

УДК [342.951+351.817]:654.165

Д.В. СУЛАЦЬКИЙ, Донецький юридичний інститут Луганського державного університету внутрішніх справ

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ПРОТИДІЇ ПРАВОПОРУШЕННЯМ У СФЕРІ ВИКОРИСТАННЯ КІНЦЕВОГО ОБЛАДНАННЯ РУХОМОГО (МОБІЛЬНОГО) ЗВ'ЯЗКУ В УКРАЇНІ

Ключові слова: протидія правопорушенням, мобільний зв'язок, кінцеве обладнання зв'язку

Протягом останніх років в Україні спостерігається стрімкий розвиток новітніх інформаційно-телекомунікаційних технологій і послуг, що зумовлює розповсюдження рухомого (мобільного) зв'язку серед широких верств населення. Загальна чисельність абонентів телекомунікаційних мереж рухомого (мобільного) телефонного зв'язку на базі радіотехнології стандарту Global System for Mobile Communications 900/1800 (далі – рухомий зв'язок), що зараз у світі, в тому числі й в Україні, найпоширеніший, складає близько 53,6 мільйонів чоловік [1, с.9; 2, с.10; 3; 4]. Слід зазначити, що наведена статистика тягне за собою не тільки позитивні наслідки для особистості, суспільства та держави, але й негативні. До останніх, насамперед, відноситься значне зростання кількості злочинів проти власності, предметом посягання яких є кінцеве обладнання рухомого зв'язку (далі – термінал) [5; 6, с.24-25; 7; 8]. Так, якщо у 2004 році в Донецькій області зареєстровано 4427 злочинів даного виду (з них нерозкритими залишилися 3029 злочинів), то у 2006 році їх вже – 9389 (з них нерозкритих – 6547). Приріст зареєстрованих злочинів за три роки складає 112,1 % (нерозкритих – 116,1 %).

Аналіз показав, що дослідження різноманітних аспектів суспільних інформаційних відносин, які проведені вітчизняними та зарубі-

жними вченими (Д.С. Азаров, І.В. Арістова, О.А. Баранов, Ю.М. Батурич, І.Л. Бачило, К.І. Беляков, П.Д. Біленчук, В.М. Брижко., В.М. Бутузов, В.Б. Вехов, В.Д. Гавловський, Ю.В. Гаврилін, В.О. Голубєв, В.І. Гурковський, М.В. Гуцалюк, Н.К. Дніпренко, О.С. Єгоришев, О.О. Казанська, М.В. Карчевський, В.Є. Козлов, В.К. Конах, Б.А. Кормич, В.В. Крилов, О.О. Кулініч, О.В. Литвиненко, О.В. Логінов, В.О. Мещеряков, У.А. Мусаєва, О.В. Олійник, С.О. Орлов, О.В. Остроушко, А.В. Пазюк, К.І. Панфілова, Е.В. Рижков, В.Ю. Рогозін, Б.В. Романюк, Г.В. Семенов, Л.М. Соловйов, О.В. Сорокін, В.С. Цимбалюк), в основному стосуються боротьби зі злочинами у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; інформаційної безпеки; захисту персональних даних; формування інформаційної політики; удосконалення державного управління в інформаційній та телекомунікаційній сферах. Разом із тим, поза увагою залишилися проблеми боротьби зі злочинами проти власності, злочинами у сфері господарської діяльності, порушеннями митних правил та іншими правопорушеннями, що здійснюються у сфері телекомунікаційних технологій і послуг. Віддаючи належне досягненням вказаних вчених, у роботі вважаємо за доцільне акцентувати увагу на дослідженні організаційно-правових засад протидії правопорушенням у сфері використання терміналів рухомого зв'язку в Україні.

Цілком закономірним постає аналіз чинного законодавства України щодо регулювання відносин в даній сфері. На сьогоднішній день регламентовано порядок ввезення з-за кордону, реалізації та застосування терміналів в Україні [9; 10, ст.25-26; 11, ст.24; 12-16; 17, ст.4]. За порушення цих норм передбачена адміністративна та кримінальна відповідальність [18, ст.146, ст.148-3, ст.148-4; 19, Розділ XVIII]. Звичайно, встановлена кримінальна відповідальність й за вчинення злочинів проти власності, предметом посягання яких є термінали [19, Розділ VI]. Водночас слід зазна-

чити, що ґрунтовний аналіз особливостей зазначених правопорушень дозволив дійти висновку про необхідності подальшого вдосконалення не лише правозастосування цих норм, але й самого законодавства. Це підтверджується також відповідними даними щодо недостатнього рівня боротьби зі злочинами у сфері використання терміналів рухомого зв'язку в Україні [5, 7].

Наукова новизна роботи полягає у комплексному підході до вирішення проблеми протидії правопорушенням у сфері використання терміналів в Україні, який виявляється в інтеграції знань у галузі адміністративного й інформаційного права, а також сучасних досліджень у сфері розробки та експлуатації новітніх інформаційно-телекомунікаційних технологій. Саме з'ясування особливостей побудови та функціонування мереж рухомого зв'язку дозволили по-новому визначити шляхи упорядкування суспільних відносин між органами державної влади України, операторами телекомунікацій, що здійснюють діяльність з надання послуг рухомого зв'язку (далі – операторами) та споживачами телекомунікаційних послуг рухомого зв'язку (далі – абонентами), а також запропонувати відповідні зміни до законодавства України задля впровадження ефективного інструменту протидії правопорушенням у зазначеній сфері – ІМЕІ-контролю. До новачій роботи, на наш погляд, слід віднести і системне дослідження правопорушень у сфері використання терміналів в Україні; що сприяло чіткому визначенню мети роботи (яка має три невід'ємні складові), та досягнення якої потребувало розробки організаційно-правових засад єдиної концепції протидії цим правопорушенням.

Отже, мета даного дослідження полягає у розробці організаційно-правових засад єдиної концепції протидії:

- злочинам проти власності, предметом посягання яких є термінали;
- контрабанді терміналів та порушенням митних правил при їх ввезенні (пересиланні) на митну територію України;
- ввезенню з-за кордону, реалізації та за-

стосуванню (використанню) терміналів без додержання відповідних умов нормативних документів у сфері телекомунікацій.

