УДК 343.14:351.745.7:343.974

Погорецький Микола Анатолійович –
доктор юридичних наук, професор,
заслужений діяч науки і техніки України,
завідувач кафедри правосуддя юридичного факультету
Київського національного університету імені Тараса Шевченка

Mykola A. Pohoretskyi –
doctor of juridical sciences, professor,
honoured worker of science and technology of Ukraine,
head of the department of justice of the Faculty of Law,
Taras Shevchenko National University of Kyiv
(60, Volodymyrska Street, Kyiv, Ukraine)

Сухачов Олексій Олександрович –
кандидат юридичних наук,
здобувач кафедри правосуддя юридичного факультету
Київського національного університету імені Тараса Шевченка

Oleksii O. Sukhachov –
candidate of juridical sciences,
external doctoral student of the department of justice
of the Faculty of Law,
Taras Shevchenko National University of Kyiv
(60, Volodymyrska Street, Kyiv, Ukraine)

Система засобів охорони державної таємниці щодо діяльності оперативних підрозділів правоохоронних органів

У статті проведено аналіз наукових джерел, положень законодавства та підзаконних нормативно-правових актів, що регулюють суспільні відносини у сфері охорони державної таємниці, а також практику оперативних підрозділів правоохоронних органів України з їх реалізації. Виявлено проблеми будови системи засобів охорони таємниці щодо діяльності оперативних підрозділів та запропоновано шляхи їх вирішення.

Ключові слова: *захист інформації, охорона державної таємниці, оперативні підрозділи, оперативно-розшукові заходи, режим секретності.*

В статье проведен анализ научных источников, положений законодательства и подзаконных нормативно-правовых актов, регулирующих общественные отношения в сфере охраны государственной тайны, а также практику оперативных подразделений правоохранительных органов Украины по их реализации. Выявлены проблемы строения системы средств охраны тайны о деятельности оперативных подразделений и предложены пути их решения.

Ключевые слова: *защита информации, охрана государственной тайны, оперативные подразделения, оперативно-розыскные мероприятия, режим секретности.*

M.A. Pohoretskyi, O.O. Sukhachov The System of Means of Sensitive Information Protection Related to the Activities of Operative Subdivisions of Law Enforcement Bodies

The article analyzes legislation which regulates legal relations in the area of sensitive information protection, as well as practice of operative law enforcement agencies of Ukraine which execute them. The issues related to establishment of the system of data protection regarding the activities of operative subdivisions have been determined and the ways of their solving have been proposed.

It has been noted that protection of sensitive information on the activities of operative subdivisions of law enforcement agencies is a component of ensuring conspiracy in their activities. Such protection is provided by the system of measures established by law. These measures can be classified at the organizational, engineering and technical, cryptographic ones and measures of background check because of the access to sensitive information.

Organizational are measures which establish, organize and ensure a proper operation of the information security procedures (a unified procedure of ensuring protection of sensitive information) and are taken in accordance with law and administrative decisions on the protection of sensitive information made by the authorized subjects.

Engineering and technical measures of protection of sensitive information include the following: engineering and technical measures of passive information protection (optical, electro-magnetic, radial screening, technical means with protection, special means of information protection in telecommunication systems etc.); technical measures of active information protection (vibroacoustic, acoustic and electromagnetic noise generators, circuit electromagnetic noise); construction measures.

Cryptographic measures of sensitive information protection are the use of systems and means which transform information using special data (key data) to hide (or renew) the content of information, to prove its authenticity, integrity, authorship.

Measures on background check because of the access to sensitive information include the following:

1. Information on individuals who apply for the access to sensitive information is collected upon their consent by the authorized subjects: i) from the official sources (responses of the authorities, local self-government bodies, enterprises, institutions, organizations to the requests submitted in accordance with the procedure provided for by law); ii) by using rights stipulated by Art. 8 of the Law "On Operative and Search Activities";

2. Analysis and evaluation of collected information to check existence or non-existence of reasons to decline in access to sensitive information.

Keywords: *protection of information, protection of sensitive information, operative subdivisions, operative and search measures, information security procedures.*

Постановка проблеми. Охорона широкого спектру інформації щодо діяльності оперативних підрозділів в боротьбі зі злочинністю є об'єктивною необхідністю. Адже організовані злочинні формування намагаються забезпечити безкарність своєї діяльності усіма можливими засобами, в тому числі шляхом проведення заходів розвідувального характеру (з використанням спеціальної техніки, а також через шантаж та підкуп працівників правоохоронних органів).

Однією з головних складових охорони інформації щодо діяльності оперативних підрозділів є забезпечення режиму секретності. З огляду на значення даного сегменту роботи оперативних підрозділів, вона має бути добре налагодженою, організованою та відповідати вимогам до системи захисту державної таємниці, що встановлюються за допомогою норм права на державному рівні. Але ця система має вади, що піддаються конструктивній критиці практиків та науковців. Тому одним з головних шляхів вирішення проблем охорони таємниці щодо діяльності оперативних підрозділів є вдосконалення вказаної системи, що зумовлює необхідність відповідного дослідження.

Аналіз останніх досліджень і публікацій. Загальні та особливі питання охорони державної таємниці в Україні розробляли О. Є. Архипов, О. В. Ботвінкін, Ю. П. Мірошник, М. С. Пастернак, О. В. Розвадовський, І. В. Романенко, С. Р. Тагіє та інші [1–9].

Проблеми забезпечення конспірації діяльності оперативних підрозділів правоохоронних органів України досліджували М. Л. Грібов, І. М. Зубач, А. Є. Івахін, П. Я. Пригунов, О. Ю. Шевчук та інші [10–14].

Незважаючи на ґрунтовні дослідження проблем охорони державної таємниці в Україні та певні досягнення у теоретичній розробці забезпечення конспірації діяльності оперативних підрозділів, дані напрями наукових досліджень майже не перетиналися. Питання засобів охорони таємниці щодо діяльності оперативних підрозділів в межах забезпечення конспірації їх діяльності залишились поза увагою науковців.

Невирішені раніше проблеми. Серед невирішених проблем обраного напряму виокремлюємо суперечливість та недостатню практичну ефективність системи засобів охорони державної таємниці щодо діяльності оперативних підрозділів.

