спілкування. У такому протоколі повинні бути відображені такі відомості:

- виявлені адреси електронної пошти, по можливості - паролі до відповідних поштових скриньок;

- зміст повідомлень електронної пошти: текстова інформація, що пересилається, файли, їх реквізити (розмір, формат, дати створення і зміни, імена користувачів, які створили і змінювали їх зміст;.

- найменування організації, у власності якої знаходяться сервера, через які передавалася електронна пошта з метою подальшого зняття інформації з транспортних телекомунікаційних мереж;

- дата і час відправлення та отримання повідомлень, системні час і дата на комп'ютерному пристрої;

- наявність на комп'ютері програм для роботи з електронною поштою, наявність у вкладках, закладках, збережених сторінках і журналі відвідувань браузера відомостей про користування підозрюваним електронною поштою;

- наявність працюючих підключень до Інтернету і збережених налаштувань доступу (дротового і бездротового).

Крім того, варто погодитися з думкою, що крім стандартних процесуальних реквізитів, які необхідно заповнити під час складання протоколу про проведення НСРД, в ньому бажано фіксувати такі відомості про використання технічних засобів і пристроїв, обчислювальної техніки та програмного забезпечення: 1) точну назву технічного засобу, пристрою, обчислювальної техніки або програмного забезпечення мовою виробника; 2) серійний номер технічного засобу, пристрою, обчислювальної техніки або програмного забезпечення; 3) наявний стан зношеності або будь-яких дефектів зовнішнього вигляду чи у роботі використаного технічного засобу, пристрою, обчислювальної техніки, програмного забезпечення (визначається зовнішнім візуальним оглядом слідчого чи оперативного працівника); 4) умови, у яких було використано технічний засіб, пристрій, обчислювальну техніку або програмне забезпечення, а також дату й точний час; 5) всю інформацію в цифровому вигляді, яка представляє процесуальний або оперативний інтерес незалежно від того, на якому носії вона знаходиться, бажано оглянути в присутності спеціаліста й понятих, після чого скопіювати її на матеріальний носій, який повинен бути долучений до протоколу проведення НСРД незалежно від того, чи долучається до цього ж протоколу оригінальний носій скопійованої інформації; 6) у процесі копіювання цифрової інформації з носія на носій, наприклад, під час огляду жорсткого диску комп'ютера, необхідно користуватись програмним забезпеченням для побітового копіювання інформації (наприклад, програми «SMART», «NED», «FTK»,«dd» тощо), а після копіювання до протоколу проведення НСРД необхідно обов'язково додати копію програмного засобу, яким це копіювання було здійснено. Використання вказаних та інших вимог положень чинного КПК України слугуватиме більш ефективному застосуванню новітніх технологій у досудовому розслідуванні, зокрема під час проведення негласних слідчих (розшукових) дій, а також під час їх

оформлення як слідчими, так і працівниками оперативних підрозділів, що виконують такі дії за їх дорученням [189, с. 92 - 93].

Якщо вилучення всієї комп'ютерної техніки видається недоцільним, інформація яка має значення для кримінального провадження може бути скопійована. Копіювання електронної інформації в даному випадку може розглядатися як пізнавальний тактичний прийом, що виконується в межах проведення зняття інформації з електронних інформаційних систем, обшуку. Копіювання електронної інформації становить собою специфічну з точки зору криміналістики операцію. Так, при вилученні, наприклад, з місця події сліду пальця руки на дактилоскопічну плівку відбувається повне перенесення сліду на інший об'єкт, тобто слід продовжує своє існування, але вже в іншому місці. При вилученні ж комп'ютерної інформації відбувається не перенесення інформації а її дуплікація, копіювання. Тобто першоджерело інформації залишається в початковому стані, проте слідство отримує нову доказову інформацію. При копіюванні такої інформації відбувається її переміщення на інший цифровий носій наприклад, зовнішній жорсткий диск, флеш-накопичувач або оптичний диск. Оптимальним варіантом копіювання є створити образ логічного диска, на якому розташована потрібна інформація. У такому випадку не відбувається порушення файлової системи, образ може бути неодноразово скопійований і досліджений в рамках окремих слідчих дій або в ході проведення судової експертизи.

У разі якщо смартфон заблокований, бажано скористатися методами, які не несуть ризику руйнування або пошкодження інформації, що знаходиться на мобільному пристрої. Вкрай бажано домогтися співпраці з власником пристрою, щоб він розблокував смартфон. Альтернативою може стати застосування фахівцем програмно-апаратних засобів, таких як, наприклад, UFED Touch, що дозволяє на фізичному рівні витягувати навіть із заблокованого телефону дані, в тому числі неушкоджені і віддалені паролі, встановлені додатки, географічні теги, інформацію про місцезнаходження, фото і відео користувача.

Концептуально цей пристрій розділений на дві частини:

- фірмовий планшет Cellebrite UFED Touch 2 (або UFED 4PC – програмний аналог Cellebrite UFED Touch 2, що встановлюється на комп’ютер або ноутбук фахівця): використовуються тільки для отримання даних;
- UFED Physical Analyzer – програмна частина, призначена для аналізу даних, витягнутих із мобільних пристроїв. Концепція використання обладнання передбачає, що за допомогою Cellebrite UFED Touch 2 фахівець отримує дані в польових умовах, а потім у лабораторії здійснює їх аналіз за допомогою UFED Physical Analyzer [59, 125].

При вилученні мобільного пристрою бажано ізолювати його від мобільного з’єднання шляхом виключення пристрою або за допомогою спеціальних пристроїв, що глушать зв'язок, всі необхідні процедури повинні проводитися в спеціально обладнаному приміщенні. Пристрій повинен бути повністю зарядженим з метою запобігання втрати інформації при проведенні процесуальних дій.

В іншому випадку при проведенні слідчої дії відбувається вилучення інформації з довготривалої пам'яті або sim- карт, встановлених в мобільний термінал. Копіюванню підлягає не тільки змістовна інформація але й операційна система пристрою, включаючи всю файлову систему [148, с. 267].

При вивченні надісланих або отриманих повідомлень в протоколі вказуються вид повідомлення (вхідне чи вихідне), абонентський номер (або логін) відправника і одержувача, дата, час надсилання та отримання, перші слова тексту, останні фрази; дослівно фіксуються ті повідомлення, які, на думку слідчого, мають значення для даного кримінального провадження. При огляді текстів повідомлень основний акцент здійснюється на вивченні змістовної сторони даних об'єктів, однак варто також звертати увагу на використані автором в тексті скорочення, вигуки, жаргони, малюнки, на особливості розташування слів у реченні, що в подальшому дозволить

провести більш глибокий аналіз змісту повідомлення і зібрати відомості про його автора [52, с. 72].

Здобуті в результаті проведення негласних заходів отримання доказової інформації відомості стосуються таємниці досудового розслідування, а також відповідних видів таємної інформації у сфері приватного та особистого життя громадян. Незаконне і безпідставне їх розголошення може створити загрозу не лише національним інтересам та безпеці держави, а й її громадян. З огляду на це така інформація підлягає засекречуванню відповідно до Закону України «Про державну таємницю» та з урахуванням Зводу відомостей, що становлять державну таємницю, належить до секретної інформації (статті 4.12.3, 4.12.4) [85].

