ISSN 1995-6134

УДК 347.731:351.74
О.В. БОЙЧЕНКО, канд. техн. наук, доц., Кримський юридичний інститут Одеського державного університету внутрішніх справ

ПРАВОВЕ РЕГУЛЮВАННЯ МІЖНАРОДНОЇ СПІВПРАЦІ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНАХ ВНУТРІШНІХ СПРАВ

Ключові слова: *інформаційна безпека, захист інформаційних ресурсів, органи внутрішніх справ*

Забезпечення інформаційної безпеки в діяльності ОВС є актуальним в умовах розбудови демократичного суспільства, міжнародних відносин України та її вступу в ВТО та інші міжнародні організації, а також з урахуванням специфіки діяльності ОВС щодо протидії злочинності та охорони конституційних прав громадян.

Необхідно зазначити, що окремі питання забезпечення інформаційної безпеки у напрямку реалізації державної інформаційної політики в діяльності ОВС, захисту персональних даних, захисту авторських прав у сфері новітніх інформаційних технологій, кримінальної відповідальності за незаконне втручання в роботу ЕОМ, організаційно-правових основ політики інформаційної безпеки України, теоретико-правових аспектів забезпечення національної безпеки ОВС України, кримінально-правової охорони інформації в комп'ютерних системах та телекомунікаційних мережах, міжнародно-правового захисту права людини на приватність персоніфікованої інформації, захисту права на комп'ютерну програму, інформаційно-аналітичного забезпечення діяльності податкової міліції, правоохоронної діяльності у сфері забезпечення міжнародного миру і безпеки та сучасного інформаційно-методичного забезпечення управління в органах внутрішніх справ розглядались в роботах І.В. Арістової, О.Г. Фролової, В.М. Брижко, С.А. Дзіса, М.В. Карчевського, Б.А. Кормича, М.Б. Левицької, С.А. Орлова, А.В. Пазюка, М.В. Селіванова, Д.Я. Семр'янова, О.О. Теличкіна та ін.

Однак системний та повний аналіз нормативно-правових аспектів забезпечення інформаційної безпеки в діяльності ОВС України відсутній. Тому метою роботи є правовий аналіз стану захищеності інформаційних ресурсів, що формуються, використовуються, коригуються та зберігаються у складі інформаційних підсистем ОВС, а також питання правового регулювання заходів інформаційної безпеки при міждержавному інформаційному обміні між органами внутрішніх справ держав-учасників СНД. Новизна статті полягає в системному аналізі законодавчо-правових актів регулювання заходів інформаційної безпеки в Україні та під час міждержавної інформаційної взаємодії ОВС держав-учасниць СНД.

Інформація є категорією, яка володіє певними якостями, і оперує специфічними поняттями, зокрема поняттям інформаційної безпеки. У колі питань, що розглядаються, необхідно виділити наступні поняття, що стосуються інформації, яка циркулює у середовищі органів внутрішніх справ та має особливе значення у міждержавній інформаційної взаємодії:

1. Конфіденційність – гарантія того, що конкретна інформація доступна тільки обмеженому колу осіб, а порушення цієї категорії є розкраданням або розкриттям інформації. Зазначене поняття є найбільш значимим, оскільки органи внутрішніх справ мають під своїм наглядом величезну кількість строго конфіденційній інформації, розголошення якої може мати дуже серйозні негативні наслідки.

2. Цілісність – гарантія того, що інформація зараз існує в її початковому вигляді, тобто при її зберіганні або передачі не було проведено несанкціонованих змін; порушення цієї категорії є фальсифікацією повідомлення. Фальсифікація інформації в діяльності органів внутрішніх справ тягне кримінальну відповідальність відповідно чинного

ISSN 1995-6134

законодавства.

3. Автентичність – гарантія того, що джерелом інформації є саме та особа, яка заявлена як її автор; порушення цієї категорії також є фальсифікацією, але відповідальність визначається Законом України “Про інтелектуальну власність».

Питання правового регулювання інформаційного забезпечення набувають форми комплексного міжгалузевого правового інституту, що включає норми конституційного, цивільного, адміністративного, кримінального, кримінально-процесуального права та інших галузей права. Відмітною особливістю таких правовідносин є те, що всі вони реалізуються з використанням нових інформаційних технологій та автоматизованих інформаційних систем.