Мета статті полягає у виявлені проблем будови системи засобів охорони державної таємниці щодо діяльності оперативних підрозділів та визначення шляхів їх вирішення.

Виклад основного матеріалу. Аналіз результатів наукових досліджень з питань історії [15; 16] та сучасного стану охорони державної таємниці в Україні засвідчують, що національна система охорони державної таємниці створювалась з урахуванням досвіду розвинених демократичних країн та випробуваних на практиці традиційних засобів і методів. Проте значною мірою вона є спадкоємцем системи захисту секретної інформації, яка існувала за часів Радянського Союзу, що ефективно діяла впродовж кількох десятиліть. Зокрема, були створені суб'єкти захисту інформації, повноваження яких на той час відповідали наявним вимогам. Оскільки секретна інформація була предметом посягань розвідувальних органів супротивника, закономірно, що з самого початку такі повноваження було покладено на контррозвідувальні підрозділи органів державної безпеки. Вони захищали секретну інформацію шляхом проведення контррозвідувальних заходів, організації режимно-секретної діяльності, військової цензури, та ін. Крім діяльності спеціальної служби, яка відгравала головну роль у охороні секретної інформації, було створено механізм захисту від розголошення секретної інформації через друковані органи. Закладена в ті часи структура проіснувала протягом всього періоду СРСР і була успадкована незалежною Україною [17]. При цьому, разом з корисними рисами, до системи охорони державної таємниці України з радянського минулого потрапили елементи, що гальмують її ефективну роботу та мають негативний вплив на виконання своїх функцій окремими державними структурами, зокрема оперативними підрозділами правоохоронних органів. Це зумовлює необхідність проведення наукових розвідок відповідного напряму.

Теоретичні дослідження, які спрямовані на вдосконалення системи охорони державної таємниці, активно проводяться як на загальному державному рівні, так і на рівні діяльності оперативних підрозділів. Але якщо на загальному державному рівні такі дослідження представлені кандидатськими та докторськими дисертаціями [3; 4; 7], то на рівні діяльності оперативних підрозділів це, здебільшого, окремі публікації, які стосуються лише питань забезпечення охорони державної таємниці щодо проведення ОРД. При цьому, автори таких публікацій часто не враховують у своїй роботі здобутки попередників, які досліджували загальнотеоретичні та організаційно-правові засади забезпечення охорони державної таємниці. Ігнорування результатів фундаментальних наукових розвідок, зокрема, щодо визначення основних понять та категорій досліджуваної тематики призводить до похибок в ході досліджень та помилкових висновків.

Так, за словами В. В. Єфімова, сьогодні захист державної таємниці в ОРД забезпечується сукупністю правових і організаційних засобів, практичною реалізацією принципів поєднання гласних і негласних заходів, конспірації, суворим дотриманням її вимог, засекречуванням відомостей щодо проведення ОРЗ, чітко визначеним порядком допуску та доступу осіб до таких відомостей. У зв'язку з допуском до державної таємниці на працівників ОВС покладаються обов'язки, які поділяються на дві групи: перша передбачає вимоги, для додержання яких працівники ОВС мають виконувати активні дії із забезпечення режиму секретності і конспірації; друга – обов'язки у формі правових зобов'язань, спрямованих на необхідність утримання від певних дій, що можуть спричинити відтік секретних відомостей, втрату секретних документів або завдати іншої шкоди охороні державної таємниці [18].

Як бачимо, автор цілком слушно пов'язує захист державної таємниці з категорією конспірації, що простежується й у працях інших науковців. Проте він не чітко визначає співвідношення цих категорій, як в теоретичному, так і у суто правовому аспекті. Це в подальшому може призводити до помилок у наукових дослідженнях обраного напряму. Адже конспірація це широка категорія, яка в числі іншого включає в себе і охорону державної таємниці щодо діяльності оперативних

підрозділів, а остання, у свою чергу охоплює режим секретності.

Аби дослідження охорони секретної інформації щодо діяльності оперативних підрозділів як складової конспірації їх діяльності було ефективним необхідно, на наш погляд, чітке розуміння основних понять та їх співвідношення. Оскільки конспірація та окремі, пов'язані з цією категорією теоретичні поняття вже досліджувались [19–21], перейдемо до розгляду термінів, які є усталеними та унормованими, зокрема це «державна таємниця», «охорона державної таємниці», «захист інформації», «віднесення інформації до державної таємниці» та пов'язаних з ними термінів.

Державну таємницю законодавець визначив як вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому законом, державною таємницею і підлягають охороні державою (ст. 1 Закону України «Про державну таємницю). При цьому, зауважимо, що поряд з терміном «державна таємниця» в Законі (у тому ж значенні) вживається також термін «секретна інформація».

Охорона державної таємниці, зазначено у Законі, – це комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв (ст. 1). Термін «захист державної таємниці» законодавець не тлумачить, хоча вживає його у п. «д» ч. 9 ст. 21 (при визначені завдань режимно-секретних органів): «здійснювати перевірки стану й організації роботи з питань захисту державної таємниці і забезпечення режиму секретності». Не вживається в Законі і терміни «захист інформації», «захист секретної інформації». Водночас в Законі використовуються такі поняття: «криптографічний захист секретної інформації» – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо (ч. 10 ст. 1); технічний захист секретної інформації – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації (ч. 17 ст. 1)

Отже, законодавець визначає та регламентує (ст. 35) окремі види захисту секретної інформації, але не подає його тлумачення в цілому. Тому не зрозуміло як дана категорія співвідноситься з категорією «охорона державної таємниці». Те саме спостерігається у багатьох наукових працях обраного напряму дослідження, автори яких вживають означені терміни, однак при цьому не розкривають їх понять. Аналіз результатів наукових досліджень щодо співвідношення понять «охорона» і «захист» дає підстави для висновку, що охорона – це широке за змістом поняття, яке, серед іншого, охоплює й захист. Тому захист державної таємниці є складовою її охорони. Даний висновок, на наш погляд, підтверджується й законодавчим переліком елементів, що входять до змісту охорони державної таємниці. Так, у ст. 18 «Основні організаційно-правові заходи щодо охорони державної таємниці» Закону України «Про державну таємницю» визначено, що з метою охорони державної таємниці впроваджуються: єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації; дозвільний порядок провадження державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з державною таємницею; обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації; обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об'єктів і технічних засобів, що їм належать; особливості здійснення державними органами їх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею; режим секретності державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею; спеціальний порядок допуску та доступу громадян до державної

таємниці; технічний та криптографічний захисти секретної інформації.