До документів, які підлягають збереженню під час проведення негласних слідчих (розшукових) дій, належать: постанова слідчого, прокурора про проведення негласної слідчої (розшукової) дії; клопотання про дозвіл на проведення негласної слідчої (розшукової) дії; ухвала слідчого судді про дозвіл на проведення негласної слідчої (розшукової) дії; протокол про проведення негласної слідчої (розшукової) дії; додатки до протоколу про проведення негласної слідчої (розшукової) дії (спеціально виготовлені копії; зразки об’єктів, речей і документів; письмові пояснення спеціалістів, які брали участь у проведенні відповідної дії; стенограма, аудіо-, відеозаписи; фототаблиці; схеми, зліпки; носії комп’ютерної інформації та інші матеріали, які пов’язані зі змістом протоколу); інші документи, що містять відомості про методи отримання таємної інформації негласним шляхом, та ті, які містять інформацію, що дає змогу ідентифікувати особу, місце або річ, щодо якої проводиться або планується проведення негласних слідчих (розшукових) дій [83, с. 80].

ВИСНОВКИ до Розділу 3

1. В юридичній літературі англійський термін «digital evidence» трактується по різному, одні автори перекладають його як «електронні докази», інші як «цифрові докази» вкладаючи різний зміст у це поняття, або ототожнюючи дані терміни. Вважаємо за більш доцільне використовувати термін «цифрові докази», який відображає природу створення даних доказів.

2. Під час проведення процесуальних дій спрямованих на обмеження таємниці спілкування органи досудового розслідування отримують різноманітні джерела доказів, однак враховуючи специфіку процесуальних дій, які у більшості випадків пов’язані із отриманням інформації із транспортних телекомунікаційних мереж та електронних інформаційних систем, слідчому доводиться мати справу із великим обсягом інформації розміщеної на матеріальних носіях інформації.

За своєю правовою природою така інформація згідно з п. 1 ч. 2 ст. 99 КПК визнається документом. Чинний КПК не встановлює спеціальних вимог до форми, змісту та процесуального порядку долучення електронних документів, що потребує внесення змін в КПК щодо запровадження інституту цифрових доказів у кримінальне провадження. Водночас, у більшості країн світу давно розробляється концепція використання цифрових (електронних) доказів.

3. Відмінність електронних носіїв інформації від «традиційних» речових доказів та інших документів призводить до необхідності використовувати різні прийоми і засоби роботи з зазначеними доказами. «Предметні» речові докази містять в якості доказової інформації сліди матеріального світу. Зміна цієї інформації неможлива без безпосереднього впливу на сам предмет. Тому для гарантування їх достовірності цілком достатньо традиційної упаковки, що забезпечує відсутність механічного впливу. Стверджувати це ж щодо електронних носіїв інформації неможливо. Тому вимога застосування спеціальних засобів, що виключають

дистанційний вплив на них, є обов'язковою вимогою під час їх огляду та вилучення.

4. Встановлення наявності адреси електронної пошти і навіть її змісту саме по собі не може бути доказом того, що ця адреса електронної пошти належить конкретній особі. Після встановлення скриньки електронної пошти, прив'язаної до адреси електронної пошти, необхідно встановити, хто користувався цією скринькою і, отже, є власником адреси електронної пошти. Відомості такого роду можуть бути отримані в ході тимчасового доступу до речей і документів, обшуків, зняття інформації з транспортних телекомунікаційних мереж і електронних інформаційних систем.

ВИСНОВКИ

У дисертації здійснено теоретичне узагальнення та запропоновано нове вирішення наукового завдання, що виявляється у отриманні нових знань щодо змісту таємниці спілкування та способів її обмеження у кримінальному провадженні. Відтак сформульовано низку висновків, пропозицій і рекомендацій, спрямованих на досягнення поставленої мети, а саме:

1. Таємниця спілкування полягає у недопущенні розголошення інформації, яка передається особами під час листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування за умови, що особи бажають її зберегти в таємниці.

2. Складовими таємниці спілкування є:

- таємниця листування;
- таємниця телефонних розмов;
- таємниця телеграфної кореспонденції;
- таємниця іншої кореспонденції;
- таємниця інших форм спілкування.

3. Систему процесуальних дій, спрямованих на обмеження таємниці спілкування становлять наступні.

Зокрема, на підставі ухвали слідчого судді суду першої інстанції проводяться наступні процесуальні дії спрямовані на обмеження таємниці спілкування:

- тимчасовий доступ до речей та документів;

- обшук.

На підставі ухвали слідчого судді апеляційного суду, слідчого судді Вищого антикорупційного суду проводяться такі негласні слідчі (розшукові) дії:

– аудіо-, відеоконтроль особи;

- накладення арешту на кореспонденцію, огляд і виїмка кореспонденції;
- зняття інформації з транспортних телекомунікаційних мереж;

- зняття інформації з електронних інформаційних систем;
- спостереження за особою;
- аудіо-, відеоконтроль місця.

4. В ході обстеження публічно недоступних місць, житла чи іншого володіння особи слідчий, працівники оперативних підрозділів не мають права втручатися у таємницю спілкування, зокрема у особисте листування особи, інші форми спілкування зафіксовані на матеріальних чи електронних носіях, які знаходяться в публічно недоступних місць, житлі чи іншому володіння особи. Така позиція зумовлено змістом даної НСРД, яка в основному носить організаційно-допоміжний характер.

5. З метою вирішення питання про можливі порушення прав людини оперативними підрозділами під час проведення НСРД у зв'язку з відсутністю належного судового контролю та прокурорського нагляду в ході їх здійснення пропонується запровадження інституту залучення особи, яка під час судового розгляду клопотань про НСРД буде забезпечувати дотримання прав осіб щодо яких будуть застосовуватися обмеження. В зв'язку з цим, пропонуємо викласти ч. 1 ст. 261 КПК в наступній редакції «Слідчий суддя зобов'язаний розглянути клопотання про надання дозволу на проведення негласної слідчої (розшукової) дії протягом шести годин з моменту його отримання. Розгляд клопотання здійснюється за участю особи, яка подала клопотання та адвоката делегованого центром безоплатної правової допомоги». Такий адвокат, повинен мати допуск до державної таємниці, а доступ до матеріалів клопотання про надання дозволу на проведення НСРД буде надаватися слідчим суддею перед його судовим розглядом.

6. У зв'язку з неоднозначністю застосування норм КПК щодо отримання інформації, яка містить таємницю спілкування та знаходиться в електронних інформаційних системах потрібно закріпити окрему слідчу дію, як різновид слідчого огляду – огляд електронної інформаційної системи. Такий огляд проводиться щодо електронних інформаційних систем, які вилучені в ході інших слідчих дій та здійснюється на підставі ухвали

слідчого судді місцевого суду.

7. Доцільним є долучення до клопотання про тимчасовий доступ до речей та документів, що знаходяться в операторів та провайдерів телекомунікацій, матеріалів радіотехнічної розвідки, які дозволяють додатково ідентифікувати базові станції через які здійснювали спілкування підозрювані, а отже обмежити порушення таємниці спілкування невизначеної кількості абонентів.

8. За своїм характером і аудіо-, відеоконтроль особи і місця мають на меті обмеження таємниці спілкування, та спрямовані на отримання доказової інформації, яка міститься в розмовах, рухах чи діях особи. Однак, якщо під час аудіо-, відеоконтролю особи нас цікавить конкретна особа, яка підозрюється у вчиненні кримінального правопорушення, то під час аудіо-, відеоконтролю місця коло осіб невизначене, в зв'язку з цим обмежується таємниця спілкування невизначеного кола осіб.