З урахуванням зазначеного пропонується визначитися з поняттям інформаційної безпеки органів внутрішніх справ, що у тому числі, цілком відповідає принципам міждержавної інформаційної взаємодії.

Інформаційна безпека органів внутрішніх справ є станом захищеності інформаційного середовища, відповідного інтересам органів внутрішніх справ, при якому забезпечуються їх формування, використання і можливості розвитку незалежно від дії внутрішніх і зовнішніх інформаційних погроз. При цьому з урахуванням відомих визначень загрози, під інформаційною загрозою розуміють сукупність умов і чинників, що створюють небезпеку інформаційному середовищу та інтересам органів внутрішніх справ.

Таким чином, актуальність правового регулювання інформаційної безпеки в діяльності органів внутрішніх справ не викликає сумнівів. Для досягнення належного рівня нормативно-правового забезпечення інформаційної безпеки потрібне визначення її наочних областей, регулювання відносин суб’єктів забезпечення з урахуванням особливостей основних об’єктів інформаційної безпеки. Тому необхідне комплексне дослідження не тільки правового регулювання інформаційної безпеки на рівні міністерств і відомств, але і дослідження стану і розвитку нормативної бази у сфері інформаційної безпеки як нашої держави, так і міждержавного обміну інформацією.

Разом із тим, оскільки інформаційна безпека ОВС насамперед визначається рівнем стану захищеності внутрішнього інформаційного середовища, то в зв’язку з цим потрібно зазначити ще одне поняття в цій сфері, таке як “державна таємниця». Державна таємниця – це відомості в області його військової, зовнішньополітичної, економічної, розвідувальної, контррозвідувальної і оперативно-розшукової діяльності, що захищаються державою, розповсюдження яких може завдати збитку безпеки держави [1]. Питання захисту інформації, яку відносять до державної таємниці, є найбільш актуальним з точки зору інформаційного обміну інформаційними ресурсами як на державному та на міжнародному рівнях.

Треба зазначити, що суттєвим та значущим елементом у напрямку реалізації міжнародного інформаційно-аналітичного співробітництва діяльності правоохоронних органів, зокрема органів та підрозділів ОВС країн-учасників СНД, є реалізація попереду усього технічної політики, яка дозволяє створити необхідні технічно-програмні та телекомунікаційні ресурси, завдяки яким можна організувати дієвий та оперативний інформаційний обмін щодо забезпечення ефективної протидії злочинності. Але оскільки це не є предметом нашого дослідження, зосередимо увагу на системному аналізові проблем нормативно-правового забезпечення інформаційної безпеки в діяльності ОВС України та у напрямку міжнародної співпраці правоохоронних органів по забезпеченню конституційних прав і свобод громадян.

Насамперед необхідно провести аналіз внутрішніх законодавчих актів, які регулюють питання інформаційної безпеки держави, оскільки вони є пріоритетами міжнародного співробітництва у сфері інформаційних правовідносин.

Ретельний аналіз законопроектів, що знаходяться на опрацюванні у Верховній Раді України та інших інформаційних джерел сві-

ISSN 1995-6134

дчить, що концептуально й законодавчо в Україні не визначено поняття "інформаційна безпека" як системний комплекс взаємопов`язаних запобіжних заходів захисту інформаційного суверенітету та інформаційного простору України.

Характерною ознакою підходів до розуміння інформаційної безпеки є наповнення цього поняття різним змістом, наслідком чого є різний зміст заходів щодо її забезпечення. В деяких випадках класифікація загроз інформаційній безпеці України носить яскраво виражений політизований характер – це виявляється в політичній ситуації в Україні постійно, починаючи з кінця 2000 р., а сьогодення вказує на різке його загострення у зв'язку з повною відсутністю взаєморозуміння гілок влади щодо політичних та фінансово-економічних перспектив України. Одні й ті ж самі фактори та умови різні політичні сили розглядали як небезпечні, загрозливі, чи навпаки, як стабілізуючі.

Так, у ст.3 проекту Закону України "Про інформаційний суверенітет та інформаційну безпеку України" [2] визначено: "Інформаційна безпека України – це захищеність життєво важливих інтересів суспільства, держави та особи, за якої виключається заподіяння їм шкоди через неповноту, несвоєчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення інформації, забороненої чи обмеженої для поширення законами України".