Отже, останнім пунктом даної статті законодавець чітко визначив свою позицію щодо захисту інформації як складової охорони державної таємниці.

У площині організації конспірації діяльності оперативних підрозділів доцільно окремо розглянути кожен із засобів охорони держаної таємниці, що визначені ст. 18 Закону України «Про державну таємницю», до яких законодавець відносить організаційно-правові, інженерно-технічні, криптографічні та оперативно-розшукових заходи (ст. 1).

До організаційно-правових заходів законодавець відносить: єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації; дозвільний порядок провадження державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з державною таємницею; обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації; обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об'єктів і технічних засобів, що їм належать; особливості здійснення державними органами їх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею; режим секретності державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею; спеціальний порядок допуску та доступу громадян до державної таємниці; технічний та криптографічний захисти секретної інформації (ст. 18).

Аналіз наведених норм Закону України «Про державну таємницю» дозволяє виявити низку невідповідностей.

По-перше у ст. 1 законодавець виокремив заходи технічного та криптографічного захисту секретної інформації, розмежувавши їх з організаційно-правовими. Водночас у ч. 8 ст. 18 законодавець відносить ці види захисту державної таємниці саме до організаційно-правових.

По-друге, на нашу думку, найменування заходів, визначених у ст. 18 Закону як організаційно-правових є недостатньо коректним. Ураховуючи сутність цих заходів, їх доцільно визначити як організаційні (такі, що спрямовані на впорядкування, налагодження системи охорони державної таємниці). Вони дійсно встановлюються за допомогою норм права, але немає необхідності визначати їх як організаційно-правові, через те що усі заходи передбачені законом є правовими. У іншому випадку, враховуючи логіку законодавця, до назви решти, визначених ним заходів, також потрібно додавати правовий компонент («криптографічно-правові», «інженерно-технічно-правові», «оперативно-розшуково-правові»).

По-третє, вимоги, порядок, обмеження, особливості та режим, визначені у ст. 18 Закону України «Про державну таємницю» встановлено Порядком організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженим постановою Кабінетів Міністрів України від 18.12.2013 № 939. Отже, режим секретності охоплює усі інші організаційні заходи у сфері охорони державної таємниці. Більше того, як слушно зауважує Ю. Дрейс, режим секретності як єдиний порядок забезпечення охорони державної таємниці включає у себе інші порядки, а саме: віднесення інформації до державної таємниці; дозвільний порядок провадження діяльності, пов’язаної з державної таємницею; порядок засекречування та розсекречування магнітних носіїв секретної інформації; порядок надання, переоформлення та скасування громадянам допуску до державної таємниці; передачі державної таємниці іноземній державі чи міжнародній організації; підготовки документів щодо надання доступу до державної таємниці іноземцям та особам без громадянства; технічного та криптографічного захисту секретної інформації; надання компенсації громадянам у зв’язку з роботою, яка передбачає доступ до державної таємниці; проведення експертизи цінності документів; організації та проведення експертиз на предмет наявності чи відсутності у матеріальних носіях інформації

відомостей, що становлять державну таємницю; проведення державної експертизи в сфері технічного захисту інформації; організації та проведення державної експертизи у сфері криптографічного захисту інформації; державного обліку секретних науково-дослідних робіт, дослідно-конструкторських робіт і дисертацій; інші порядки [22, с. 182]. З нашого погляду, система усіх перерахованих порядків становить зміст організації режиму секретності.

Отже, в теоретичному плані важливою є конкретизація змістовного наповнення поняття «режим секретності», уточнення того, що саме мається на увазі під «єдиним порядком забезпечення охорони державної таємниці», змістом заходів, що здійснюються для забезпечення єдиного порядку та методів їх реалізації. Актуальність даного завдання зумовлює і потреба у гармонізації термінології сфери інформаційної безпеки в Україні до європейських стандартів. З цього приводу О. Є. Архипов, О. Є. Муратов, В. Р. Муратов, слушно зауважують: якщо у сферах технічного захисту інформації та управління інформаційною безпекою така гармонізація вже розпочалася, то більш консервативні складові режиму секретності ще залишаються незадіяними у цьому процесі. За умови збереження такого стану речей слід очікувати, що незабаром виникнуть тенденції децентралізації у системі охорони державної таємниці, яка поєднує всі зазначені сфери [23]. Вказане питання є предметом окремого дослідження. Але ще до його проведення цілком можливо, аналізуючи практику, визначити проблеми, що виникають із забезпеченням режиму секретності (відповідно до норм Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженим постановою Кабінетів Міністрів України від 18.12.2013 № 939) в діяльності оперативних підрозділів.

Зокрема, це проблеми, що унеможливлюють ефективне виконання своїх функцій оперативними працівниками, а відповідно стимулюють їх до пошуку шляхів уникнення виконання вимог зазначених вище нормативно-правових актів, що може призвести до негативних наслідків охорони державної таємниці в їх діяльності, у тому числі й кримінально-правового характеру. Так, комп'ютерна техніка, яка використовується для виконання та зберігання секретних документів потребує ліцензування у встановленому порядку, що у свою чергу потребує значних фінансових затрат, які покладено безпосередньо на підприємство, установу, організацію, що потребує такої техніки (у нашому випадку (райміськвідділи поліції, СБУ та ін. відомств). Тому, на значну за штатним розкладом та розгалуженістю структуру ліцензування проходять один або декілька комп'ютерів. Як наслідок, виявляється, що на одному комп'ютері протягом дня працює від 20 до 50 людей (оперативних працівників), які виконують від 400 до 1000 аркушів секретних документів. Природно, що це не реально. Результати анонімного опитування працівників оперативних підрозділів правоохоронних органів свідчать про те, вказані документи виконуються ними на власній комп'ютерній техніці і лише обліковуються як такі, що виконанні на ліцензованому комп'ютері. Це є грубим порушенням вимог законодавства та підзаконних нормативно-правових актів, що регулюють суспільні відносини у сфері охорони державної таємниці. Все вказане певною мірою стосується не лише оперативних підрозділів, а й органів досудового розслідування, прокуратури, суду, навчальних закладів МВС, СБУ, Державної прикордонної служби України тощо.