9. Вважаємо за доцільне розширити сферу НСРД - арешт, огляд і виїмка кореспонденції і зокрема передбачити в ході її проведення право відшуковувати поштово-телеграфну кореспонденцію, на яку необхідно накладати арешт. Така кореспонденція може відшуковуватися за почерком, за виглядом упаковки, місцем відправки чи одержання тощо.

10. Під час проведення процесуальних дій спрямованих на обмеження таємниці спілкування органи досудового розслідування отримують різноманітні джерела доказів, однак враховуючи специфіку процесуальних дій, які у більшості випадків пов'язані із отриманням інформації із транспортних телекомунікаційних мереж та електронних інформаційних систем, слідчому доводиться мати справу із великим обсягом інформації розміщеної на матеріальних носіях інформації.

За своєю правовою природою така інформація згідно з п. 1 ч. 2 ст. 99 КПК визнається документом. Чинний КПК не встановлює спеціальних вимог до форми, змісту та процесуального порядку долучення електронних документів, що потребує внесення змін в КПК щодо запровадження

інституту цифрових доказів у кримінальне провадження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Abdelhameed A.M., Hassan K.H. Modern Means of Evidence Collection and their Effects on the Accused Privacy. *The US Law. Journal of Politics and Law.* 2019. Vol. 12, № 1. P. 85 - 97.

2. Anti-Cartel Enforcement Manual: Chapter on Digital Evidence Gathering. ICN Cartel Working Group, 2014. URL: https://www.internationalcompetitionnetwork.org/wp-content/uploads/2018/05/CWG_ACEMDigitalEvidence.pdf (Last accessed: 11.12.2019).

3. Banisar D., Davies S. Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. *Journal of Computer & Information Law.* 1999. Vol. 18, № 1. 112 p.

4. Bloustein E. J. Privacy as an Aspect of Human Dignity : An Answer to Dean Prosser / ed. Schoeman F. D. *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press, 1984. P. 156–202.

5. Case of Bosphorus Hava Yollari Turizm Ve Ticaret Anonim Sirketi v. Ireland (Application no. 45036/98): Judgment European Court of Human Rights (Grand Chamber), 30 June 2005. URL: http://hudoc.echr.coe.int/eng?i=001-69564 (Last accessed: 12.08.2019).

6. Case of Baranowski v. Poland (Application no. 28358/95): Judgment European Court of Human Rights (Firts Section), 28 March.2000. URL: http://hudoc.echr.coe.int/eng?i=001-58525 (Last accessed: 21.11.2020).

7. Case of Belyaev and Digtyar v. Ukraine (Application no. 16984/04): Judgment European Court of Human Rights (Firts Section), 16 February 2012. URL: http://hudoc.echr.coe.int/eng?i=001-109122 (Last accessed: 13.12.2020).

8. Case of Copland v. United Kingdom (Application no. 62617/00): Judgment European Court of Human Rights, 03 April 2007. URL: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-117767&filename=001-117767.pdf&TID=ihgdqbxnfi (Last accessed: 19.12.2020).

9. Case of Domenichini v. Italy (Application no. 15943/90): Judgment European Court of Human Rights (Chamber), 15 November 1996. URL: http://hudoc.echr.coe.int/eng?i=001-58073 (Last accessed: 12.11.2020).

10. Case of Dudgeon v. The United Kingdom (Application no. 7525/76): Judgment European Court of Human Rights (Chamber), 24 February 1982. URL: http://hudoc.echr.coe.int/eng?i=001-57472 (Last accessed: 03.05.2019).

11. Case of Halford v. The United Kingdom (Application no. 20605/92): Judgment European Court of Human Rights (Chamber), 25 June 1997. URL: http://hudoc.echr.coe.int/eng?i=001-58039 (Last accessed: 27.09.2019).

12. Case of Katz v. United States: Supreme Court of the United States, 1967. URL: https://tile.loc.gov/storage-services/service/ll/usrep/usrep389/usrep389347/usrep389347.pdf (Last accessed: 28.10.2020).

13. Case of Lyashko v. Ukraine (Application no. 21040/02): Judgment European Court of Human Rights (First Section), 10 August 2006. URL: http://hudoc.echr.coe.int/eng?i=001-76714 (Last accessed: 23.11.2020).

14. Case of Niedbała v. Poland (Application no. 27915/95): Judgment European Court of Human Rights (First Section), 04 July 2000. URL: http://hudoc.echr.coe.int/eng?i=001-58739 (Last accessed: 11.05.2019).

15. Case of Niemietz v. Germany (Application no. 13710/88): Judgment European Court of Human Rights (Chamber), 16 December 1992. URL: http://hudoc.echr.coe.int/eng?i=001-57887 (Last accessed: 12.08.2019).

16. Case of P. G. and J. H. v. The United Kingdom (Application no. 44787/98): Judgment European Court of Human Rights, 25 September 2001. URL: http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-59665&filename=001-59665.pdf (Last accessed: 03.12.2019).

17. Case of Popescu v. Romania (Application no. 71525/01): Judgment European Court of Human Rights, 26 April 2007. URL: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-1995439-2103500&filename=003-1995439-2103500.pdf (Last accessed: 29.11.2020).

18. Case of Sałapa v. Poland (Application no. 35489/97): Judgment European Court of Human Rights (Third Section), 19 December 2002. URL: http://hudoc.echr.coe.int/eng?i=001-60854 (Last accessed: 22.08.2019).

19. Case of Silver and others v. The United Kingdom (Application no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75): Judgment European Court of Human Rights (Chamber), 25 March 1983. URL: http://hudoc.echr.coe.int/eng?i=001-57577 (Last accessed: 11.02.2019).

20. Case of Von Hannover v. Germany (Application no. 59320/00): Judgment European Court of Human Rights (Third Section), 24 June 2004. URL: http://hudoc.echr.coe.int/eng?i=001-61853 (Last accessed: 12.08.2019).

21. Case of Z v. Finland (Application no. 2209/93): Judgment European Court of Human Rights (Chamber), 25 February 1997. URL: http://hudoc.echr.coe.int/eng?i=001-58033 (Last accessed: 19.11.2019).

22. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet. New York; London: Academic Press is an imprint of Elsevier, 2011. 837 p.

23. Constitution of the German Democratic Republic as published on 7 October 1949. URL: https://www.cvce.eu/obj/constitution_of_the_german_democratic_republic_7_october_1949-en-33cc8de2-3cff-4102-b524-c1648172a838.html (Last accessed: 27.11.2020).

24. Cortez E. K. Data Protection Around the World. *Privacy laws in action*. T.M.C. Asser Press. 2021. Vol. 33, № 1. 279 p.

25. DeCew J. W. The Conceptual Coherence of Privacy as Developed in Law. *Core Concepts and Contemporary Issues in Privacy*. / Cudd A. E., Navin M. C. Springer International Publishing AG. 2018. Vol. 8, № 1. P. 17 - 31.

26. Digital Evidence: Standards and Principles. *Forensic Sciennce Communications*. 2000. Vol. 2, № 2. URL: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm (Last accessed: 02.12.2019).

27. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. OJ L 119, 4.5. 2016. P 89 - 131.

28. Electronic Communications Privacy Act (ECPA): 1986. URL: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 (Last accessed: 12.11.2020).