Передусім, вважаємо за доцільне дослідити окремі особливості побудови й функціонування мереж рухомого зв'язку. Кожному терміналу при виробництві присвоюється унікальний міжнародний ідентифікаційний номер – International Mobile Equipment Identity (далі – ІМЕІ) [20, с.166]. Цей номер містить у собі відомості щодо країни виготовлення, моделі, кінцевого виробника та серійного номеру терміналу [5; 6, с.25-26; 7; 21].

При використанні терміналу, при процедурі реєстрації та при всіх з'єднаннях абонента, ІМЕІ передається в мережу оператора телекомунікацій, який здійснює діяльність з надання послуг рухомого зв'язку (далі – оператор). Після отримання мережею, що являє собою комплекс програмно-технічних засобів, ІМЕІ направляється до реєстру ідентифікації обладнання – Equipment Identity Register (далі – реєстр оператора). Реєстр оператора відповідає за допуск терміналів до використання, містить централізовану базу даних, що складається зі списків, які організовані в такий спосіб:

- “чорний список” призначений для розміщення відомостей про ІМЕІ терміналів, які з якої-небудь причини не можуть використовуватися в мережі, іншими словами робота яких буде блокуватися оператором;
- “білий список” – для ІМЕІ терміналів, що можуть застосовуватися в мережі;
- “сірий список” – для ІМЕІ терміналів, що можуть застосовуватися в мережі, але за якими ведеться постійне спостереження програмно-технічними засобами оператора.

Ці особливості побудови та функціонування передбачені стандартом рухомого зв'язку, отже властиві всім мережам в світі [22, с.330-334; 23, с.62-63]. Ми вбачаємо в них ефективний інструмент протидії правопорушенням у сфері використання терміналів рухомого зв'язку.

Так, якщо внести ІМЕІ викрадених терміналів до “чорних списків” реєстрів вітчизня-

них операторів, можна виключити технічну можливість їх використання після здійснення злочину на території країни. Це, в свою чергу, призупинить розвиток вторинного ринку “кримінальних” терміналів і, як наслідок, призведе до гарантованого зменшення числа злочинів проти власності, що пов’язані з їх незаконним заволодінням.

Формування ж “білих списків” реєстрів операторів виключно ІМЕІ терміналів, які пройшли митне оформлення в установленому законом порядку та відповідають умовам нормативних документів у сфері телекомунікацій, виключить економічну доцільність ввезення з-за кордону, реалізації та застосування терміналів з порушеннями норм діючого законодавства.

Таким чином, мережі рухомого зв’язку містять у собі вбудований механізм, застосування якого не вимагає від оператора відчужених технічних і прямих матеріальних витрат, практично дозволяє виявляти та блокувати роботу наступних категорій терміналів (далі – ІМЕІ-контроль):

- що є викраденими;
- що не проходили митного оформлення в установленому законом порядку;
- що не відповідають умовам нормативних документів у сфері телекомунікацій.

Проте, сьогодні нормами діючого законодавства безпосередньо не передбачені підстави для введення ІМЕІ-контролю в Україні [10, 11, 24-26], й всі оператори тільки реєструють ІМЕІ терміналів, що застосовуються їх абонентами.

Впровадження ж ІМЕІ-контролю в Україні, на нашу думку, вимагає в першу чергу вирішення двох наступних задач:

1) пошук ефективного механізму збору й обробки відомостей щодо терміналів, їх ввезення до списків реєстрів операторів;

2) визначення правових підстав для зобов’язання операторів вести облік відомостей щодо терміналів у списках власних реєстрів та на їх підставі обмежувати доступ споживачів (далі – абоненти) до телекомунікаційних

послуг рухомого зв’язку без наявності їх відповідного волевиявлення.

Як зазначалося вище, необхідною умовою здійснення ІМЕІ-контролю є постійна робота по формуванню списків реєстрів операторів відомостями про розглянуті категорії терміналів. Це, в свою чергу, потребує початкового збору інформації, організацію та проведення якого ми пропонуємо покласти на відповідні державні органи.

Так, запобігання незаконному заволодінню терміналами відноситься до основних завдань та обов’язків міліції в Україні [27, п.2 ст.2, п.2 ст.10]. У той же час, у Міністерстві внутрішніх справ України (далі – МВС) розроблений та функціонує Автоматизований банк даних, в якому серед іншого накопичується інформація про всі викрадені на території держави термінали, що наочно представлено на рис. [27, п.13 ст.11; 28; 29; 30, с.474-493]. Отже, МВС вже сьогодні без додаткових витрат з Державного бюджету України (далі – бюджет) спроможне надавати відомості щодо ІМЕІ викрадених терміналів для формування “чорних списків” реєстрів операторів.

Важливо відмітити, що ІМЕІ-контроль не один рік використовується для боротьби з крадіжками терміналів у Великобританії [31-33]. Результатом цього нововведення стало зниження кількості злочинів даної категорії на 95 % [34-36]. Безсумнівно, що британський опит впровадження та застосування ІМЕІ-контролю в частині його організаційного, правового, технічного забезпечення необхідно ретельно аналізувати та запозичати.

Однак, як свідчить той же світовий досвід, остаточне вирішення питання термінального злодійства лише через введення ІМЕІ-контролю на національному рівні малоімовірно [32, 34-35]. Причина цього – можливість реалізації та використання викрадених терміналів за межами України. Безумовне домінування мереж рухомого зв’язку розглянутого стандарту у світі й, особливо, на пострадянському просторі створює широкий ринок збуту викраденого [1, с.9; 4].