До інженерно-технічних заходів охорони державної таємниці, Ю. Дрейс, посилаючись на «Положення про технічний захист інформації в Україні» (затвердженого Указом Президента України № 1229/99 від 27.09.1999), відносить: створення або визначення підрозділів, на які покладається забезпечення технічного захисту інформації (ТЗІ) та контроль за його станом, узгодження основних завдань та функцій цих підрозділів; видання за погодженням з Адміністрацією Державної служби спеціального зв'язку та захисту інформації України та впровадження нормативно-правових актів з питань ТЗІ; погодження з Адміністрацією Державної служби спеціального зв'язку та захисту інформації України проведення підприємствами, установами, організаціями тих науково-дослідних, дослідно-конструкторських і дослідно-технологічних робіт, спрямованих на розвиток нормативно-правової та матеріально-

технічної бази системи ТЗІ, які здійснюються за рахунок коштів державного бюджету; створення або визначення за погодженням з Адміністрацією Державної служби спеціального зв'язку та захисту інформації України підприємств, установ та організацій, що забезпечують ТЗІ; забезпечення підготовки, перепідготовки та підвищення кваліфікації кадрів з ТЗІ; дослідження загроз для інформації на об'єктах, функціонування яких пов'язано з інформацією, що підлягає охороні; створення та виробництво засобів забезпечення ТЗІ; розроблення, впровадження, супроводження комплексів ТЗІ для забезпечення конфіденційності, цілісності та унеможливлення блокування інформації [22].

Проведений нами аналіз змісту зазначених заходів дає нам підстави для висновку, що за своєю сутністю вони не можуть бути віднесені до інженерно-технічних. Це – організаційні заходи з впорядкування, налагодження, системи технічного захисту інформації. Адже видання нормативно-правових актів; створення підприємств, установ, організацій та їх підрозділів; підготовка, перепідготовка та підвищення кваліфікації кадрів є елементами системи управління в галузі ТЗІ, вони здійснюються соціальними засобами, без використання технічних засобів захисту інформації.

Загально визнаним є виокремлення у ТЗІ двох основних методів: пасивний та активний методи захисту інформації. Активний захист побудовано на постановці перешкоди зняттю інформації шляхом випромінювання завад у канал витоку, рівень яких перевищує рівень небезпечних сигналів, які можна зняти з каналів витоку. До активного захисту також відносяться методи протидії, що засновані на постійному контролі середовища розповсюдження небезпечних сигналів необхідними для цього приладами та комплексами, які дозволяють виявляти спроби зняття інформації та активного пошуку і знешкодження засобів зняття інформації. Пасивний захист побудовано на зниженні спроможності певного технічного джерела витоку або середи розповсюдження небезпечних сигналів до передачі інформації шляхом технічних змін його властивостей, наприклад, шляхом екранування електромагнітного випромінювання. Для ТЗІ використовуються обидва напрямки захисту. Але слід відзначити, що пасивні методи захисту не використовують фізичних процесів, які шкідливі для здоров'я оточуючих та заважають повсякденній діяльності людей. Однак у більшості випадків застосування активних методів захисту є необхідним, які разом з пасивними методами захисту забезпечують потрібний ступень рівня технічного захисту інформації [24, с. 69]. Практична реалізація вказаних методів відбувається за рахунок відповідних заходів, а саме:

- інженерно-технічні заходи пасивного захисту інформації (оптичне, акустичне, електромагнітне, радіаційне екранування, технічні засоби із захистом, спеціальні засоби захисту інформації в телефонних та інших проводових лініях тощо);
- технічні заходи активного захисту інформації (генератори віброакустичного, просторового акустичного та електромагнітного зашумлення, лінійного електромагнітного зашумлення) [25].

Вважаємо цілком логічною позицію тих дослідників, які до інженерно-технічних заходів захисту інформації відносять архітектурно-будівельні [25], а також тих, які активні і пасивні заходи захисту інформації класифікують на заходи виявлення та блокування технічних каналів витоку акустичної інформації; заходи захисту акустичної інформації від зняття радіозакладними пристроями заходи пошуку радіозакладних пристроїв; заходи захисту інформації від витоку по технічних каналах, утворених допоміжними технічними засобами; заходи захисту інформації від несанкціонованого запису звукозаписувальними пристроями; заходи захисту електронної інформації; заходи захисту письмової інформації від оптичного зняття [24].

Керуючись на «Положення про порядок здійснення криптографічного захисту інформації в Україні» (затвердженого Указом Президента України № 505/98 від 22.05.1998), Ю. Дрейс до криптографічних заходів охорони державної таємниці належить: перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо – криптографічний захист; надання послуг із криптографічного

захисту інформації; використання криптосистем і засобів криптографічного захисту інформації за погодженням з Адміністрацією Державної служба спеціального зв'язку та захисту інформації України, допущені до експлуатації, мають сертифікат відповідності і перебувають у державній власності; проведення сертифікаційних випробувань криптосистем і засобів криптографічного захисту з метою визначення рівня захищеності від несанкціонованого доступу до інформації з обмеженим доступом [22].

З нашого погляду, лише «використання криптосистем і засобів криптографічного захисту інформації» відповідає категорії криптографічних заходів. Адже перший пункт наведеного переліку (перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства) є визначенням поняття криптографічного захисту інформації, а заходи з «надання послуг», «проведення сертифікаційних випробувань», «підвищення кваліфікації фахівців» власне не є криптографічними та належать до інших видів діяльності, що мають організаційно-забезпечувальне значення в роботі з криптографічного захисту інформації.

Технічний та криптографічний захисти секретної інформації становлять невід'ємну складову системи засобів. Але їх використання у практичній діяльності оперативних підрозділів, як і інших складових цієї системи часто пов'язане з певними труднощами, які здебільшого виникають з фінансових та організаційних проблем.

У різних оперативних підрозділах тих чи інших правоохоронних органів України ці проблеми мають певні відмінності, що пов'язані із специфікою виконуваних завдань, фінансування та організації роботи.