29. Explanations relating to the Charter of Fundamental Rights. Special edition in Croatian: Chapter 01. *Official Journal of the European Union*. 2007. Vol. 007. P. 17 - 35. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32007X1214%2801%29 (Last accessed: 13.11.2019).

30. Federal Constitution of the Swiss Confederation of 18 April 1999. URL: https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/1999/404/20210101/en/pdf-a/fedlex-data-admin-ch-eli-cc-1999-404-20210101-en-pdf-a.pdf (Last accessed: 26.11.2020).

31. German Code of Criminal Procedure as published on 7 April 1987. Federal Law Gazette. URL: https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html (Last accessed: 11.12.2020).

32. Hijmans H. Privacy and Data Protection as Values of the EU That Matter, Also in the Information Society. *The European Union as Guardian of Internet Privacy*. Springer International Publishing, 2016. Vol. 31, № 1. P. 17 - 75.

33. Horowitz I. L. Privacy, Publicity and Security: the American Context: Privacy is not Only a Right but Also an Obligation. *EMBO reportsm* 2006. № 7. P. 40-44 p.

34. IT-Glossaiy. URL: https://www.gartner.com/it-glossary/imei-

international-mobile-equip- ment-identifier (Last accessed: 21.12.2020).

35. Kostoris R. E. Handbook of European Criminal Procedure. Springer International Publishing AG, 2018. 445 p.

36. Lee S. P. The nature and value of privacy. *Core Concepts and Contemporary Issues in Privacy* / Cudd A. E., Navin M. C. Springer International Publishing AG. 2018. Vol. 8, № 1. P. 47 - 63.

37. Moore A. D. Privacy: Its Meaning and Value. *American Philosophical Quarterly*. 2003. Vol. 40, № 3. P. 215 – 227.

38. Murgio D. Telephone Tapping in International Law and Seven European Countries. The Helsinki Foundation for Human Rights. Warsaw, Poland, 1996. 96 p.

39. Post R. C. Three Concepts of Privacy. *The Georgetown law journal.* 2001. Vol. 89. P. 2087-2098.

40. Privacy Act of 1974, as amended, 5 U.S.C. § 552a. The United States Department of Justice. Office of Privacy and Civil Liberties. URL: https://www.justice.gov/opcl/privacy-act-1974 (Last accessed: 12.08.2019)

41. Prosser W. R. Privacy. Philosophical Dimensions of Privacy: An Anthology / Ed. F. Schoeman. Cambridge: Cambridge University Press, 1984. P. 104–155.

42. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf (Last accessed: 24.11.2019).

43. Summaries of EU court decisions relating to data protection 2000-2015 prepared by Laraine Laudati, Olaf data protection officer. 2016. 61 p. URL: https://ec.europa.eu/anti-fraud/sites/default/files/caselaw_2001_2015_en.pdf (Last accessed: 27.19.2020).

44. The Bill of rights, 15 December 1791. URL:

https://www.archives.gov/files/legislative/resources/education/bill-of-rights/images/handout-3.pdf (Last accessed: 23.11.2019).

45. The Constitution of the United States of America, 17 September 1787. URL: https://www.gpo.gov/fdsys/pkg/CDOC-110hdoc50/pdf/CDOC-110hdoc50.pdf (Last accessed: 19.01.2021).

46. US Code Title 18 Chapter 119 - Wire and Electronic Communications Interception and Interception of Oral Communications. The United States Department of Justice. URL: https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter119&edition=prelim (Last accessed: 12.10.2020).

47. Адигамова Г.З., Назмутдинова А.Т. Технологии связи в уголовном судопроизводстве. *Пробелы в российском законодательстве*. 2014. № 6. С. 213 - 216.

48. Алєксєєва-Процюк Д. О. Особливості проведення тимчасового доступу до речей та документів для отримання інформації від операторів мобільного зв'язку. *Митна справа.* 2013. № 6. С. 58 - 65.

49. Американська конвенція про права людини від 22 листопада 1969 р. URL: https://constituanta.blogspot.com/2011/02/1969.html (Last accessed: 00.00.2019).

50. Амирханов Б. К. Понятие негласных следственных действий и их соотношение с розыскными мерами. *Қазақстан Республикасы Заңнама институтының жаршысы.* 2016. № 3 (44). С. 98 - 105.

51. Арабська хартія прав людини від 14 вересня 1994р. URL: http://www1.umn.edu/humanrts/instree/arabcharter.html (Last accessed: 00.00.2019).

52. Архипова Н.А. Организационно-тактические особенности получения и использования содержания текстовых сообщении в процессе раскрытия и расследования преступлений. *Известия Алтайского государственного ун-та*. 2012. № 2. С. 71 - 73.

53. Асылханов К. Ж.. К вопросу охраны прав на

неприкосновенность частной жизни в междуанродно-правовых документах и в законодательстве зарубежних стран. *Весник Института законодательства Республики Казахстан.* 2010. № 3 (19). С. 187 - 192.

54. Бабкова В. С. Проблеми визнання результатів зняття інформації з транспортних телекомунікаційних мереж належними та допустимими доказами. *Юрист України.* 2018. № 2. С. 68 - 75.

55. Багрій М. В., Луцик В. В. Процесуальні аспекти негласного отримання інформації: вітчизняний та зарубіжний досвід: монографія. Харків: Право, 2017. 376 с.

56. Бараненко Б. І. Негласні слідчі (розшукові) дії та особливості їх проведення оперативними підрозділами органів внутрішніх справ: навч.-практ. посіб. / за ред. А. В. Іщенка, Б. І. Бараненка. Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2014. 416 с.

57. Беляева Н. Г. Право на неприкосновенность частной жизни: международно-правовое и внутригосударственное регулирование. *Российский юридический журнал.* 2000. № 1 (25). С. 38 - 44.

58. Білічак О. А. Втручання у приватне спілкування за кримінальним процесуальним законодавством України. *Слово Національної школи суддів України.* 2018. № 2. С. 94 - 110.

59. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 255 с.

60. Бойкле В. Уголовно-процессуальное право ФРГ: учебник. 6-е изд., с доп. и изм.: пер. с нем. Я.М. Плошкиной / под ред. Л. В. Майоровой. Красноярск, 2004. 352 с.

61. Вегера-Іжевська І. В. Забезпечення права на недоторканність житла чи іншого володіння особи в кримінальному провадженні: монографія. Харків : Право, 2019. 232 с.

62. Вехов В. Б. Электронные доказательства: проблемы теории и практики. *Правопорядок: история, теория, практика*. 2016. № 4 (11). С. 46 -

50.

63. Використання можливостей операторів стільникового (мобільного) зв'язку для розкриття та розслідування злочинів: метод. рек. / Чернявський С. С., Татаров О. Ю. , Алексеєва-Процюк Д. О. та ін. Київ: Нац. акад. внутр. Справ, 2012. 58 с.

64. Вирок Дарницького районного суду м. Києва від 28. жовтня 2019 р., судова справа № 753/16804/17. URL: https://reyestr.court.gov.ua/Review/85223497 (дата звернення: 11.01.2021).

65. Вирок Печерського районного суду м. Києва від 7 травня 2018 р., судова справа № 756/7676/17-к. URL: https://reyestr.court.gov.ua/Review/73948517 (дата звернення: 11.01.2021).