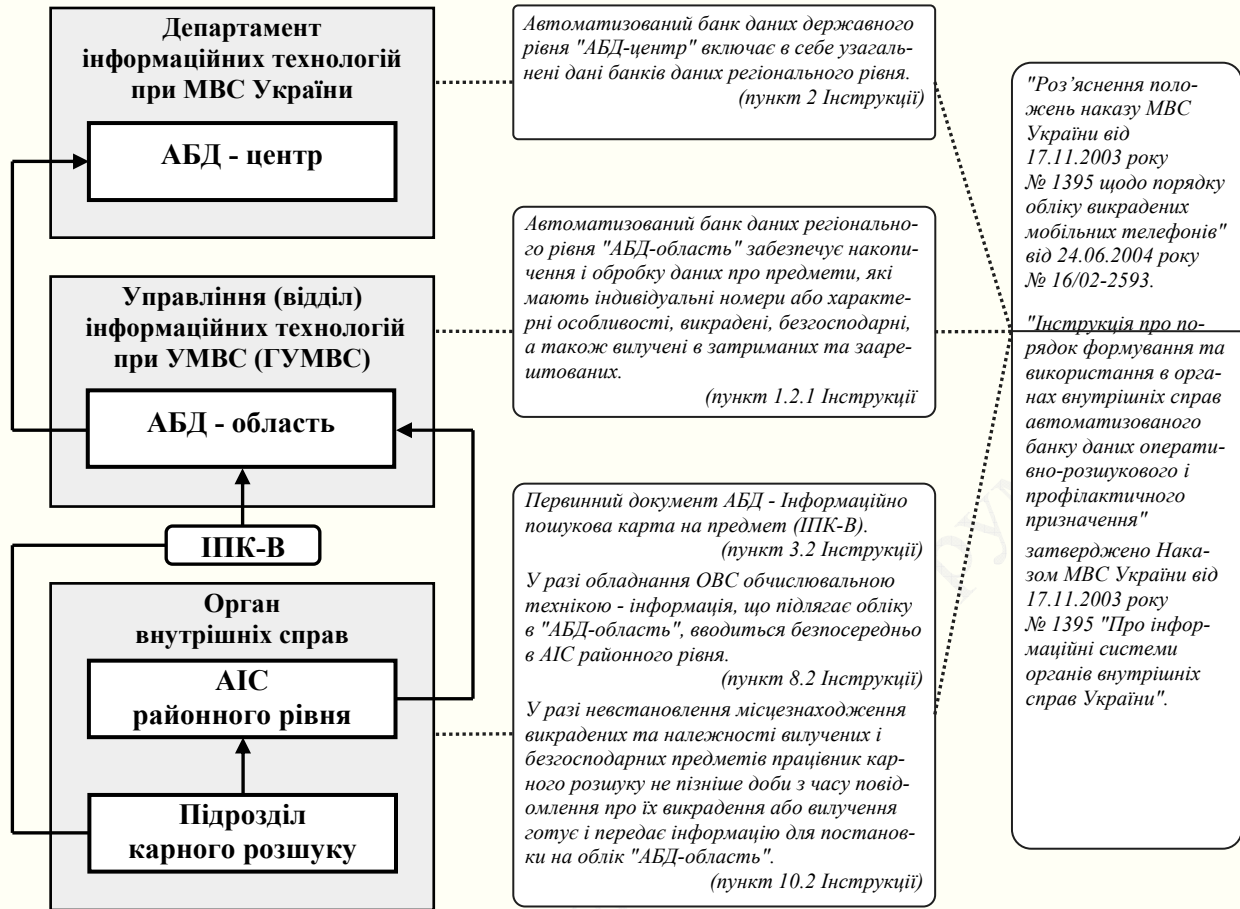


Рисунок - Схема організації та функціонування Автоматизованого банку даних МВС України щодо накопичення відомостей про викрадені термінали рухомого зв'язку

Враховуючи вищевикладене, приходимо до висновку, що ефективно вирішення проблеми протидії злочинам проти власності, предметом посягання яких є термінали, на території України не можливо без міжнародного співробітництва. Тим більше, що таке починання вже є – з метою міждержавного обміну інформацією про викрадені термінали створено Центральний реєстр ідентифікації обладнання (Central Equipment Identity Register), і європейські країни на його підставі починають впроваджувати IMEI-контроль [7; 32-34; 36].

Дослідження показали, що боротьба з контрабандою терміналів та порушеннями митних правил при їх ввезенні (пересиланні) на митну територію України (далі – контрабанда) в умовах бурхливого розвитку рухомого зв'язку постає одним із важливих завдань ми-

тних органів України [7; 12, п.10 ч.2 ст.11]. Вважаємо, що його успішне вирішення можливе, серед іншого, і шляхом зобов'язання митних органів створити інформаційну систему для накопичення відомостей про термінали, які пройшли митне оформлення в установленому законом порядку, з метою подальшого формування "білих списків" реєстрів операторів. Координацію цих робіт доречно доручити Держаній митній службі України (далі – ДМС).

З огляду на представлені на Восьмій міжнародній науково-практичній конференції "Ринок послуг комплексних транспортних систем і проблеми логістики" напрацювання ДМС у створенні багатфункціональної комплексної інформаційної системи "Електронна митниця", вважаємо за доцільне саме з допомогою її підсистем організувати ведення об-

ліку відомостей про термінали [37].

Щодо терміналів, які функціонуватимуть на території України до моменту впровадження зазначених нововведень, будемо вважати їх такими, що пройшли митне оформлення в установленому законом порядку, тобто ми пропонуємо автоматично внести їх ІМЕІ до “білих списків” реєстрів операторів, звісно, якщо це у кожному окремому випадку не буде суперечити чинному законодавству України в інших сферах.

Реалізація даних пропозицій потребує фінансування та внесення відповідних змін і доповнень до сукупності норм, встановлених законодавством України з питань митної справи, що залежно від заявленої мети переміщення терміналів через митний кордон України визначають порядок такого переміщення й обсяг митних процедур, які при цьому здійснюються [9, 12, 16-17]. Безумовно, це питання потребує більш ґрунтовного наукового дослідження.

Слід зауважити, що теоретично проблему контрабанди можна вирішити шляхом скасування ввізного мита на термінали. Але, за нашим переконанням, це неприпустимо, оскільки позбавляє бюджет перспективного джерела наповнення та буквально анулює й без того низьку ймовірність появи вітчизняного виробника терміналів. Таким чином, застосування ІМЕІ-контролю для протидії контрабанді терміналів з часом дозволить Україні отримати відчутні економічні вигоди.

Зважаючи на третю складову мети дослідження, тобто протидію застосуванню (використанню) терміналів, які не відповідають умовам нормативних документів у сфері телекомунікацій, то спочатку охарактеризуємо ці порушення:

- відсутність у конкретного типу терміналу документального підтвердження відповідності стандартам і технічним регламентам, виданих акредитованими в установленому порядку органами сертифікації, уповноваженими на проведення цієї діяльності, перелік яких узгоджується з Національною комісією з питань регулювання зв'язку України (далі – НКРЗ) [10, п.2 ч.1, ч.2 ст.25; 11, ч.1, 2, 9

ст.24];

- невключення конкретного типу терміналу до реєстру радіоелектронних засобів та випромінювальних пристроїв, що можуть застосовуватися на території України в смугах радіочастот загального користування, який веде НКРЗ (далі – Реєстр НКРЗ) [10, п.1 ч.1, ч.3 ст.25; 14]. Слід підкреслити, що внесення конкретного типу терміналу до Реєстру НКРЗ – це одна з необхідних умов для проведення його сертифікації [14, п.2.8].