Досліджуючи поняття охорони державної таємниці, слід зауважити, що одним з її засобів Законом України «Про державну таємницю» визначено оперативно-розшукові заходи. У зв'язку з цим О. Б. Розвадовський, аналізуючи пункти 2 і 4 частини першої, частину другу статті 23, абзац 2 статті 24 Закону України «Про державну таємницю», доходить небезпідставного висновку, що оперативно-розшукові заходи (під час перевірки особи у зв'язку з її допуском до державної таємниці) мають бути спрямовані, насамперед, на отримання інформації щодо: можливого сприяння громадянином діяльності іноземної держави, іноземної організації чи їх представників, а також окремих іноземців чи осіб без громадянства, що завдає шкоди інтересам національної безпеки України або участі громадянина в діяльності політичних партій та громадських організацій, діяльність яких заборонена законом; невиконання громадянином обов'язків щодо збереження державної таємниці, яка йому довірена або довірялася раніше; фактів повідомлення громадянином під час оформлення допуску недостовірних відомостей про себе, зокрема про наявність судимості за тяжкі або особливо тяжкі злочини, не погашеної чи не знятої в установленому порядку; оформлення документів на виїзд для постійного проживання за кордоном тощо [26]. Проте аналіз ст. 1 Закону України «Про оперативно-розшукову діяльність» дає підстави для висновку, що будь-які заходи з охорони державної таємниці не можуть бути віднесені до категорії оперативно-розшукових. Адже завданням оперативно-розшукової діяльності є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави. Захист секретної інформації до кола завдань ОРД не входить.

Водночас, у суперечність наведеному положенню, законодавець у ст. 6 означеного закону, як одну з підстав для проведення оперативно-розшукової діяльності визначає «запити повноважних державних органів, установ та організацій про перевірку осіб у зв'язку з їх допуском до державної таємниці і до роботи з ядерними матеріалами та на ядерних установках». Далі, вже вкотре створюючи колізію між нормами закону, зазначає у ч. 1 ст. 9, що у кожному випадку наявності підстав для проведення оперативно-розшукової діяльності заводиться оперативно-розшукова справа, а у ст. 9-1 ігнорує визначення категорії оперативно-розшукової справи, яку можна було б завести для

виконання вказаних вище запитів (до переліку оперативно-розшукових справ законодавцем віднесено справи: щодо невстановлених осіб, які готують вчинення злочину, а також осіб, які переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування кримінального покарання; щодо осіб безвісно відсутніх; щодо осіб, стосовно яких є дані про участь у підготовці до вчинення злочину; щодо здійснення розвідувальних заходів в інтересах безпеки суспільства і держави; 5) щодо осіб, стосовно яких є дані про їх участь або причетність до терористичної діяльності, терористичної групи чи терористичної організації, а так само до матеріального, організаційного чи іншого сприяння створенню терористичної групи чи терористичної організації).

О. Б. Розвадовський зауважував, що Служба безпеки України як державний правоохоронний орган спеціального призначення, який забезпечує державну безпеку України та є спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці, відповідно до п. 2 ч. 1 ст. 5 Закону України «Про оперативно-розшукову діяльність» наділена правом проводити оперативно-розшукові заходи по відношенню до осіб, які порушили питання про можливість надання їм допуску до державної таємниці (при цьому, оперативно-розшукова справа не заводиться. Перевірка повинна тривати не більш як два місяці). При цьому вчений не звертає уваги на суперечливість норм вказаного закону.

Натомість науковець констатує, що виконання визначених законом завдань щодо вивчення і перевірки осіб, які оформлюються для допуску до державної таємниці, згідно з п. 2 ч. 1 ст. 6 Закону «Про контррозвідувальну діяльність» є також підставою для проведення контррозвідувальної діяльності. На його думку, ця норма вимагає узгодження із Законом України «Про державну таємницю», оскільки в ньому йдеться лише про можливість проведення оперативно-розшукових заходів [26].

З нашого погляду, перевірочні заходи, що проводяться у зв'язку з допуском осіб до державної таємниці і до роботи з ядерними матеріалами та на ядерних установках, як і заходи конспірації (у тому числі конспірації діяльності оперативних підрозділів), мають урегульовуватись безпосередньо в Законі України «Про державну таємницю». Безумовно такі заходи за своїм змістом можуть співпадати з оперативно-розшуковими, а також межувати з виконанням завдань контррозвідувальної діяльності. Крім того, вони можуть виконуватися суб'єктами оперативно-розшукової та контррозвідувальної діяльності. Однак фактично такі заходи не входять до сфери правового регулювання цих видів діяльності, а належать до окремої сфери суспільних відносин, що регулюються Законом України «Про державну таємницю». За аналогічним принципом (хоча і недосконало) сьогодні врегульовано участь оперативних підрозділів правоохоронних органів у кримінальному процесі: вони діють у кримінальному провадженні на підставі доручень слідчого, прокурора.

Водночас слід зауважити, що до заходів перевірки осіб у зв'язку з допуском до державної таємниці входять не лише заходи, що передбачені ст. 8 Закону України «Про оперативно-розшукову діяльність», а й збирання інформації у інший спосіб, з офіційних джерел – одержання відповідей органів влади, місцевого самоврядування, підприємств, установ, організацій на запити, оформлені в установленому порядку уповноваженими законом суб'єктами. Крім того, перевірка осіб у зв'язку з допуском до державної таємниці не може включати лише збирання інформації, а повинна охоплювати її аналіз та оцінку на предмет наявності або відсутності підстав для відмови громадянинові у наданні допуску до державної таємниці.

У зв'язку з викладеним, потрібно зазначити, що вимога законодавця щодо спеціального порядку допуску та доступу громадян до державної таємниці є цілком виправданою. Адже, як слушно зауважує В. В. Єфімов, дуже небезпечною для органів внутрішніх справ є протиправна діяльність організованих злочинних формувань, спрямована на викриття сил і засобів органів внутрішніх справ, виявлення запланованих і оперативно-розшукових заходів, що вже проводяться, слідчих дій, створення всіляких завад при їхньому здійсненні, а також вироблення контрзаходів, спрямованих на зрив здійснення оперативно-розшукової та

кримінально-процесуальної діяльності взагалі [18]. З цією метою учасники організованих злочинних формувань впроваджуються до правоохоронних органів. Відомі випадки коли зловмисники проводили операції з впровадження, що мали стратегічний характер: вони організовували вступ до навчальних закладів системи МВС та СБУ своїх спільників (відповідного віку), зокрема на факультети, що готують кадри для негласних оперативних підрозділів. Після навчання впроваджені особи направлялися на роботу за спеціальністю та вже через нетривалий час адаптації починали постачати організованим злочинним формуванням інформацію про те по відношенню кого, коли, де і ким провадяться оперативно-розшукові заходи. На той час законодавча вимога щодо спеціального порядку допуску та доступу громадян до державної таємниці вже була чинною. Але очевидно, що цей засіб охорони державної таємниці не спрацьовував через недостатній обсяг заходів негласного збирання інформації про особу, у зв'язку з її допуском до державної таємниці.