66. Гарасимів О.Ю. Вплив практики Європейського Суду з прав людини на вдосконалення правозахисного законодавства в Україні (загальнотеоретичний аспект): дис. … канд. юрид. наук: 12.00.01 / Львівський національний університет імені І. Франка. Львів, 2020. 281 с.

67. Гловюк І. В. Розгляд слідчим суддею клопотання про тимчасовий доступ до речей і документів. *Актуальні питання досудового розслідування слідчими органів внутрішніх справ: проблеми теорії та практики*: матеріали всеукр. наук.-практ. конф. (м.Дніпропетровськ, 18-19 квітня 2013р.). Київ: Хай-Тек Прес, 2013. С. 52 - 56.

68. Говорун В. В. Організаційно-правові гарантії непорушності (недоторканності) права громадян на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. *Правові новели*. 2018. № 6. С. 65 - 71.

69. Говоруха В. І., Степанов В. А. Зняття інформації з електронних інформаційних систем як різновид негласних слідчих (розшукових) дій. *Інформація і право*. 2020. № 3. С. 69 - 74.

70. Головненков П., Спица Н. Уголовно-процессуальный кодекс Федеративной республики Германия – Strafprozessordnung (StPO): науч.-практ. коммент. и пер. текста закона. Потсдам: университет Потсдама, 2012.

405 с.

71. Гольдберг Н. О. Забезпечення конституційних прав і свобод особи при проведенні негласних слідчих (розшукових) дій у її житлі та іншому володінні. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2016. № 74. С. 47-58.

72. Горпинюк О. П. Застосування стандартів Конвенції про захист прав людини і основоположних свобод у кримінальних провадженнях в Україні: навч.-метод. посіб. Львів: ЛьвДУВС, 2020. 224 с.

73. Григорьев В. Н., Максимов О. А. Некоторые вопросы использования электронных носителей информации при расследовании уголовных дел. *Полицейская деятельность.* 2018. № 1. С 1 - 8.

74. Грібов М. Л. Удосконалення термінологічного апарату глави 21 Кримінального процесуального кодексу України. *Юридичний часопис Національної академії внутрішніх справ.* 2017. № 1. С. 238-249.

75. Гумін О. М. Особливості тимчасового доступу до речей і документів, які містять інформацію про надання телекомунікаційних послуг. *Митна справа.* 2013. № 6. С. 53 - 57.

76. Директива 95/46/ЄС Європейського Парламенту і Ради "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" від 24 жовтня 1995 р. URL: hhttps://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення: 23.11.2019).

77. Дунаева М. С. Право на неприкосновенность частной жизни граждан и его содержание в уголовном судопроизводстве: исторический и сравнительно-правовой анализ. *Вестник ИрГТУ. Гуманитарные науки*. №3 (50). 2011. С. 207 - 211.

78. Ермолович Г. П. Население и полиция: противостояние преступности в США: монография. Санкт-Петербург: Фонд поддержки науки и образов. в обл. правоох. деят. 2004. 284 с.

79. Ємчук Л. В. Конституційно-правове регулювання особистого та

сімейного життя людини і громадянина: дис. … канд. юрид. наук: 12.00.02 / ДВНЗ “Ужгородський національний університет”. Ужгород, 2015. 225 с.

80. Єськов С. В. Аудіо-, відеоконтроль особи як різновид втручання у приватне спілкування : системно-структурний аналіз. URL: www.corp-lguvd.lg.ua/d130203.html (дата звернення: 11.12.2019).

81. Єськов С. В. Втручання у приватне спілкування: вітчизняний досвід регламентації у світлі резолюцій, конвенцій та стандартів Організації Об’єднаних Націй. *Наукові записки Інституту законодавства Верховної Ради України.* 2014. № 2. С. 107 - 113.

82. Єськов С. В. Втручання у приватне спілкування як елемент системи негласних слідчих (розшукових) дій. *Науковий вісник Львівського державного університету внутрішніх справ*. 2013. № 2. С. 264 - 274.

83. Єфіменко І. Порядок збереження інформації, отриманої в результаті проведення негласних слідчих (розшукових) дій . *Вісник Національної академії прокуратури України.* 2015. № 4. С. 78 - 83.

84. Загальна декларація прав людини. URL: http://zakon2.rada.gov.ua/laws/show/995_015 (дата звернення: 12.11.2019).

85. Звід відомостей, що становлять державну таємницю: затв. наказом Служби безпеки України від 23.12.2020 р. № 383. URL: https://zakon.rada.gov.ua/laws/show/z0052-21#n7 (дата звернення: 13.12.2019).

86. Зуев С.В. Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С.В. Зуева. Москва: Юрлитинформ, 2019. 400 с.

87. Іскендеров Е. Ф. Зняття інформації з транспортних телекомунікаційних мереж як засіб отримання доказів оперативними підрозділами. *Вісник кримінального судочинства.* 2016. № 4. С. 33-39.

88. Климкевич Р. А. Проблеми захисту персональних даних у кримінальному процесі. Українська модель кримінальної юстиції: блукаючи задзеркаллям. *VI Львівський форум кримінальної юстиції:* збірник матеріалів наук.-прак. конф. (Львів, 17–18 вересня 2020 року). Львів: ЛьвДУВС, 2020. С.

49 - 53.

89. Ковалёв Н. Судебный контроль на этапе досудебного производства в уголовном процессе Узбекистана. Управления ООН по наркотикам и преступности. Ташкент, 2020. 28 с.

90. Коваль А. А. Негласні слідчі (розшукові) дії в аспекті проблем юридичної техніки. *Вісник Південного регіонального центру Національної академії правових наук України*. 2018. № 17. С. 196 - 202.

91. Колесник В. А. Втручання в приватне спілкування і забезпечення прав особи під час проведення негласних слідчих (розшукових) дій. *Вісник Академії адвокатури України.* 2014. № 3. С. 37 - 44.

92. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. URL: http://zakon2. rada.gov.ua/laws/show/994_326 (дата звернення: 13.02.2019).

93. Конвенція про захист прав людини і основоположних свобод. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 24.05.2019).

94. Консолідовані версії Договору про Європейський Союз та Договору про функціонування Європейського Союзу (2010/С 83/01). URL: http://zakon5.rada.gov.ua/laws/show/994_b06 (дата звернення: 28.11.2019).

95. Конституции государств Европейского Союза / под общ. ред. Л.А. Окунькова. Москва: НОРМА, 1999. 816 с.

96. Конституция Республики Казахстан от 30 августа 1995 года (с изменениями и дополнениями по состоянию на 23.03.2019 г.). URL: http: https://online.zakon.kz/document/?doc_id=1005029 (дата обращения: 11.12.2019).

97. Конституция Республики Узбекистан от 8 декабря 1992 года (с изменениями и дополнениями на 08.02.2021). URL: https://online.zakon.kz/Document/?doc_id=30433237#pos=204;-54 (дата обращения: 11.12.2019).

98. Коровайко О. І. Реалізація у кримінальному судочинстві України

міжнародних стандартів права особи на повагу до приватного і сімейного життя. *Форум права.* 2017. № 1. С 77 - 83.

99. Корчагин А. А. Обнаружение, фиксация и изъятие файлов и их фрагментов на электронных устройствах, их доказательственное значение. Электронные носители информации в криминалистике: монография / под ред. докт. юрид. наук. О.С. Кучина. Москва, 2017. 219 с.