Контроль за недопущенням вказаних порушень, а також встановлення порядку реалізації, застосування терміналів на території України, порядку їх ввезення з-за кордону та координацію робіт з підтвердження їх відповідності здійснює НКРЗ [10, п.п.10, 11 ч.2 ст.14; 11, ч.7 ст.24; 13-15]. Саме в межах здійснення даних повноважень у Реєстрі НКРЗ накопичуються масиви інформації щодо конкретних типів терміналів, застосування яких не суперечить законодавству України в сфері телекомунікацій [14, п.2.3]. Звідси випливає можливість НКРЗ в автоматичному режимі генерувати ІМЕІ кожної дозволеної до застосування одиниці терміналів [5; 6, с.25-26; 7; 21]. Як зазначалося вище, задля забезпечення використання ІМЕІ-контролю щодо протидії правопорушенням даного виду ці відомості підлягають обов'язковому внесенню до “білих списків” реєстрів операторів.

З цього питання важливо додати, що з метою підвищення рівня національної безпеки, запобігання розповсюдженню ввезення з-за кордону та реалізації терміналів з порушенням законодавства України, сприяння захисту українського ринку від неякісних і заборонених до використання терміналів поряд з веденням Реєстру НКРЗ комісією запроваджуються “додаткові заходи” [13, п.4; 15, п.4]. Вони полягають в обов'язковому подвійному маркуванні терміналів: захисними знаками й обліковими марками [13, п.1.5, п.1.7; 15, п.1.6].

Проаналізуємо докладніше процес маркування терміналів обліковими марками. “Облікова марка – контрольна етикетка одноразового використання з нанесеними даними кон-

трольно-облікової інформації у вигляді дво-мірного штрихового коду, який дозволяє в автоматизованому режимі ідентифікувати кожну промарковану одиницю ...” терміналів [13, п.1.6; 15, п.1.8]. Отже процес маркування терміналів обліковими марками забезпечує накопичення відомостей про кожну одиницю дозволених до використання на території України терміналів. Таким чином, проявляється ще один механізм організації обліку відомостей про термінали, що відповідають умовам нормативних документів у сфері телекомунікацій, який, у свою чергу, також можна використовувати для забезпечення функціонування ІМЕІ-контролю.

На підставі вищевикладеного, можна зробити висновок, що організація НКРЗ збору й обробки інформації про зазначену категорію терміналів, є практично реалізуємою та відповідає діючим законам України в сфері телекомунікацій [10, 11]. Цілком зрозуміло, що остаточне висвітлення всіх проблемних аспектів з цього приводу потребує окремих досліджень та ймовірних послідовних корегувань відповідних нормативних актів НКРЗ.

Розглянемо питання організації безпосереднього внесення відомостей про термінали з інформаційних обліків МВС, ДМС і НКРЗ до списків реєстрів операторів. На нашу думку, для його вирішення варто навести окремі повноваження НКРЗ:

- внесення пропозицій до органів державної влади щодо проектів законів та інших нормативно-правових актів, стандартів у сфері телекомунікацій [11, п.1 ч.1 ст.18];

- видання нормативних актів з питань, що належать до компетенції НКРЗ, та контроль за їх виконанням [10, п.2 ч.2 ст.14; 11, п.2 ч.1 ст.18];

- забезпечення державного нагляду за додержанням операторами законодавства про телекомунікації [11, п.3 ч.1 ст.18];

- ліцензування у сфері надання телекомунікаційних послуг та у сфері користування радіочастотним ресурсом [10, п.1 ч.2 ст.14; 11, п.4 ч.1 ст.18];

- здійснення організаційно-правового забезпечення загальнодоступних телекомуніка-

ційних послуг [11, п.9 ч.1 ст.18];

- прийняття в межах компетенції рішень, які є обов'язковими для виконання операторами [11, п.12 ч.1 ст.18];

- застосування до операторів і абонентів адміністративних стягнень, інших санкцій у порядку, передбаченому законом [10, п.15 ч.2 ст.14; 11, п.13 ч.1 ст.18, п.3 ч.3 ст.19];

- звернення до суду з відповідними позовними заявами в разі порушення операторами законодавства про телекомунікації [11, п.15 ч.1 ст.18];

- здійснює співробітництво з відповідними органами регулювання у сфері телекомунікацій інших держав [11, п.22 ч.1 ст.18].

Враховуючи обсяги та зміст даних повноважень, вважаємо за доцільне на НКРЗ, як на центральний орган виконавчої влади зі спеціальним статусом, що підконтрольний Президенту України, здійснює регулювання у сфері телекомунікацій і користування радіочастотним ресурсом України (у смугах радіочастот загального користування) [10, ст.12; 11, ст.17], покласти всі організаційні заходи щодо введення та забезпечення функціонування ІМЕІ-контролю. Основними з них є:

- взаємодія з МВС та ДМС задля отримання, подальшої обробки й аналізу інформації щодо терміналів тощо;

- взаємодія з операторами з метою формування списків їх реєстрів тощо;

- нагляд за здійсненням операторами ІМЕІ-контролю;

- міжнародне співробітництво з метою обміну інформацією про термінали тощо.

Досягнення мети даної роботи потребує розв'язання задачі дослідження правових підстав впровадження ІМЕІ-контролю в Україні. Для розробки правового забезпечення взаємодії НКРЗ, МВС та ДМС щодо формування загальних інформаційних масивів, на наш погляд, не існує принципових труднощів: спільна розробка положення (інструкції) цими державними органами або відповідний нормативно-правовий акт Кабінету Міністрів України (далі – КМУ) може вирішити всі неузгодженості.

Вважається, що існують проблеми право-

вого регулювання діяльності операторів з виконання умов ІМЕІ-контролю. Адже, як зазначалося вище, в чинних законах України відсутні відповідні правові норми [10; 11]. Проте, ми не бачимо необхідності у численних нововведеннях до законів, що здійснюють регулювання у сфері телекомунікацій та користування радіочастотним ресурсом України, задля закріплення обов'язків операторів щодо здійснення ІМЕІ-контролю [10, ч.2 ст.6; 11, ст.39]. Діюче законодавство передбачає ліцензування діяльності операторів НКРЗ, і ми вважаємо, що саме цей інститут дозволяє реалізувати ІМЕІ-контроль на Україні [10, п.1 ч.2 ст.30; 11, ч.2, п.2 ч.3 ст.42; 25, п.1.1; 26, п.1.1].