У проекті "Концепції (Основах державної політики) інформаційної безпеки України" інформаційну безпеку розглядають як "стан захищеності національних інтересів України в інформаційній сфері, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі…". Тут було запропоновано тотожні напрями, за якими може бути заподіяно шкоду, як і в проекті вище наведеного Закону.

Надані поняття "інформаційна безпека України" не враховують, на нашу думку, світовий досвід, результати досліджень українських та російських вчених і спеціалістів. Наприклад, у "Доктрині інформаційної безпеки Російської Федерації" зміст поняття "інформаційна безпека" наповнюється широким розумінням. Про це свідчать визначення інтересів особистості, суспільства й держави (ст.1), загрози інформаційній безпеці (ст.2), особливості її забезпечення в різних сферах суспільного життя (ст.6), в тому числі в економіці, внутрішній та зовнішній політиці, в галузях науки й техніки, духовному житті, державних інформаційних та телекомунікаційних системах, обороні, правоохоронній та судовій системах, а також в умовах надзвичайних ситуацій. Російська "Доктрина" розглядає інформаційну безпеку економіки як ключову сферу забезпечення національної безпеки (ст.6) [3].

Як відомо, інформаційна безпека, захист якої згідно ст.17 Конституції України, поряд із суверенітетом, територіальною цілісністю та економічною безпекою, є найважливішою функцією держави, досягається шляхом розробки та впровадження сучасних безпечних інформаційних технологій, побудовою функціонально повної національної інфраструктури, формуванням і розвитком інформаційних відносин тощо.

Редакції поняття "інформаційна безпека", запропоновані в ст.3 проекту Закону "Про інформаційний суверенітет та інформаційну безпеку України" та проекті "Концепції (Основах державної політики) інформаційної безпеки України", мають значні розбіжності з вимогами розділу IV "Концепції (Основ державної політики) національної безпеки України"[1], де визначалися основні напрями державної політики в інформаційній сфері та важливі здобутки вітчизняної науки. Рівень розвитку і безпека інформаційного простору, котрі є системоутворюючими факторами у всіх сферах національної безпеки, активно впливають на стан політичної, економічної, оборонної та інших складових національної безпеки кожної держави. У той самий час, забезпечення інформаційної безпеки представляє собою важливу самостійну сферу.

[1] Наведено як довідкову, сьогодні не чинна.

ISSN 1995-6134

Інформаційна безпека й безпека в інформаційній сфері не тотожні за змістом. Інформаційна сфера на змістовному рівні визначається інформацією та сферою її обігу. Тому безпека інформаційної сфери визначається станом захищеності інформації та сфер її створення, накопичення, зберігання, оброблення, розповсюдження й використання [4].

Для всебічного обґрунтування системоутворюючих у галузі понять "інформаційна безпека" та "безпека інформаційної сфери", доцільно визначитися з інформаційними загрозами, для усунення яких або послаблення їх дії державою власне й створюється система інформаційної безпеки.

Аналізуючи Проект Закону "Про інформаційну безпеку України» [5] (вперше було внесено на розгляд Верховної Ради України 07.07.1998 р., подано на повторний розгляд 5 сесії IV скликання 01.07.2004 р., але й на наступному повторному розгляді 6 сесією IV скликання 14.01.2005 р. Закон не прийнято), слід зазначити суттєві недоліки законодавчого регулювання процесів забезпечення інформаційної безпеки у всіх сферах життєдіяльності суспільства, що в кінцевому результаті визначає його недосконаліть.

Безумовно критиці підлягає стаття 2 Проекту Закону, основним положенням якої є визначення інформаційної безпеки України як комплексу системних превентивних заходів із надання гарантій захисту життєво важливих інтересів особистості, суспільства й держави від негативних інформаційних впливів в економіці, внутрішній і зовнішній політиці, в науково-технологічній, соціокультурній і оборонній сферах, системі державного управління, самостійного й незалежного розвитку всіх елементів національного інформаційного простору та забезпечення інформаційного суверенітету країни, захисту від маніпулювання інформацією і дезінформування та впливів на свідомість, підсвідомість і психіку як індивіда, так і суспільства в цілому, спроможність держави нейтралізувати чи послабити дію внутрішніх і зовнішніх інформаційних загроз.