100. Кримінальне провадження №120181140000000196. Архів ГУНП у Львівській області.

101. Кримінальне провадження №12017140040000720. Архів ГУНП у Львівській області.

102. Кримінальний процес : підручник / за ред.: Ю. М. Грошевий, В. Я. Тацій, А.Р. Туманянц та ін.; за заг. ред. В.Я. Тація, Ю.М. Грошевого, О.В. Капліної, О.Г. Шило. Харків: Право, 2013. 824 с.

103. Кримінальний процес України: наук.-практ. комент. / за заг. ред. проф. В. Г. Гончаренка, В. Т. Нора, М. Є. Шумила. Київ: Юстініан, 2012. 1223 с.

104. Кримінальний процесуальний кодекс України: наук.-практ. комент. / відп. ред. С. В. Ківалов, С. М. Міщенко, В. Ю. Захарченко. Харків: Одіссей, 2013. 1104 с.

105. Крицька І. О. Речові докази та цифрова інформація: поняття та співвідношення. *Часопис Київського університету права.* 2016. № 1. С. 301 - 305.

106. Кряковцев С. М. Дотримання особистих прав людини в процесі зняття інформації з транспортних телекомунікаційних мереж. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка.* 2014. №. 2. С. 291 - 299.

107. Куцій М. С. Сучасні комунікаційні технології для посередницького зв'язку в конфіденційному співробітництві. *Науковий вісник Херсонського державного університету.* 2016. №2. С. 83 - 89.

108. Кучинська О. П Принципи кримінального провадження у світлі

практики Європейського суду з прав людини: монографія. Ніжин: Аспект-Поліграф, 2013. 228 с.

109. Лисюк Ю. В. Аудіо- та відеоконтроль як різновиди втручання в приватне спілкування під час здійснення негласних слідчих дій у кримінальному провадженні. *Актуальні проблеми держави і права: зб. наук. пр.* 2013. №. 70. С. 335 - 339.

110. Лук'янчиков Є. Д. Визначення та система негласних слідчих (розшукових) дій. *Часопис Національного університету "Острозька академія"*. 2014. №1. URL http://lj.oa.edu.ua/articles/2014/ n1/14lydsrd.pdf (дата звернення: 11.12.2020).

111. Луцик В. В. Зняття інформації з електронних інформаційних систем. *Вісник Чернівецького факультету Національного університету "Одеська юридична академія".* 2014. №4. С. 222 - 230.

112. Луцик В. В., Савченко В.А., Самарін В.І. Сучасний кримінальний процес країн Європи: монографія. Харків: Право, 2018. 792 с.

113. Мачковский Л. Г. Охрана личных, политических и трудовых прав в уголовном законодательстве России и зарубежных государств. Москва: РУССО. 2004. 304 с.

114. Меживой О. В. Правова кваліфікація та регламентація зняття інформації з транспортних телекомунікаційних мереж за новим КПК України. *Вісник Донецького національного університету.* 2013. № 1. С. 229 - 233.

115. Митин Е. В. Право на тайну сообщений, передаваемых по электронным почтовым ящикам: проблемы реализации. *Теория и практика общественного развития*. 2012. № 2. С. 271 - 273.

116. Мишин А. А., Власихин В. А. Конституция США: Политико-правовой комментарий. Москва: Международные отношения, 1985. 334 с.

117. Міжнародний пакт про громадянські і політичні права. URL: http://zakon2.rada.gov.ua/laws/show/995043 (дата звернення: 15.12.2019).

118. Морквін Д. А. Співвідношення негласного проникнення до житла

особи та негласного обстеження житла особи. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2016. № 3. С. 265 - 271.

119. Мухін В. Державне втручання у приватне спілкування: процесуальні аспекти. *Вісник Національної академії прокуратури України.* 2014. № 1. С. 90 - 97.

120. Нагребельний В. П. Телеграфний зв'язок. Юридична енциклопедія: у 6 т. / ред. кол. Шемшученко Ю. С. та ін. Київ: Українська енциклопедія, 2004. 768 с.

121. Науково-практичний коментар до Кримінального процесуального кодексу України від 13 квітня 2012 року / за ред. О. А. Банчука, Р.О. Куйбіди, М. І. Хавронюка. – Харків: Фактор, 2013. 1058 с.

122. Негласні слідчі (розшукові) дії та використання результатів оперативно-розшукової діяльності у кримінальному провадженні: навч.-практ. посіб. / Кудінов С. С., Шехавцов Р. М., Дроздов О. М., Гриненко С. О. Харків: Оберіг, 2013. 344 с.

123. Негодченко О. В. Таємниця кореспонденції, листування, телефонних розмов та спілкування в сучасних умовах: реалії та колізії. *Право і суспільство*. 2013. № 4. С. 55 - 61.

124. Нодиров М. А. Сравнительный анализ законов об оперативно-розыскной деятельности стран Содружества Независимых Государств. *Отечественная юриспруденция*. 2019. № 7 (39). С. 53 - 58.

125. Олашин М. М. Кримінальні процесуальні аспекти зняття інформації з електронних інформаційних систем. *Вісник Львівського торговельно-економічного університету. Юридичні науки.* 2018. № 7. С. 233 - 242.

126. Орлов Ю. Ю. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ.* 2017. № 1. С. 12 -24.

127. Панкевич О. З. Філософсько-правові засади обмежування прав

людини у міжнародно-правових та конституційних актах. *Науковий вісник Львівського державного університету внутрішніх справ*. Львів: ЛьвДУВС. 2016. № 1. С. 373 - 383.

128. Погорецький М., Старенький О. Негласні слідчі (розшукові) дії як засоби отримання доказів: окремі проблемні питання. *Право України.* 2018. №8. С. 85-106.

129. Посібник за статтею 8 Конвенції про захист прав людини та основоположних свобод. Право на повагу до приватного і сімейного життя / перекл. з доповненнями адвокатів, кандидатів юридичних наук О. Дроздова, О. Дроздової. Рада Європи. 2020. 83 с. URL: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf (дата звернення: 07.09.2020).

130. Постанова Великої палати Верховного суду від 16 жовтня 2019 р., судова справа № 640/6847/15-к (провадження № 13-43кс19). URL: .https://reyestr.court.gov.ua/Review/85174578 (дата звернення: 07.09.2020).

131. Постанова Великої Палати Верховного Суду від 16 січня 2019 р., судова справа № 751/7557/15-к (провадження № 13-37кс18). URL: https://reyestr.court.gov.ua/Review/79298340 (дата звернення: 07.09.2020).

132. Постанова Верховного Суду від 09 квітня 2020 р., судова справа №727/6578/17. URL https://zakononline.com.ua/court-decisions/show/88749345 (дата звернення: 07.09.2020).

133. Постанова Верховного Суду України від 16 березня 2017 р., судова справа №5-364 кс 16. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/VS170204.html (дата звернення: 07.09.2020).

134. Постанова Пленуму Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ № 3 від 07 лютого 2014 р., “Про узагальнення судової практики щодо розгляду слідчим суддею клопотань про дозвіл на проведення негласної слідчої (розшукової) дії” URL: http://zakon3.rada.gov.ua/laws/show/v0003740-14 (дата звернення: 27.12.2020).

135. Правила надання послуг поштового зв’язку: затв. постановою Кабінету Міністрів України від 5 березня 2009р. № 270 (із змінами і доповненнями на 08.04.2013). URL: https://zakon.rada.gov.ua/laws/show/270-2009-%D0%BF#Text (дата звернення: 18.11.2020).