Обґрунтуємо цю позицію. Оператор може здійснювати свою діяльність тільки на підставі ліцензії, повинен виконувати весь перелік організаційних, кваліфікаційних, технологічних та інших спеціальних вимог ліцензійних умов [10, п.2 ч.2 ст.6, ч.1 ст.36; 11, п.1 ч.1 ст.39, ч.1 ст.44; 25, п.1.2 - 1.6; 26, п.1.2 - 1.5]. НКРЗ повноважне розширювати вказаний перелік вимог додатковими умовами та обов'язками [11, п.18 ч.1 ст.39, ч.2, ч.3 ст.44; 25, п.4.2]. Ми пропонуємо, до "Ліцензійних умов здійснення діяльності у сфері телекомунікацій з надання послуг рухомого (мобільного) телефонного зв'язку з правом технічного обслуговування та експлуатації телекомунікаційних мереж і надання в користування каналів електров'язку" [25] включити особливі умови, які зобов'язують операторів:

- за наданими НКРЗ відомостями щодо терміналів, які є викраденими, пройшли митне оформлення в установленому законом порядку, відповідають умовам нормативних документів у сфері телекомунікацій, формувати відповідні списки власних реєстрів;

- здійснювати власними програмно-технічними засобами постійний контроль за ІМЕІ терміналів, що використовуються у власних мережах;

- блокувати у власних мережах роботу терміналів, що стоять на обліку в "чорних списках" власних реєстрів операторів або не стоять на обліку в "білих списках";

- заносити до "сірих списків" власних реєстрів термінали з однаковими ІМЕІ, надавати дані відомості до НКРЗ;

- вести облік відомостей про спроби використання у власних мережах терміналів, що стоять на обліку в "чорних списках" реєстрів операторів або не стоять на обліку в "білих списках", надавати дані відомості до НКРЗ.

Необхідно підкреслити, що наведені пропозиції відносно організаційно-правових заasad функціонування ІМЕІ-контролю повною мірою спираються на діючий механізм адміністративно-правового впливу на операторів, що здійснюється НКРЗ у межах чинного законодавства України.

Разом із тим, остаточне вирішення питання правового забезпечення впровадження ІМЕІ-контролю в Україні потребує дослідження підстав та законності обмеження операторами доступу до телекомунікаційних послуг рухомого зв'язку без наявності відповідного волевиявлення абонентів.

Проаналізуємо з цього приводу норми Закону України від 18.11.2003 р. № 1280-IV "Про телекомунікації" [11] (далі – Закон) та "Правил надання та отримання телекомунікаційних послуг", затверджених Постановою КМУ від 09.08.2005 року № 720 [24] (далі – Правила).

Абоненти операторів рухомого зв'язку зобов'язані:

- "...дотримуватися Правил надання та отримання телекомунікаційних послуг, що затверджує Кабінет Міністрів України (720-2005-п), зокрема:

- 1) використовувати кінцеве обладнання, що має документ про підтвердження відповідності;

- 2) не допускати використання кінцевого обладнання споживача для вчинення протиправних дій або дій, що суперечать інтересам національної безпеки, оборони та охорони правопорядку;

- 3) не допускати дій, що можуть створювати загрозу для безпеки експлуатації мереж телекомунікацій, підтримки цілісності та взаємодії мереж телекомунікацій, захисту інформаційної безпеки мереж телекомунікацій,

електромагнітної сумісності радіоелектронних засобів, ускладнювати чи унеможливити надання послуг іншим споживачам...” [11, п.1-3 ч.1 ст.33];

- “...повідомляти на запит оператора, провайдера тип кінцевого обладнання, що використовується для отримання телекомунікаційних послуг...” [24, п.32].

В свою чергу оператори мають право:

- на “...скорочення переліку або припинення надання телекомунікаційних послуг споживачам, які порушують правила надання і отримання телекомунікаційних послуг, або на відключення кінцевого обладнання споживача, якщо воно не має виданого в установленому законодавством порядку документа про підтвердження відповідності вимогам нормативних документів у сфері телекомунікацій, у порядку, визначеному цими правилами ...” [11, п.8 ч.1 ст.38];

- на “... відключення на підставі рішення суду кінцевого обладнання, якщо воно використовується абонентом для вчинення протиправних дій або дій, що загрожують інтересам державної безпеки ...” [11, п.9 ч.1 ст.38];

- “... не підключати до телекомунікаційної мережі кінцеве обладнання у разі відсутності документів про підтвердження його відповідності вимогам нормативних документів у сфері телекомунікацій...” [24, п.27];

- відключати термінали абонентів: “...у разі відсутності виданого в установленому законодавством порядку документа про підтвердження його відповідності вимогам нормативних документів у сфері телекомунікацій; на підставі рішення суду, якщо це обладнання використовується абонентом для вчинення протиправних дій або дій, що загрожують інтересам державної безпеки;...” [24, п.27].

Узагальнюючи розглянуте, зазначимо, що Закон та Правила:

1) містять практично тотожні за змістом норми щодо повноважень операторів і обов’язків абонентів у сфері використання терміналів;

2) прямо вказують на право оператора відключати (не підключати) у власних мережах термінали:

- які не мають документів про підтвердження їх відповідності вимогам нормативних документів у сфері телекомунікацій;

- які використовуються абонентом для вчинення протиправних дій або дій, що загрожують інтересам державної безпеки, при наявності відповідного судового рішення.

Таким чином, впровадження та застосування ІМЕІ-контролю для протидії правопорушенням, пов’язаним з використанням терміналів, які не відповідають умовам нормативних документів у сфері телекомунікацій, однозначно відповідає вимогам чинного законодавства України. Тобто оператори повноважні блокувати у власних мережах роботу таких терміналів, що за наданими НКРЗ відомостями не стоять на обліку в “білих списках” реєстрів операторів.

Відносно вирішення питання про законність блокування викрадених терміналів доцільно звернутися до Правил: “У разі втрати абонентом кінцевого обладнання або SIM-карти оператор за усною заявою абонента припиняє обслуговування цього кінцевого обладнання або SIM-карти Повідомлення про втрату кінцевого обладнання або SIM-карти абонент повинен підтвердити також письмово. У разі звернення або скарги з приводу припинення обслуговування кінцевого обладнання або SIM-карти надання послуг відновлюється і може бути припинено повторно тільки за письмовою заявою абонента” [24, п.225].