На нашу думку, інформаційна безпека є станом захищеності інформації (при цьому інформацією є сама інформація як така, інформаційні ресурси, а також й інформаційні технології), при якому її застосування для розвитку суспільства (та його складових) є результативним, дієвим і раціональним, а також при якому гарантованим є захищеність від загроз несанкціонованого доступу до її суті.

Стаття 5 Проекту Закону "Об'єкти інформаційної безпеки» є невичерпною відповідно складових структури об'єктів інформаційної безпеки сучасного суспільства. Так, у статті зазначається відповідний перелік об'єктів інформаційної безпеки у сфері економіки, в галузі оборони, у духовній та політичній сфері. Але в статті не зазначається хоч би в загальному вигляді питання, які стосуються забезпечення інформаційної безпеки в діяльності правоохоронних органів і тих суб'єктів, що відносяться до цієї діяльності.

Протиріччя Проекту Закону знаходяться в багатьох наступних статтях. Так, положення статті 8 "Забезпечення інформаційної безпеки України» вказують на захист права власності всіх учасників інформаційної діяльності в національному інформаційному просторі України, збереження права власності держави на стратегічні об'єкти інформаційної інфраструктури України, охорони державної таємниці, а також інформації з обмеженим доступом, що є об'єктом права власності або об'єктом лише володіння, користування чи розпорядження державою, створення загальної системи охорони інформації, зокрема, охорони державної таємниці, а також іншої інформації з обмеженим доступом, активізацію упереджувальної діяльності інститутів державної влади (зрозуміло, що це насамперед стосується правоохоронних органів, в тому числі й ОВС) щодо запобігання інформаційно-пропагандистському втручанню у внутрішні справи країни.

Але напрямки такої діяльності, тобто конкретизацію всього комплексу заходів інформаційної безпеки, Проект Закону на жаль не визначає. Не визначається також роль основного важелю правоохоронної діяльності –

ISSN 1995-6134

ОВС України – в забезпеченні заходів безпеки інформаційного простору України.

Невичерпною є й стаття 9 Проекту Закону, якою приведений перелік Законів, що складають правову основу забезпечення інформаційної безпеки в Україні. Обов'язково, на нашу думку, до основних нормативних документів потрібно включити Закони України "Про захист інформації в автоматизованих системах» [6], "Про захист інформації в інформаційних телекомунікаційних системах», "Про електронні документи та електронний документообіг», "Про електронний цифровий підпис», "Про захист персональних даних», з приводу того, що зазначені закони вміщують у собі положення, які мають безпосереднє відношення до інформаційної безпеки держави. Зазначене підтверджується ще й тим, що положення статті 2 "Основні поняття і терміни, використані в цьому Законі» визначається поняття злочину у цифрових телекомунікаційних мережах, а сам нормативний документ, який регламентує порядок застосування цифрових телекомунікаційних мереж, не зазначений у переліку основних нормативних документів Проекту Закону.

Не можна не відмітити те, що на сучасному етапі інформаційна політика України здійснюється в умовах, коли концепція інформаційної безпеки, на жаль, ще перебуває в стадії формування. Тобто, процес усвідомлення і проголошення доктрини національних інтересів нашої держави невиправдано довго затягнувся у часі (чергове засідання робочої групи в Апараті РНБО України з підготовки проекту Доктрини інформаційної безпеки України відбулося 04.08.2008 року), а сам документ також до наступного часу не прийнято.

Щодо аналізу нормативних документів у напрямку міжнародного співробітництва забезпечення інформаційної безпеки інформаційно-аналітичної підтримки діяльності правоохоронних органів держав-учасниць СНД, слід зазначити, що, рішенням Ради урядів Співдружності Незалежних Держав 04.06.1999 року була прийнята Концепція міждержавної підсистеми інформаційного обміну між органами внутрішніх справ держав-учасників СНД. Концепція визначає основні принципи, завдання, структуру і етапи створення міждержавної підсистеми інформаційного обміну між органами внутрішніх справ держав-учасників СНД (МПІО-ОВС), як підсистеми Автоматизованої системи інформаційного обміну між державами-учасниками Співдружності [7].