136. Правила надання та отримання телекомунікаційних послуг: затв. постановою Кабінету Міністрів України від 11 квітня 2012 р. № 295 (із змінами і доповненнями на 08.04.2013). URL: https://zakon.rada.gov.ua/laws/show/295-2012-%D0%BF#Text (дата звернення: 17.11.2020).

137. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 17.11.2020).

138. Про поштовий зв’язок: Закон України від 04.10.2001 р. № № 2759-III. URL: https://zakon.rada.gov.ua/laws/show/2759-14#Text (дата звернення: 17.11.2020).

139. Психологічний тлумачний словник найсучасніших термінів. Харків: Прапор, 2009. 672 с.

140. Развитие информационных технологий в уголовном судопроизводстве: монография / под ред. докг. юрид. наук С. В. Зуева. Москва: Юрлитинформ, 2018. 248 с.

141. Резолюція Ради Європейського союзу “Про законне перехоплення телекомунікацій” (96/C 329/01) від 17 січня 1995 р. URL: https://zakon.rada.gov.ua/laws/show/994_235#Text (дата звернення: 13.11.2020).

142. Резолюція Ради Європейського союзу “Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг” (ENFOPOL) від 20 червня 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_234#Text (дата звернення: 26.12.2020).

143. Рішення Конституційного Суду України від 20 січня 2012 р. № 2-рп/2012 у справі за конституційним поданням Жашківської районної ради

Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12 (дата звернення: 13.11.2020).

144. Рогальська В. Отримання речей і документів стороною обвинувачення в кримінальному провадженні за законодавством України. *Jurnalul juridic national: teorie si practica.* 2018. № 4. С. 128 - 131.

145. Савляк І. І. Таємниця спілкування як засада кримінального провадження: автореф. дис. … канд. юрид. наук : 12.00.09 / Нац. акад. внутр. справ. Київ, 2018. 25 с.

146. Садовник Т. В. Обмеження таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції шляхом зняття інформації з телекомунікаційних мереж. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2010. № 2. С. 61 - 64.

147. Сербінов О. С. Окремі види інформації про абонента, яка знаходиться у користуванні операторів мобільного зв'язку та може бути отримана у ході проведення оперативно-розшукових заходів або слідчих дій. *Адвокат.* 2009. № 1. С. 36 - 39.

148. Сергеев М. С. Критерии доказывания электронных преступлений при применении мобильных приложений. Особенности их изъятия. *Актуальные проблемы экономики и права.* 2016. № 2. С. 264 - 272 .

149. Сергєєва Д. Б. Напрямки використання результатів негласних слідчих (розшукових) дій у кримінальному процесуальному доказуванні. *Вісник кримінального судочинства.* 2018. № 2. С. 81-т91.

150. Серьогін В. Зміст і обсяг права на недоторканість приватного життя (прайвесі). *Вісник академії правових наук України.* 2010. № 4. С. 88---97.

151. Серьогін В. О. Прайвесі у США: політико-правова теорія і практика. *Форум права.* 2011. № 1. С. 891-897.

152. Сліпченко В. І. Тимчасовий доступ до речей і документів: процесуальний порядок отримання. *Науковий вісник Дніпропетровського*

державного університету внутрішніх справ. 2013. № 2. С. 507 - 514.

153. Справа "Волохи проти України" (Заява № 23543/02): Рішення Європейського суду з прав людини від 2 листопада 2006 р. URL: https://zakon.rada.gov.ua/laws/show/974_138#Text (дата звернення: 19.09.2020).

154. Тагієв С. Р. Тимчасовий доступ до інформації, яка знаходиться в операторів та провайдерів телекомунікацій, у кримінальному провадженні. *Часопис цивільного і кримінального судочинства.* 2013. № 4. С. 98 - 110.

155. Тагієв С. Р. Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Слово Національної школи суддів України.* 2013. № 2. С. 13 - 24.

156. Теория оперативно-розыскной деятельности: учебник / под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова. – Москва: ИНФРА-М, 2009. 832 с.

157. Ткачик А. Обмеження таємниці спілкування в ході проведення тимчасового доступу до речей та документів. *KELM.* 2020. № 6. С. 224-229.

158. Ткачик А. Б. Європейські стандарти забезпечення таємниці спілкування у кримінальному провадженні. *Вісник Чернівецького факультету Національного університету "Одеська юридична академія".* 2019. №. 2. С. 208 - 218 с.

159. Ткачик А. Б. Зарубіжний досвід правового регулювання таємниці спілкування. *International Journal Law & Society*. 2021. № 3. С. 79 - 86.

160. Ткачик А. Б. Поняття та зміст таємниці спілкування у кримінальному провадженні. *Юридична наука.* 2020. №1. С. 156 - 161.

161. Трепак В. М. Протидія корупції в Україні: теоретико-прикладні проблеми : монографія. Львів: ЛНУ ім. Івана Франка, 2020. 442 с.

162. Трефилов А. А. Негласные следственные действия: опыт Швейцарии. *Концептуальные основы современной криминалистики: теория и практика*. 2019. С. 274 - 279.

163. Трефилов А. А. Уголовный процесс зарубежных стран. Том 1.

Уголовный процесс Швейцарии. Москва. 2016. 1012 с.

164. Уваров В. Г. Зняття інформації з телекомунікаційних мереж. *Актуальні проблеми вітчизняної юриспруденції.* 2017. № 2. С.121- 124.

165. Уголовно-процессуальный кодекс республики Казахстан: Закон от 07.11.14 г. № 231-V (с изменениями и дополнениями по состоянию на 02.01.2021 г.). URL: http: https://online.zakon.kz/document/?doc_id=31575852 (дата обращения: 01.02.2020).

166. Уголовно-процессуальный кодекс Республики Молдова: Закон от 14 марта 2003 г. № 122-XV (с изм. и доп. по состоянию на 01 января 2020 г.). URL: http: online.zakon.kz/Document/?doc_id=30397729 (дата обращения: 01.02.2020).

167. Уголовно-процессуальный кодекс Республики Узбекистан: Закон от 22 сентября 1994 г. № 2013-XII (с изм. и доп. по состоянию на 01 января 2020г.) URL: http: online.zakon.kz/Document/?doc_id=30421101 (дата обращения: 01.02.2020).

168. Удовенко Ж. В. Проблеми забезпечення охорони таємниці приватного життя під час зняття інформації з транспортних телекомунікаційних мереж. *Наукові записки НаУКМА. Юридичні науки.* 2019. С. 120-126.

169. Ухвала слідчого судді Амур-Нижньодніпровського районного суду м. Дніпропетровська про тимчасовий доступ до речей і документів від 09.02.2018 р., судова справа № 199/677/18. URL: https://zakononline.com.ua/court-decisions/show/64472641 (дата звернення: 12.01.2021)

170. Ухвала слідчого судді Галицького районного суду м. Львова про тимчасовий доступ до речей і документів від 05.12.2019 р., судова справа № 461/9256/19. Архів Галицького районного суду м. Львова.

171. Ухвала слідчого судді Галицького районного суду м. Львова про тимчасовий доступ до речей і документів від 11.10.2019 р., судова справа № 461/5038/19. Архів Галицького районного суду м. Львова.

