УДК: 341.23:351.746:007

Зарубіжний досвід взаємодії правоохоронних органів із суб'єктами господарювання у процесі захисту інформації з обмеженим доступом

Жевелєва Ірина Сергіївна –
старший викладач кафедри Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України

У статті розглядаються питання вивчення і впровадження зарубіжного досвіду (на прикладі США та Російської Федерації) в побудову системи взаємодії правоохоронних органів України з суб'єктами господарювання у процесі захисту інформації з обмеженим доступом.

Ключові слова: інформаційне суспільство, інформаційна безпека держави, взаємодія правоохоронних органів, суб'єкти господарювання, захист інформації з обмеженим доступом, зарубіжний досвід.

Постановка проблеми в загальному вигляді. В умовах інформаційного суспільства проблема забезпечення інформаційної безпеки держави набуває критичного змісту, відтак потребує вдосконалення не лише правовими засобами, а й пошуком, розробкою нових форм, механізмів і заходів, що підвищували б ефективність функціонування системи її забезпечення.

Актуальною проблемою національного рівня є корегування моделі забезпечення національної безпеки, а також розбудова недержавної системи безпеки підприємництва, організації належного функціонування і взаємодії державних і недержавних суб'єктів сектору безпеки України.

Аналіз останніх досліджень і публікацій. Окремі теоретичні та практичні аспекти досліджуваного питання знайшли відображення у працях наступних вітчизняних і зарубіжних учених: В. Андрійчука, К. Іполітова, В. Соколова та ін.

Виділення не вирішених раніше частин загальної проблеми. Наявні правові та організаційні засоби функціонування недержавних служб безпеки, відсутність чіткої взаємодії їх з правоохоронними органами – не дозволяють у повній мірі реалізувати їх значний потенціал для сприяння державним суб'єктам і забезпечення національної та інформаційної безпеки України, тому вкрай актуальною для України постає проблема вивчення міжнародного досвіду в зазначеній сфері і, на його основі, створення системи недержавної безпеки підприємницької діяльності в Україні як закономірного фактору в зміцненні демократичних принципів в управлінні державою.

Метою статті є узагальнення досвіду зарубіжних країн щодо практичної реалізації сучасної системно-структурної парадигми взаємодії державного та недержавного секторів безпеки у сфері захисту інформації з обмеженим доступом.

Виклад основного матеріалу. Дослідження зарубіжного досвіду свідчить, що в іноземних державах щоразу нові вимоги з боку суспільства до забезпечення правопорядку впливають на організацію правоохоронної діяльності. У багатьох країнах дедалі більше орієнтуються не лише на поліцейські органи, а й на широке використання для правоохоронних цілей приватних детективних і охоронних служб.

Світовий досвід переконує, що не всі види правоохоронних функцій у належному обсязі можуть виконувати державні органи. Внаслідок цього за кордоном значного поширення набули адвокатські контори, приватні розшукові, детективні бюро тощо.

За оцінками фахівців американського Центру стратегічних і міжнародних досліджень Стептоу і Джонсона [1], приблизно 75 % комп'ютеризованих систем управління промисловими об'єктами США пов'язані з Інтернетом або мережами аналогічної архітектури.

Розглядаючи питання забезпечення інформаційної безпеки різних сторін соціальної та гуманітарної сфер життєдіяльності як необхідну умову прогресивного розвитку суспільства, запоруку внутрішньополітичної стабільності в державі, на сучасному етапі важливою є взаємодія державних і недержавних суб'єктів безпеки, яка може мати різноманітний вигляд.

© І. С. Жевелєва, 2014

Взаємодія органів державної влади США і приватного сектору з питань забезпечення інформаційної безпеки