Висновки. Охорона державної таємниці щодо діяльності оперативних підрозділів правоохоронних органів є складовою забезпечення конспірації їх діяльності. Така охорона здійснюється за допомогою системи засобів, що встановлюються за допомогою норм права.

Зазначена система має низку вад, зумовлених суперечливістю правового регулювання. Для її вдосконалення необхідно впорядкувати законодавчу класифікацію заходів охорони державної таємниці, виокремивши серед них: організаційні, технічні, криптографічні та заходи з перевірки осіб у зв'язку з наданням допуску державної таємниці.

При цьому, в законі потрібно визначити зміст кожної категорії вказаних заходів, з урахуванням наведених нижче положень.

Організаційними є заходи з встановлення, впорядкування та забезпечення належного функціонування режиму секретності (єдиного порядку забезпечення охорони державної таємниці), які здійснюються шляхом правового регулювання та прийняття й виконання уповноваженими суб'єктами управлінських рішень у сфері охорони державної таємниці.

До інженерно-технічних заходів охорони державної таємниці належать: інженерно-технічні заходи пасивного захисту інформації (оптичне, акустичне, електромагнітне, радіаційне екранування, технічні засоби із захистом, спеціальні засоби захисту інформації в телекомунікаційних мережах тощо), технічні заходи активного захисту інформації (генератори віброакустичного, просторового акустичного та електромагнітного зашумлення, лінійного електромагнітного зашумлення), архітектурно-будівельні заходи;

криптографічними заходами охорони державної таємниці є використання систем і засобів перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства.

Заходи з перевірки осіб у зв'язку з наданням допуску державної таємниці включають:

1. Збирання інформації про осіб, які претендують на надання допуску до державної таємниці, що здійснюється за їх згодою, уповноваженими законом суб'єктами:

а) з офіційних джерел (відповіді органів влади, місцевого самоврядування, підприємств, установ, організацій на запити, оформлені в установленому порядку);

б) із застосуванням прав, передбачених ст. 8 Закону України «Про оперативно-розшукову діяльність»

Оперативно-розшукова справа при цьому не заводиться. Підставною проведення відповідних заходів є звернення громадянина щодо надання допуску до державної таємниці, яке одночасно є його згодою на їх проведення.

2. Аналіз та оцінку зібраної інформації на предмет наявності або відсутності підстав для відмови громадянинові у наданні допуску до державної таємниці.

Список використаних джерел:

1. Архипов О. Є. Системні аспекти оцінювання рівня важливості секретної інформації / О. Є. Архипов, В. П. Ворожко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2007. – Вип. 2 (15). – С. 10–12.
2. Ботвінкін О. Система охорони державної таємниці в Україні: історичний аспект / О. Ботвінкін // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – № 2 (13). – С. 83–89.
3. Мірошник Ю. П. Охорона державної таємниці в Україні: теоретико-управлінські засади : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.07 / Ю. П. Мірошник ; НА СБ України. – К., 2004. – 20 с.
4. Пастернак М. С. Правові основи віднесення інформації до державної таємниці в Україні : 12.00.07 / М. С. Пастернак ; НА СБ України. – К., 2013. – 20 с.
5. Розвадовський О. В. Теоретичні та організаційно-правові засади забезпечення охорони державної таємниці та службової інформації в сучасних умовах : автореф. дис. на здобуття наук. ступеня доктора юрид. наук : 21.07.01 / О. В. Розвадовський ; НА СБ України. – К., 2014. – 36 с.
6. Романенко І. В. Правове регулювання допуску до державної таємниці України : автореф. дис. на здобуття наук. ступеня канд.. юрид. наук : 21.07.01 / І. В. Романенко ; НА СБ України. – К., 2014. – 10 с.
7. Тагієв С. Р. Правове регулювання застосування режиму секретності під час проведення негласних слідчих (розшукових) дій / С. Р. Тагієв // Науковий вісник національної академії внутрішніх справ. – 2015. – № 1. – С. 166–172.
8. Погорецький М. А. Кримінально-процесуальні гарантії державної таємниці: до визначення поняття / М. А. Погорецький // Вісник прокуратури. – 2009. – № 11. – С. 88–96.
9. Погорецький М. Державна таємниця у кримінальному процесі України / М. Погорецький, Д. Куценко // Державна безпека України : наук.-практ. зб. НАН України і СБ України. – К., 2008. – № 13–14. – С. 94–98.
10. Грібов М. Л. Сутність конспірації в оперативно-розшуковій діяльності / М. Л. Грібов // Проблеми створення та використання легендованих підприємств в оперативно-розшуковій діяльності : матеріали Всеукр. наук.-практ. семінару. – Одеса : Одес. держ. ун-т внутр. справ, 2010. – С. 16–20.
11. Грібов М. Л. Використання засобів забезпечення конспірації при проведенні негласних слідчих (розшукових) дій / М. Л. Грібов // Форум права. – 2014. – № 2. – С. 94–98 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/jpdf/FP_index.htm_2014_2_17.pdf.
12. Зубач И. Н. Негласность как правовой феномен в уголовоном процессе Украины / И. Н. Зубач // Міжнародний науковий журнал «Науковий огляд» – 2014. – № 8 [Електронний ресурс]. – Режим доступу : http://www.sciary.com/journal-ukrainian-scientific-scirew-article-558217.
13. Ивахин А. Е. Оперативная деятельность и вопросы конспирации в работе спецслужб : по материалам открытой печати и лит. : [в 6 т. Т. 2] / А. Е. Ивахин, П. Я. Прыгунов. – [2-е изд. стереотип.]. – К. : КНТ, 2008. – 224 с.
14. Шевчук О. Ю. Конспірація як спеціальний принцип оперативно-розшукової діяльності / О. Ю. Шевчук // Науковий вісник Київського національного університету внутрішніх справ. – 2008. – № 1, ч. 2. – С. 123–128.
15. Ботвінкін О. В. Історія охорони державної таємниці в Україні : монографія / О. В. Ботвінкін, В. М. Шлапаченко, В. П. Ворожко, А. С. Пашков. – К. : Наук.-вид. відділ НА Служби безпеки України, 2008. – 155 с.
16. Мастяниця Й. У. Охорона державних секретів незалежної України (Історично-правові нариси) / Й. У. Мастяниця, Л. Є. Шиманський, О. В. Олійник, В. П. Ворожко ; за заг. ред. П. О. Мисника, О. В. Зайчука. – К. : Інститут законодавства Верховної Ради України, 2010. – 128 с.
17. Ботвінкін О. Система охорони державної таємниці в Україні: історичний аспект / О. Ботвінкін // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – № 2 (13). – С. 83–89.