Отже Правила передбачають блокування терміналів операторами за заявою абонента, визначають його порядок. Доведення ж відомостей про викрадені термінали з метою їх блокування до операторів через МВС, за нашим переконанням, не обмежує прав абонентів, не суперечить чинному законодавству України у сфері телекомунікацій.

З іншого боку ми визнаємо, що цей висновок має дискусійний характер. Тому для остаточного розв’язання проблеми щодо законності блокування оператором, як викрадених терміналів, так і тих, що не проходили митного оформлення в установленому законом порядку, ми пропонуємо скористатися іншими

нормами законодавства у сфері телекомунікацій.

Безперечним є той факт, що злочини проти власності та контрабанда, предметом яких являються термінали, є загрозою інтересам “національної безпеки”, “державної безпеки” й “охорони правопорядку”. Отже НКРЗ може звернутися до суду з відповідною позовною заявою про законність блокування роботи цих категорій терміналів операторами. Рішення суду в рамках чинного законодавства України остаточно визначить законність впровадження ІМЕІ-контролю в частині його використання для протидії:

- злочинам проти власності, предметом посягання яких є термінали;
- контрабанді терміналів та порушенням митних правил при їх ввезенні (пересиланні) на митну територію України.

В разі визнання судом неправомірності введення ІМЕІ-контролю повністю або в який-небудь частині, постанова суду слугуватиме відправним базисом для подальших наукових досліджень з приводу реформування діючого законодавства України.

У рамках дослідження засад впровадження ІМЕІ-контролю в Україні не можна не розглядати той факт, що існує можливість несанкціонованої зміни, подробиці ІМЕІ терміналу, який встановлений його виробником (далі – зміна ІМЕІ), за допомогою персонального комп’ютера, спеціальних програмно-технічних засобів тощо [5; 6, с.26; 7; 34; 36; 38-39]. Це може робитися з метою приховування “зв’язків” терміналу з правопорушеннями, викликати появу терміналів з однаковими ІМЕІ [5, 7, 39]. Особливо це актуально в умовах організованої скупки викрадених терміналів, їх реалізації та застосування без проходження митного оформлення в установленому законом порядку та без додержання відповідних умов нормативних документів у сфері телекомунікацій [5, 7].

З метою запобігання змінам ІМЕІ терміналів пропонуємо визнати їх кримінальними злочинами, адже на даний час чинним законодавством України безпосередньо за такі дії юридична відповідальність не передбачена.

Проте, ми не є прихильниками доповнення Кримінального кодексу України (далі – ККУ) додатковою статтею, що буде визначати новий склад злочину. На нашу думку, питання кваліфікації діянь, що пов’язані зі зміною ІМЕІ, може вирішуватися на основі діючого законодавства України про кримінальну відповідальність – статей Розділу XVI ККУ “Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку” [19]. В той же час, вказана пропозиція залишиться нездійсненою без напрацювання відповідних методик експертних досліджень, оперативно-розшукової, слідчої та судової практик, а отже потребує окремих ретельних наукових досліджень.

Щодо терміналів з однаковими ІМЕІ, то, на нашу думку, їх роботу слід блокувати, але кожний такий випадок повинен спочатку розглядатися правоохоронними органами та НКРЗ в межах чинного законодавства України. Вважаємо, що зазначені вимоги сприятимуть впровадженню та дієвому функціонуванню ІМЕІ-контролю.

Слід зауважити, що на сьогодні діяльність суб’єктів господарювання з ремонту та технічного обслуговування як апаратних, так і програмних складових терміналів (далі – ремонт та сервіс), що може бути безпосередньо пов’язана зі зміною ІМЕІ, здійснюється взагалі без контролю з боку органів державної влади. Зазначимо, що некомпетентне втручання в роботу терміналу може призвести не тільки до його некоректного функціонування, а навіть завдати шкоди здоров’ю користувача. Це питання може бути вирішено, базуючись прикладі діючого порядку оптової та роздрібно-реалізації терміналів на території України: ремонт та сервіс терміналів повинен здійснюватися тільки на дозвільній основі в порядку, передбаченому НКРЗ [10, п.10 ч.2 ст.14; 15, п.1.3; 18, ст.146]. Причому в особливих умовах дозволу повинні бути вказані перелік послуг, що можуть надаватися, конкретні типи терміналів, ремонт та сервіс яких дозволяється суб’єкту господарювання [15, п.1.4].

На нашу думку, мета дослідження досяг-

нута, а саме: визначено основні організаційно-правові засади протидії правопорушенням у сфері використання терміналів рухомого зв'язку, чітко сформульовані напрямки діяльності з впровадження ІМЕІ-контролю на Україні, переконливо доведена нагальна необхідність та практична здійснимість його введення, що дозволить:

1) ефективно попереджувати:

- злочини проти власності, предметом посягання яких є термінали;
- злочини у сфері господарської діяльності – контрабанду терміналів, порушення митних правил при їх ввезенні (пересиланні) на митну територію України;
- порушення умов нормативних документів у сфері телекомунікацій при ввезенні з-за кордону, реалізації та застосуванні (використанні) терміналів на території України;

2) отримати економічні вигоди для України:

- зменшити витрати з бюджету на боротьбу з вищевказаними правопорушеннями;
- збільшити державні доходи за рахунок зростання обсягів виплат ввізного мита на термінали, платежів і зборів, які передбачені нормативними документами у сфері телекомунікацій при ввезенні з-за кордону, реалізації та застосуванні (використанні) терміналів на території України;
- стимулювати появу вітчизняного виробника терміналів;

3) захистити вітчизняного споживача:

- від застосування терміналів, що не відповідають умовам нормативних документів у сфері телекомунікацій;
- від отримання неякісних послуг з ремонту та технічного обслуговування програмно-апаратних складових терміналів.

Вважаємо за необхідне наголосити, що ґрунтовний аналіз чинного законодавства України дозволив дійти висновку про існування відповідних положень підзаконних нормативно-правових актів, що відповідають діючим законам України, дозволяють шляхом їх певного корегування та доповнення здійснити ефективну процедуру введення ІМЕІ-контролю. Крім того варто додати, що ІМЕІ-

контроль можна застосовувати щодо протидії окремим із зазначених видів правопорушень, тобто впроваджувати його поступово.