172. Ухвала слідчого судді Галицького районного суду м. Львова про тимчасовий доступ до речей і документів у справі від 11.10.2019 р., судова справа №461/5038/19. Архів Галицького районного суду м. Львова.

173. Ухвала слідчого судді Галицького районного суду м. Львова про тимчасовий доступ до речей і документів від 20.02.2019 р., судова справа №461/9493/18. Архів Галицького районного суду м. Львова.

174. Ухвала слідчого судді Сватівського районного суду Луганської області про тимчасовий доступ до речей і документів від 09 грудня 2019 р., судова справа № 426/14319/19. URL: https://reyestr.court.gov.ua/Review/86218932. (дата звернення: 17.01.2021)

175. Федотов Н. Н. Форензика – компьютерная криминалистика. Москва: Юридический Мир, 2007. 432 с.

176. Фулей Т.І. Застосування практики Європейського суду з прав людини при здійсненні правосуддя: наук.-метод. посіб. для суддів. 2-ге вид. випр., допов. Київ. 2015. 208 с.

177. Хартія основних прав Європейського Союзу від 7 грудня 2000 року URL: https://zakon.rada.gov.ua/laws/show/994_524 (дата звернення: 25.11.2019).

178. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету*. 2013. № 5. С. 256 - 260.

179. Чернявський С. С., Фінагеєв В. О. Проблеми тимчасового доступу до інформації, яка знаходиться в операторів та провайдерів комунікацій. *Юридичний часопис Національної академії внутрішніх справ.* 2013. № 1. С. 179–185.

180. Шевчук С. Судовий захист прав людини: практика Європейського суду з прав людини у контексті західної правової традиції. Київ: Реферат, 2007. 848 с.

181. Шепітько В. Ю., Журавель В. А. Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції :

монографія. Харків: Апостиль, 2017. 260 с.

182. Шило А. В. Отримання інформації з вилученої електронної техніки як спосіб збирання доказів: спірні питання практичного правозастосування. *Правові новели.* 2018. № 5. С. 172-178.

183. Шило О. Г. Теоретико-прикладні основи реалізації конституційного права людини і громадянина на судовий захист у досудовому провадженні в кримінальному процесі України. Харків: Право, 2011. 472 с.

184. Шум В. В. Забезпечення оперативності при накладенні арешту на кореспонденцію. *Форум права.* 2012. № 4. С. 1086 - 1091.

185. Шумило М. Є. Інформаційна теорія доказів та проблеми використання електронних засобів доказування у кримінальному провадженні/ Юрка Р., Капліна В. А.. *Вісник Національної академії правових наук України.* 2019. № 2. С. 137-152.

186. Щербаковський М. Г. Тактичні та організаційні особливості зняття інформації з транспортних телекомунікаційних мереж / Коршенко В. А. *Криміналістика і судова експертиза.* 2018. № 63(1). С. 154-162.

187. Юрчишин В. М. Слідчий суддя в кримінальному процесі України. *Вісник Чернівецького факультету Національного університету "Одеська юридична академія*". 2017. № 1. С. 248-259.

188. Юрчишин В. М. Судовий контроль за застосуванням запобіжних заходів, затримання особи в зоні АТО: обмеження чи доцільність. *Вісник Чернівецького факультету Національного університету "Одеська юридична академія"*. 2017. № 4. С. 240 - 246.

189. Юхно О. О. Особливості використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуальне оформлення. *Вісник Харківського національного університету внутрішніх справ.* 2016. № 2. С. 86-95.

ДОДАТКИ

Додаток №1

ЗАТВЕРДЖУЮ
Заступник начальника СУ
Головного Управління Національної
поліції України у Львівській області
підполковник поліції
_____ Андрій **КУМЕЧКО**
05.березня 2021

АКТ

05 березня 2021 м. Львів №_3__

Про впровадження результатів дисертації
Ткачика Андрія Богдановича
на здобуття наукового ступеня доктора філософії
за темою: «Таємниця спілкування та її обмеження у кримінальному провадженні»

Комісія з у складі:
Начальник відділу СУ ГУНП у Львівській області підполковник поліції Ошенков Ярослав Іванович; старший слідчий в ОВС СУ ГУНП у Львівській області майор поліції Кобісар Іванна Василівна

розглянула й узагальнила наукові праці аспіранта кафедри кримінального процесу і криміналістики факультету №1 Інституту з підготовки фахівців для підрозділів Національної поліції Львівського державного університету внутрішніх справ Ткачика Андрія Богдановича за темою дисертації «Таємниця спілкування та її обмеження у кримінальному провадженні».

Наукові праці в яких опубліковані основні наукові результати дисертації:

1. Ткачик А.Б. Поняття та зміст таємниці спілкування у кримінальному провадженні. *Юридична наука*. 2020. №1. С. 156-161.
2. Ткачик А.Б. Зарубіжний досвід правового регулювання таємниці спілкування. *International Journal Law & Society*. Issue 3. 2021. С. 79-86.
3. Ткачик А. Обмеження таємниці спілкування в ході проведення тимчасового доступу до речей та документів. *KELM*. 2020. № 6. С. 224-229 .
4. Ткачик А.Б. Європейські стандарти забезпечення таємниці спілкування у кримінальному провадженні. *Вісник Чернівецького факультету*

Національного університету «Одеська юридична академія». 2019. Вип. 2. С. 208-218.

5. Забезпечення відшкодування шкоди у злочинах, пов'язаних з торгівлею людьми, на стадії досудового розслідування: довідник / Хитра А.Я., Кучер В.О., Ткачик А.Б. Видавництво: ЛьвДУВС, Львів, 2019. 128 с.
6. Кримінально-правова характеристика злочинів, пов'язаних з незаконним обігом зброї та вибухівки: посібник для підрозділів Національної поліції у схемах / Мармура О.З., Письменський Є.О., Ткачик А.Б. Видавництво: ЛьвДУВС, Львів, 2019. 44с.
7. Ткачик А.Б. Обмеження таємниці спілкування в практиці європейського суду з прав людини. Процесуальне та криміналістичне забезпечення досудового розслідування: збірник тез науково-практичного семінару (01 грудня 2017 року) / упор. А.Я. Хитра, Р.М. Шехавцов, Є.В. Пряхін, С.І. Марко. Львів: ЛьвДУВС. С. 112-115.
8. Ткачик А.Б. Обмеження таємниці спілкування шляхом проведення зняття інформації з транспортних телекомунікаційних мереж. Процесуальне та криміналістичне забезпечення досудового розслідування: тези доповідей учасників науково-практичного семінару (30 листопада 2018 року) / упор. А.Я. Хитра. Львів: ЛьвДУВС. С. 93-96.
9. Ткачик А.Б. Обмеження таємниці спілкування в ході проведення аудіо-, відеоконтролю особи та місця. Правова система України: сучасний стан та актуальні проблеми: Збірник матеріалів восьмої Всеукраїнської науково-практичної конференції (Івано-Франківськ, 13 листопада 2020 року). Івано-Франківськ: видавник Голіней О.В., 2020. С. 114-117.

На основі проведеного аналізу комісія дійшла висновку, що наукові праці Ткачика Андрія Богдановича містять науково обґрунтовані теоретичні положення та практичні рекомендації та можуть використовуватись у практичній діяльності підрозділів досудового розслідування СУ ГУНП України у Львівській області, а також під час проведення занять зі службової підготовки.

Члени комісії:

1. _____
2. _____