18. Єфімов В. В. Забезпечення державної таємниці в оперативно-розшуковій діяльності / В. В. Єфімов // Науковий вісник Дніпропетровського державного університету внутрішніх справ. – 2011. – № 4 – С. 412 – 418.

19. Сухачов О. О. Поняття конспірації в діяльності оперативних підрозділів / О. О. Сухачов // Форум права. – 2014. – № 4. – С. 316–321 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/jpdf/FP_index.htm_2014_2_17.pdf.

20. Сухачов О. О. Поняття негласності в кримінальному процесі України / О. О. Сухачов // Проблеми правознавства та правоохоронної діяльності. – 2014. – № 4 – С. 170–180.

21. Sukhachov O. Meaning of the Term “Conspiration” in the Law of Ukraine and other Countries / Mykola Pogoretskyj, Oleksij Sukhachov // Internal security. – 2014. – Volume 6. – Issue 2. – Pp. 69–78.

22. Dreis Yu. Functioning of the State Secrets Security System in Ukraine: Organizational and Legal Structure, Principles and Objectives / Yu. Dreis // Ukrainian Scientific Journal of Information Security. – 2014. Vol. 20. – Issue 2. – Pp. 176–184.

23. Архипов О. Є. Щодо змісту поняття «режим секретності» у системі забезпечення інформаційної безпеки / О. Є. Архипов, О. Є. Муратов, В. Р. Муратов // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф., 30 березня 2012 р., м. Київ. – К. : Наук-вид. відділ НА СБ України, 2012. – С. 125–128.

24. Рибальський О. В. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України / О. В. Рибальський, В. Г. Хахановський, В. А. Кудінов. – К. : Вид. НАВС, 2012. – 104 с.

25. Богуславський Р. Г. Порядок створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності / Р. Г. Богуславський // Захист інформації в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності : матеріали доповідей семінару (27–28 жовтня 2005 р.) : Національний технічний університет України «Київський політехнічний інститут», м. Київ. – С. 2–5. [Електронний ресурс]. – Режим доступу : http://www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=15363597747F0169E70B57E03D875F15?art_id=44847&cat_id=103357.

26. Розвадовський О. Б. Забезпечення конституційних гарантій, прав і свобод людини у процесі здійснення оперативно-розшукової діяльності при перевірці громадян у зв’язку з допуском до держаної таємниці / О. Б. Розвадовський // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф., 30 березня 2012 р., м. Київ. – К. : Наук-вид. відділ НА СБ України, 2012. – С. 198.

References

1. O. Ye. Arkhypov, Systematical Aspects of Evaluation of Secret Information Importance / O. Ye. Arkhypov, V. P. Vorozhko // Pravove, normatyvne ta metrolohichne zapezpechennia systemy zakhystu informatsii v Ukraini (Legal, Normative and Metrological Ensuring of Information Security in Ukraine). – 2007. – Issue 2 (15). – Pp. 10-12.

2. O. Botvinkin, The System of Protection of Sensitive Information in Ukraine: Historical Aspect / O. Botvinkin // Pravove, normatyvne ta metrolohichne zapezpechennia systemy zakhystu informatsii v Ukraini (Legal, Normative and Metrological Ensuring of Information Security in Ukraine). – 2006. – No. 2 (13). – Pp. 83-89.

3. Yu. P. Miroshnyk, Protection of Sensitive Information in Ukraine: Theoretical and Administrative Grounds : synopsis of a thesis for a candidate of juridical sciences : 12.00.07 / Yu. P. Miroshnyk. – K., 2004. – 20 p.

4. M. S. Pasternak, Legal Grounds of Information Reference to the Sensitive Information in Ukraine : synopsis of a thesis for a candidate of juridical sciences : 12.00.07 / M. S. Pasternak ; the National Academy of Sciences. – K., 2013. – 20 p.

5. O. V. Rozavadovskyi, Theoretical, Organizational and Legal Principles for the Protection of Sensitive and Official Information under Current Conditions : synopsis of a thesis for a doctor of juridical sciences : 21.07.01 / O. V. Rozavadovskyi ; the National Academy of Sciences. – K., 2014. – 36 p.

6. I. V. Romanenko, Legal Regulation of Access to Sensitive Information of Ukraine : synopsis of a thesis for a candidate of juridical sciences : 21.07.01 / I. V. Romanenko ; the National Academy of Sciences. – K., 2014. – 10 p.

7. S. R. Tahiiev, Legal Regulation of Information Security Procedures during Secret Investigative (Search) Actions / S. R. Tahiiev // Naukovyi visnyk natsionalnoi akademii vnutrishnikh sprav (Scientific Bulletin of the National Academy of Internal Affairs). – 2015. – No. 1. – Pp. 166-172.

8. M. A. Pohoretskyi, Criminal and Procedural Guarantees of the Sensitive Information: to the Definition of Term / M. A. Pohoretskyi // Visnyk prokuratury (Bulletin of Public Prosecution Office). – No. 11. – Pp. 88-96.