Слід підкреслити, що деякі сформульовані у даній роботі положення мають дискусійний характер і можуть виступати підставою для подальших наукових досліджень цієї проблеми. Вбачаємо за доцільне зорієнтувати науковий пошук за наступними напрямками:

- аналіз світового досвіду впровадження та використання ІМЕІ-контролю в частині його організаційного, правового, технічного забезпечення;

- вирішення питань узгодженості організаційно-правового забезпечення використання ІМЕІ-контролю для блокування контрабандних терміналів та вимог сукупності правових норм, встановлених законодавством України з питань митної справи, що залежно від заявленої мети переміщення терміналів через митний кордон України визначають порядок такого переміщення й обсяг митних процедур, які при цьому здійснюються;

- визначення механізму організації та правового забезпечення збору НКРЗ відомостей про термінали, які відповідають умовам нормативних документів у сфері телекомунікацій;

- розв'язання теоретичних та прикладних проблем кваліфікації діянь, що пов'язані зі зміною ІМЕІ терміналів, як злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електров'язку.

ЛІТЕРАТУРА

1. Горностаев Ю.М. Перспективные рынки мобильной связи: Сер. "Связь и бизнес". –М.: МЦНТИ, ООО "Мобильные коммуникации", 2000. –213 с.

2. Сотовая статистика // Мир связи. –2006. -№ 2. -С.10.

3. Число абонентов мобильной связи в Украине в сентябре с. г. выросло на 1,6 % – до 53,588 млн. человек /Международная Маркетинговая Группа [Электронный ресурс]. - Режим доступа: <http://www.rbc.ua/rus/>

newsline/2007/10/16/253340.shtml.

4. GSM subscriber statistics. GSM Association 2007 –URL: [http://uk.sitestat.com/gsm/gsmworld/s?Stats_Q1_2007&ns_type=pdf&ns_url=\[http://www.gsmworld.com/news/statistics/pdf/gsma_stats_q1_07.pdf](http://uk.sitestat.com/gsm/gsmworld/s?Stats_Q1_2007&ns_type=pdf&ns_url=[http://www.gsmworld.com/news/statistics/pdf/gsma_stats_q1_07.pdf).

5. Дубецький А. Мобілки без стоп-крану /Перша щоденна газета “Поступ” [Електронний ресурс]. -Режим доступу: <http://postup.net.ua/articles/item;1174/?r=29&df=&dt=&k=>. -08.02.2006 р.

6. Маркович А. Мобильная связь без секретов. –М.: ЗАО “Новый издательский дом”, 2004. –352 с.

7. Степанчиков С. Невловими “трубки”. Борьба з крадіжками мобільних телефонів зайшла в глухий кут. Потрібні радикальні заходи // Дзеркало тижня. -03.2006. -№ 7.

8. Is mobile phone theft a bigger issue now than in the past? FAQ's. The Mobile Industry Crime Action Forum. –URL: http://www.micaf.co.uk/home.asp?Page_Info=13.

9. Закон України “Про порядок ввезення (пересилання) в Україну, митного оформлення й оподаткування особистих речей, товарів та транспортних засобів, що ввозяться (пересилаються) громадянами на митну територію України” від 13.09.2001 р., № 2681-III // ВВР України. –2002. –№ 1. –Ст.2.

10. Закон України “Про радіочастотний ресурс України” від 01.06.2000 р., № 1770-III // ВВР України. –2000. –№ 36. –Ст.298.

11. Закон України “Про телекомунікації” від 18.11.2003 р., № 1280-IV // ВВР України. –2004. –№ 12. –Ст.155.

12. Митний кодекс України 11.07.2002 р., № 92-IV // ВВР України. –2002. –№ 38. –Ст.288.

13. Положення про надання дозволів на ввезення з-за кордону в Україну радіоелектронних засобів та випромінювальних пристроїв /Затв. Рішенням Національної комісії з питань регулювання зв'язку України “Про затвердження Положення про надання дозволів на ввезення з-за кордону в Україну радіоелектронних засобів та випромінювальних пристроїв” від 20.06.2007 р., № 802 // Офіційний вісник України. –2007. –№ 51. –Ст.2073.

14. Положення про порядок і форму ведення реєстру радіоелектронних засобів та випромінювальних пристроїв, що можуть застосовуватися на території України в смугах радіочастот загального користування /Затв. Рішенням Національної комісії з питань регулювання зв'язку України “Про затвердження Положення про порядок і форму ведення реєстру радіоелектронних засобів та випромінювальних пристроїв, що можуть застосовуватися на території України в смугах радіочастот загального користування” від 03.11.2005 р., № 117 // Офіційний вісник України. –2006. –№ 1. –Ст.63.

15. Порядок реалізації в Україні радіоелектронних засобів та випромінювальних пристроїв /Затв. Рішенням Національної комісії з питань регулювання зв'язку України “Про затвердження Порядку реалізації в Україні радіоелектронних засобів та випромінювальних пристроїв” від 20.06.2007 р., № 803 // Офіційний вісник України. –2007. –№ 51. –Ст.2074.

16. Постанова Кабінету Міністрів України “Про обсяги та порядок ввезення громадянами на митну територію України продуктів харчування для власного споживання та перелік предметів, що не можуть бути віднесені до особистих речей громадян” від 13.12.2001 р., № 1652 // Офіційний вісник України. –2001. –№ 51. –Ст.2273.

17. Угода щодо співробітництва у розвитку та використанні систем стільникового рухомого зв'язку від 17.01.1997 р. /Ратифіковано Законом України від 03.03.1998 р., № 149/98-ВР // ВВР України. –1998. –№ 26. –Ст.165.

18. Кодекс України про адміністративні правопорушення від 07.12.1984 р., № 8073-X [Електронний ресурс]. -Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=80731%2D10&p=1187700748298790>.

19. Кримінальний кодекс України від 05.04.2001 р., № 2341-III [Електронний ресурс]. -Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341%2D14&p=1187700748298790>.

20. Ипатов В.П., Орлов В.К., Самолов И.М., Смирнов В.Н. Системы мобильной свя-

зи: Учебное пособие /Под ред. Ипатов В.П. – М.: Горячая линия-Телеком, 2003. –272 с.