Зазначена Концепція розроблена на основі Концепції формування інформаційного простору Співдружності Незалежних Держав, затвердженою Рішенням Ради урядів СНД від 18.10.1996 року та Міждержавної програми сумісних заходів боротьби з організованою злочинністю і іншими видами небезпечних злочинів на території держав-учасників СНД на період до 2000 року, затвердженою Рішенням Ради урядів держав СНД від 17.05.1996 року.

Відповідно Концепції, основними завданнями МПІО-ОВС є:

- інформаційне забезпечення Ради міністрів внутрішніх справ держав-учасників СНД, зокрема Бюро по координації боротьби з організованою злочинністю і іншими небезпечними видами злочинів на територіях держав-учасників СНД;
- забезпечення інформаційної взаємодії органів внутрішніх справ держав-учасників СНД з урахуванням загальних інтересів в справі розвитку співпраці в боротьбі із злочинністю;
- формування єдиного інформаційного простору органів внутрішніх справ держав учасників СНД і забезпечення їх оперативного доступу до наявних інформаційних ресурсів.

МПІО-ОВС базується на наступних основних принципах:

- дотримання суверенних прав держав-учасників СНД на незалежне формування національного інформаційного простору;
- дотримання основних принципів Загальної декларації прав людини, інших міжнародних документів і прийнятих в рамках СНД угод і договорів у сфері міждержавного обміну інформацією;
- взаємовигідності міждержавних інфор-

ISSN 1995-6134

маційних обмінів;

- забезпечення достатнього рівня інформаційної безпеки кожною з держав-учасників СНД на єдиній методичній основі;

- збереження, розвитку і ефективного використання існуючої інформаційної інфраструктури держав-учасників СНД;

- проведення узгодженої науково-технічної політики, що забезпечує взаємодію національних інформаційних систем, з урахуванням інформаційного обміну по лінії Міжнародної організації кримінальної поліції - Інтерполу;

- визнання рівності сторін в праві на отримання і розповсюдження інформації.

Аналіз свідчить, що одним із визначних принципів ефективної інформаційної взаємодії органів внутрішніх справ країн-учасниць СНД є забезпечення достатнього рівня безпеки на єдиній методичній основі.

Розробка методичного забезпечення інформаційної безпеки при інформаційній взаємодії органів внутрішніх справ країн-учасниць СНД покладається безпосередньо на МВС кожної країни.

Так, МВС України затверджено ряд наказів, що регламентують заходи інформаційної безпеки в діяльності ОВС в частині організації та контролю застосування системи технічного захисту інформації (№ 170 від 25.02.2002 р. “Про затвердження положення про центр ТЗІ при МВС України, типового положення про підрозділ ТЗІ, Положення про координаційну раду МВС України з питань ТЗІ” та № 745 від 25.07.2002 р. “Про затвердження положення про контроль за функціонуванням системи ТЗІ в органах і підрозділах ОВС України” (втратив чинність) [8, 9].

Наказами визначено окремі питання забезпечення безпеки конфіденційної інформації (технічна складова), що є доволі дієвим інструментом протидії загрозам інформації, яка формується, коригується, зберігається та передається в діяльності ОВС. Крім того, окремі питання інформаційної безпеки визначаються наказами МВС, що регламентують режим секретності в діяльності ОВС.

Але для створення більш надійної системи інформаційного захисту інформаційних ресурсів ОВС необхідно прийняття комплексного нормативного акту, який має містити увесь перелік необхідних заходів інформаційної безпеки у складі організаційних, інженерно-технічних, системно-програмних та інших заходів. Зазначене є нагальним відповідно до організації застосування інтегрованих інформаційно-аналітичних систем інформаційної підтримки діяльності ОВС. Впровадження відповідних інформаційно-пошукових систем здійснюється за наказами МВС України, зокрема, № 1395 від 17.11.2003 р. “Про інформаційні системи органів внутрішніх справ України» [10]. Але суттєвої правової регламентації заходів інформаційної безпеки такі документи не містять. Тому необхідним також є видання відповідних відомчих документів з питань застосування заходів інформаційної безпеки при використанні інтегрованих інформаційно-аналітичних системі ОВС.