9. M. Pohoretskyi, Sensitive Information in Criminal Procedure of Ukraine / M. Pohoretskyi, D. Kutsenko // Derzhavna bezpeka Ukrainy (National Security of Ukraine) : scient. collec. of papers of the National Academy of Sciences and the Security Service of Ukraine. – K., 2008. – No. 13-14. – Pp. 94-98.

10. M. L. Hribov, The Essence of Conspiracy in Operative and Search Activity / M. L. Hribov // Issues of Establishment and Use of Legendized Enterprises in Operative and Search Activity : materials of All-Ukr. Scient. And Pract. Seminar. – Odesa : Odesa State University of Internal Affairs, 2010. – Pp. 16-20.

11. M. L. Hribov, Use of Conspiracy Means during Secret Investigative (Search) Actions / M. L. Hribov // Forum prava (Forum of Law). – 2014. – No. 2. – Pp. 94-98 [Online resource]. – Access : http://nbuv.gov.ua/jpdf/FP_index.htm_2014_2_17.pdf.

12. I. N. Zubach, Secrecy as a Legal Phenomenon in Criminal Procedure of Ukraine / I. N. Zubach // Mizhnarodnyi naukovyi zhurnal "Naukovyi ohliad" (International Scientific Journal "Scientific Review") – 2014. – No. 8 [Online resource]. – Access : http://www.sciary.com/journal-ukrainian-scientific-scirew-article-558217.

13. A. E. Ivakhin, Operative Activity and Issues of Conspiracy in the Work of Special Services : according to materials of public media and lit. : [in 6 vol. Vol. 2] / A. E. Ivakhin, P. Ya. Prygunov. – [2nd ed. ster.] – K. : KNT, 2008. – 224 p.

14. O. Yu. Shevchuk, Conspiracy as a Special Principle of Operative and Search Activities / O. Yu. Shevchuk // Naukovyi visnyk Kyivskoho natsionalnoho universytetu vnutrishnikh sprav (Scientific Bulletin of Kyiv National University of Internal Affairs). – 2008. – No. 1, p. 2. – Pp. 123-128.

15. O. V. Botvinkin, History of Protection of Sensitive Information in Ukraine : monograph / O. V. Botvinkin, V. M. Shlapachenko, V. P. Vorozhko, A. S. Pashkov. – K. : Ed. Department of the National Academy of the Security Service of Ukraine, 2008. – 155 p.

16. I. U. Mastianytsia, Informational Security of Independent Ukraine (Historical and Legal Sketch) / I. U. Mastianytsia, L. Ye. Shymanskyi, O. V. Oliinyk, V. P. Vorozhko ; under the general editorship of P. O. Mysnyk, O. V. Zaichuk. – K. : Legislation Institute of the Verkhovna Rada of Ukraine, 2010. – 128 p.

17. O. Botvikin, The System of Protection of Sensitive Information in Ukraine: Historical Aspect / O. Botvinkin // Pravove, normatyvne ta metrolohichne zapezpechennia systemy zakhystu informatsii v Ukraini (Legal, Normative and Metrological Ensuring of Information Security in Ukraine). – 2006. – No. 2 (13). – Pp. 83-89.

18. V. V. Yefimov, Protection of Sensitive Information in Operative and Search Activity / V. V. Yefimov // Naukovyi visnyk Dnipropetrovskoho derzhavnoho universytetu vnutrishnikh sprav (Scientific Bulletin of Dnipropetrovsk State University of Internal Affairs). – 2011. – No. 4. – Pp. 412-418.

19. O. O. Sukhachov, Definition of Conspiracy in the Activities of Operative Subdivisions of Ukraine / O. O. Sukhachov // Forum prava (Forum of Law). – 2014. – No.4. – Pp. 316-321 [Online resource]. – Access : http://nbuv.gov.ua/jpdf/FP_index.htm_2014_2_17.pdf.

20. O. O. Sukhachov, Definition of Secrecy in Criminal Procedure of Ukraine / O. O. Sukhachov // Problemy pravoznavstva ta pravookhoronnoi diialnosti (Issues of Legal Studies and Law Enforcement Activity). – 2014. – No. 4. – Pp. 170-180.

21. Sukhachov O. Meaning of the Term "Conspiration" in the Law of Ukraine and Other Countries / Mykola Pogoretskyj, Oleksij Sukhachov // Internal security. – 2014. – Volume 6. – Issue 2. – Pp. 69–78.

22. Dreis Yu. Functioning of the State Secrets Security System in Ukraine: Organizational and Legal Structure, Principles and Objectives / Yu. Dreis // Ukrainian Scientific Journal of Information Security. – 2014. Vol. 20. – Issue 2. – Pp. 176–184.

23. O. Ye. Arkhipov, To the Content of the Term "Information Security Procedures" in the System of Information Security / O. Ye. Arkhipov, O. Ye. Muratov, V. R. Muratov // Current Issues of Management of Information Security of the State : coll. of mater. of scient. and pract. conf., March, 30, 2012, Kyiv. – K. : Ed. Department of the National Academy of the Security Service of Ukraine, 2012. – Pp. 125-128.

24. O. V. Rybalskyi, Basics of Informational Security and Technical Protection of Information : tutorial for cadets of the higher education establishments of the Ministry of Internal Affairs of Ukraine / O. V. Rybalskyi, V. H. Khakhanovskyi, V. A. Kudinov. – K. : Publishing House of the National Academy of Internal Affairs, 2012. – 104 p.

25. R. H. Bohuslavskyi, The Procedure of Establishing the Complexes for Technical Protection of Information at the Informational Activities Premises / R. H. Bohuslavskyi // Protection of Information in the Telecommunication Systems and at the Informational Activities Premises : materials of seminar papers (October 27-28, 2005) : the National Technical University of Ukraine "Kyiv Polytechnic Institute," Kyiv. – Pp. 2-5 [Online resource]. – Access : http://www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=15363597747F0169E70B57E03D875F15?art_id=44847&cat_id=103357.

26. O. B. Rozvadovskyi, Ensuring of Constitutional Guarantees, Human Rights and Freedoms during Operative and Search Activities when the Citizens are Checked to Get an Access to Sensitive Information / O. B. Rozvadovskyi // Current Issues of Management of State Information Security : collec. of papers of scient. conf., March 30, 2012, Kyiv. – K. : Nauk.-Vyd. viddil NA SB Ukrainy, 2012. – P. 198.