21. International Mobile Equipment Identity (IMEI). The National Mobile Phone Crime Unit. –URL: <http://www.met.police.uk/mobilephone/imei.htm>.

22. Стекло В.К., Беркман Л.Н. Нові інформаційні технології: Транспортні мережі телекомунікацій. –К.: Техніка, 2004. –486 с.

23. Чекалин А.А., Заряев А.В., Скрыль С.В., Вохминцев В.А., Обухов А.Н., Хохлов Н.С., Немцов А.Д., Щербаков В.Б., Потанин В.Е. Защита информации в системах мобильной связи: Учебное пособие /Под общ. ред. А.В. Заряева, С.В. Скрыля. –М.: Горячая линия-Телеком, 2005. –171 с.

24. Правила надання та отримання телекомунікаційних послуг /Затв. Постановою Кабінету Міністрів України “Про затвердження Правил надання та отримання телекомунікаційних послуг” від 09.08.2005 р., № 720 // Офіційний вісник України. –2005. –№ 32. –Ст.1935.

25. Ліцензійні умови здійснення діяльності у сфері телекомунікацій з надання послуг рухомого (мобільного) телефонного зв'язку з правом технічного обслуговування та експлуатації телекомунікаційних мереж і надання в користування каналів електрозв'язку /Затв. Рішенням Національної комісії з питань регулювання зв'язку України “Про затвердження Ліцензійних умов здійснення діяльності у сфері телекомунікацій з надання послуг рухомого (мобільного) телефонного зв'язку з правом технічного обслуговування та експлуатації телекомунікаційних мереж і надання в користування каналів електрозв'язку” від 26.01.2006 р., № 179 // Офіційний вісник України. –2006. –№ 8. –Ст.465.

26. Ліцензійні умови користування радіочастотним ресурсом України /Затв. Рішенням Національної комісії з питань регулювання зв'язку України “Про затвердження Ліцензійних умов користування радіочастотним ресурсом України” від 19.08.2005 р., № 53 // Офіційний вісник України. –2005. –№ 43. –Ст.2723.

27. Закон України “Про міліцію” від

20.12.1990 р., № 565-XII [Електронний ресурс]. –Режим доступу: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=565-12&p=1190113883284477>.

28. Інструкція про порядок формування та використання в органах внутрішніх справ автоматизованого банку даних оперативно-розшукового і профілактичного призначення /Затв. наказом МВС України “Про інформаційні системи органів внутрішніх справ України” від 17.11.2003 р., № 1395.

29. Роз'яснення положень наказу МВС України від 17.11.2003 р., № 1395 щодо порядку обліку викрадених мобільних телефонів від 24.06.2004 р., № 16/02-2593.

30. Системна інформатизація законотворчої та правоохоронної діяльності: Монографія /Кер. авт. кол. Швець М.Я.; За ред. В.В. Дурдинця, В.О. Зайчука, В.Я. Тація. –К.: Навч. книга. 2005. –639 с.

31. New Measures To Combat Mobile Phone Robbery. Press Releases. Press Officer. Home Officer. –URL: <http://press.homeoffice.gov.uk/press-releases/mobile-phone-robbery?version=1>.

32. CEIR Back in the Spotlight. GSM Association 2007. –URL: <http://www.gsmworld.com/using/security/index.shtml>.

33. Central Equipment Identity Register (CEIR). The National Mobile Phone Crime Unit. –URL: <http://www.met.police.uk/mobilephone/ceir.htm>.

34. Игошина Д. “Мобильных” воров поймают на СИМ-карте // Национальная информационная служба Страна.Ru. [Электронный ресурс]. –Режим доступа: <http://www.strana.ru/stories/03/12/26/3458/251362.html>. –21.06.2005.

35. Семенов Г.В. Криминалистическая классификация способов совершения мошенничества в системе сотовой связи // ИНФОРМОСТ: Средства связи. –2001. –№ 3. –С.37-45.

36. Сотовых операторов могут обязать отключать краденные мобильные телефоны /Ассоциация операторов сетей GSM [Электронный ресурс]. –Режим доступа: <http://www.gsmrus.ru/news/113/?show=4&year=2005>. –25.04.2005.

37. Україна випереджає Європейський

Союз у створенні “Електронної митниці” /Урядовий портал: Новини центральних органів влади. Прес-служба Держмитслужби України [Електронний ресурс]. -Режим доступу: http://www.kmu.gov.ua/control/publish/article?art_id=50068652. -05.10.2006.

38. Муртазин Э. Перепрошивка телефонов

в России – уголовные дела открыты // Mobile-review.com [Электронный ресурс]. -Режим доступа: <http://www.mobile-review.com/articles/2005/turma.shtml>. -05.07.2005.

39. Re-programming. The National Mobile Phone Crime Unit. –URL: <http://www.met.police.uk/mobilephone/reprogramming.htm>.

Сулацький Д.В. Організаційно-правові засади протидії правопорушенням у сфері використання кінцевого обладнання рухомого (мобільного) зв'язку в Україні // Форум права. -2008. -№ 1. –С.395-407 [Електронний ресурс]. –Режим доступу: <http://www.nbuv.gov.ua/e-journals/FP/2008-1/08cdvzv.pdf>

Проведено системне дослідження правопорушень у сфері використання кінцевого обладнання рухомого (мобільного) зв'язку, визначені організаційно-правові засади застосування можливостей інформаційно-телекомунікаційних технологій для протидії даним правопорушенням, сформульовані пропозиції до чинного законодавства України щодо впровадження інформаційно-правового механізму попередження зазначених правопорушень.

Сулацький Д.В. Организационно-правовые основы противодействия правонарушениям в сфере использования оконечного оборудования подвижной (мобильной) связи в Украине

Проведено системное исследование правонарушений в сфере использования оконечного оборудования подвижной (мобильной) связи, определены организационно-правовые основы применения возможностей информационно-телекоммуникационных технологий для противодействия данным правонарушениям, сформулированы предложения к действующему законодательству Украины с целью обеспечения внедрения информационно-правового механизма предупреждения указанных правонарушений.

Sulatskiy D.V. The Organizationally-legal bases of counteraction to offences in sphere of using the terminal equipment for mobile communications in Ukraine

The offences in sphere of using terminal equipment for mobile communications are investigated, organizationally-legal bases of the using the abilities of the informationally-telecommunicational technologies for counteraction to these offences are certain, corresponding recommendations to the current legislation of Ukraine are offered.

Форум