Особливу актуальність вирішення питання нормативно-правового забезпечення інформаційної безпеки набуває у напрямку міжнародної співпраці ОВС країн-учасниць СНД. Тому прийняття відповідних Законів України, а на їх основі, й наказів МВС України, буде сприяти найскорішому міжнародному інформаційному співробітництву ОВС України з урахуванням всього переліку питань інформаційної безпеки.

ЛІТЕРАТУРА

1. Закон України “Про державну таємницю” : від 21.01.1994 р., № 34/94-ВР // ВВР України. – 1994. - № 16. - Ст. 93.

2. Проект Закону України «Про інформаційний суверенітет та інформаційну безпеку України» (реєстр № 1207-дП : від 12.08.1999 р.) / народний депутат Чиж І. С. [Електронний ресурс]. – Режим доступу: http://www.rada.gov.ua/zakon.

3. Матеріали Інтернет-конференції «Основні положення Доктрини інформаційної безпеки Російської Федерації» // Независи-

ISSN 1995-6134

мое военное обозрение. – 2000. – № 38.

4. Бойченко О. В. Проблемні питання управління захистом інформації в діяльності міліції / О. В. Бойченко // Актуальні проблеми сучасної науки в дослідженнях молодих учених. – 2007. – Вип. 10. – С. 31-34.

5. Проект Закону «Про інформаційну безпеку України» (реєстр. № 5732 : від 22.09.2004 р.) / народний депутат Кирилов В. Д.; doc_54904[1] [Електронний ресурс]. – Режим доступу: http://ilaw.org.ua.

6. Закон України "Про захист інформації в автоматизованих системах" : від 05.07.1994 р., № 80/94-ВР // ВВР України. – 1994. - № 31. - Ст. 287.

7. Концепція міждержавної підсистеми інформаційного обміну між органами внутрішніх справ держав-учасників СНД : від 04.06.1999 р. [Електронний ресурс]. – Режим доступу: http://search.liga.kiev.ua.

8. Наказ МВС України "Про затвердження положення про центр ТЗІ при МВС України, типового положення про підрозділ ТЗІ, Положення про координаційну раду МВС України з питань ТЗІ" : від 25.02. 2002 р., № 170.

9. Наказ МВС України "Про затвердження положення про контроль за функціонуванням системи ТЗІ в органах і підрозділах ОВС України" : від 25.07.2002 р., № 745.

10. Наказ МВС України "Про інформаційні системи органів внутрішніх справ України": від № 17.11.2003 р., № 1395.

Бойченко О. В. Правове регулювання міжнародної співпраці щодо забезпечення інформаційної безпеки в органах внутрішніх справ / О. В. Бойченко // Форум права. – 2008. - № 3. –С. 46-52 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2008-3/08bovovs.pdf

Виконано аналіз стану правового регулювання захищеності інформаційних ресурсів ОВС. Встановлена недосконаліть нормативно-правової бази заходів із інформаційної безпеки в Україні та під час міждержавної інформаційної взаємодії ОВС держав-учасниць СНД. Запропоновано прийняття відповідних законів України та наказів МВС України для забезпечення інформаційної безпеки у міжнародному інформаційному співробітництві.

***

Бойченко О.В. Правовое регулирование международного сотрудничества по обеспечению информационной безопасности в органах внутренних дел

Выполнен анализ состояния правового регулирования защищенности информационных ресурсов ОВД. Установлено несовершенство нормативно-правовой базы мероприятий по информационной безопасности в Украине и при межгосударственном информационном взаимодействии ОВД государств-участников СНГ. Предложено принятие соответствующих законов Украины и приказов МВД Украины для обеспечения информационной безопасности в международном информационном сотрудничестве.

***

Bojchenko O.V. Legal Regulation of the International Cooperation on Maintenance of Information Safety in Law-Enforcement Bodies

The analysis of a condition of legal regulation of security of information resources of law-enforcement bodies is executed. Imperfection of normative-legal base of actions for information safety in Ukraine is established and at interstate information interaction of law-enforcement bodies state-participants of the CIS. Acceptance of the appropriate laws of Ukraine and orders of the Ministry of Internal Affairs of Ukraine for maintenance of information safety in the international information cooperation is offered.