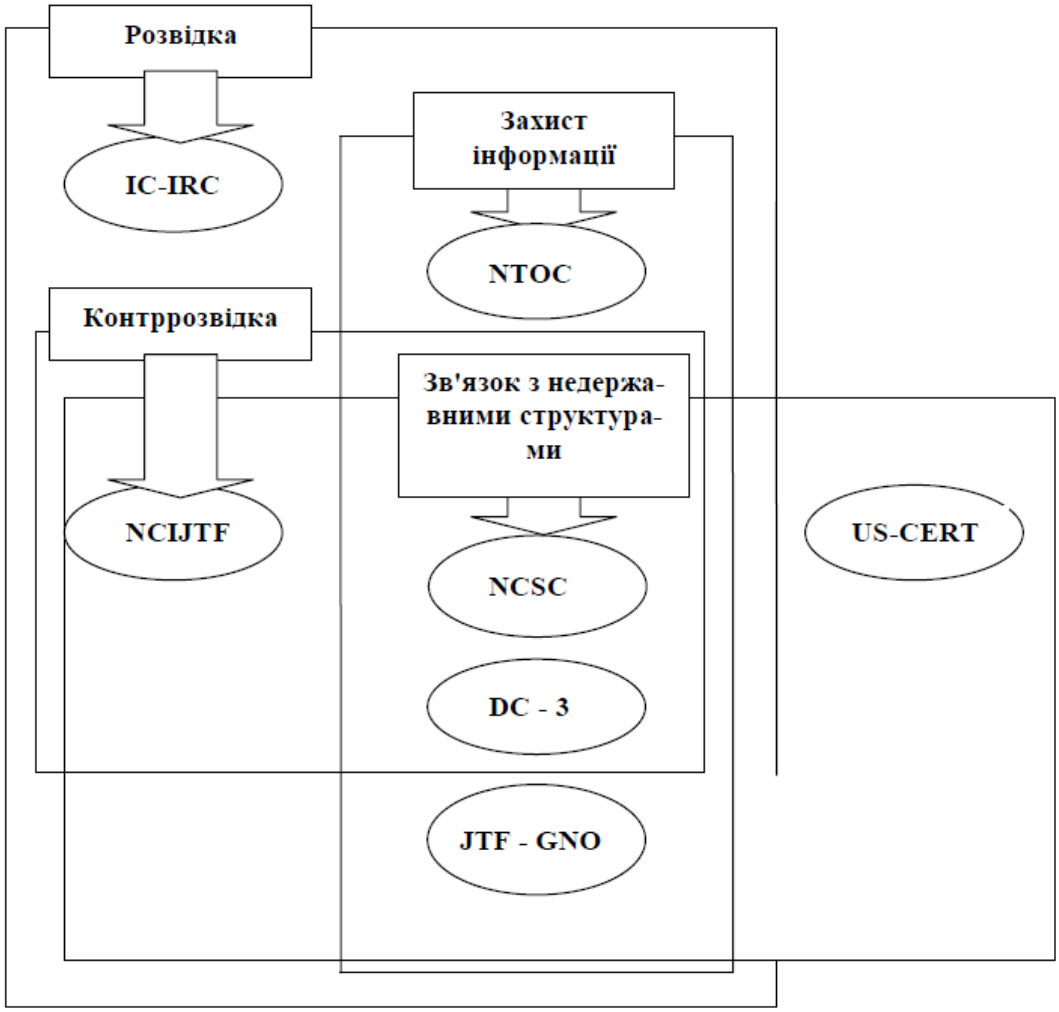

Рис. 1. Структурно-функціональна схема взаємодії державних суб'єктів безпеки США з питань боротьби з кіберзлочинністю

Провідні державні суб'єкти безпеки США у межах (рис. 1) схеми взаємин виконують такі основні функції [2]:

IC–IRC – підрозділ об'єднаного розвідувального співтовариства (федерації) державних і недержавних структур (**DNI**) на чолі з Директором національної розвідки, до функцій якого відповідно до предмета дослідження належать: моніторинг інформаційного простору, збір, узагальнення та аналіз проявів кіберзлочинності; визначення потенційних загроз і поширення досвіду реагування, упередження і протистояння наявним викликам мережевими засобами; розширення зовнішніх зв'язків із цих питань; проведення спеціальних операцій, сприяння військовому плануванню;

US–CERT – підпорядкований Міністерству захисту держави (**DHS**) підрозділ, основні функції якого пов'язані з: запобіганням поширенню та ліквідацією наслідків кібератак на федеральні державні і місцеві системи управління, а також на мережі передачі даних; політичним та економічним співробітництвом з партнерами з цих питань;

JTF–GNO (USCYBERCOM) – підпорядкована структура Стратегічного командування Збройних Сил США, реорганізована у вересні 2010 р. в кіберкомандування США (**USCYBERCOM**), функції якого полягають у: забезпеченні функціонування та захисті глобальної мережі передачі інформації в інтересах підтримки стратегічних, оперативних і тактичних операцій Міністерства оборони (**DoD**); централізації управління операціями в інформаційному просторі; концентрації наявних ресурсів; синхронізації заходів захисту військових інформаційно-комунікаційних мереж;

NTOC – координаційний центр Агентства національної безпеки (**NSA**) – провідної структури у складі **DNI**, функції якого стосуються: виявлення, аналітичного опрацювання та класифікації кіберзагроз; ситуаційного аналізу процесів, що відбуваються в інформаційному просторі; розробки стратегій пом'якшення наслідків кіберзлочинів;

заходів запобігання та протидії кібератакам, поширення обізнаності щодо застосування таких заходів у середовищі союзників і партнерів;

NCSC – підрозділ Міністерства захисту держави (**DHS**), функції якого полягають у: захисті від несанкціонованого внутрішнього та зовнішнього доступу урядових систем зв'язку; контролі, зборі, узагальненні та поширенні інформації з цих питань; співробітництві з іншими підрозділами Міністерства, ФБР, Міністерством оборони, АНБ тощо;

NCIJTF – діючий під керівництвом Федерального бюро розслідувань (**FBI**) міжвідомчий цільовий координаційний центр Міністерства юстиції (**DOJ**), функціями якого є: об'єднання зусиль усіх державних структур, спецслужб і правоохоронних органів; узагальнення та поширення інформації про всі внутрішні прояви кіберзагроз, кібератак і кіберзлочинності, включаючи прояви терористичної діяльності; програмування та реалізація заходів переслідування і притягнення до відповідальності злочинців, шпигунів, терористів тощо;

DC3 – спеціалізований центр Міністерства оборони (DoD), виконуючий функції: розробки стандартів цифрової обробки та захисту інформації від несанкціонованого доступу, контролю за їх дотриманням; діагностики та відновлення працездатності носіїв інформації; застосування комп'ютеризованих технологій у криміналістиці, розслідуванні злочинів, зокрема антитерористичної діяльності, фаховій підготовці кадрів із цих питань для інших структур [3, с. 55].

На рис 2. наведено орієнтовну структурну схему взаємодії державного і недержавного секторів безпеки США.

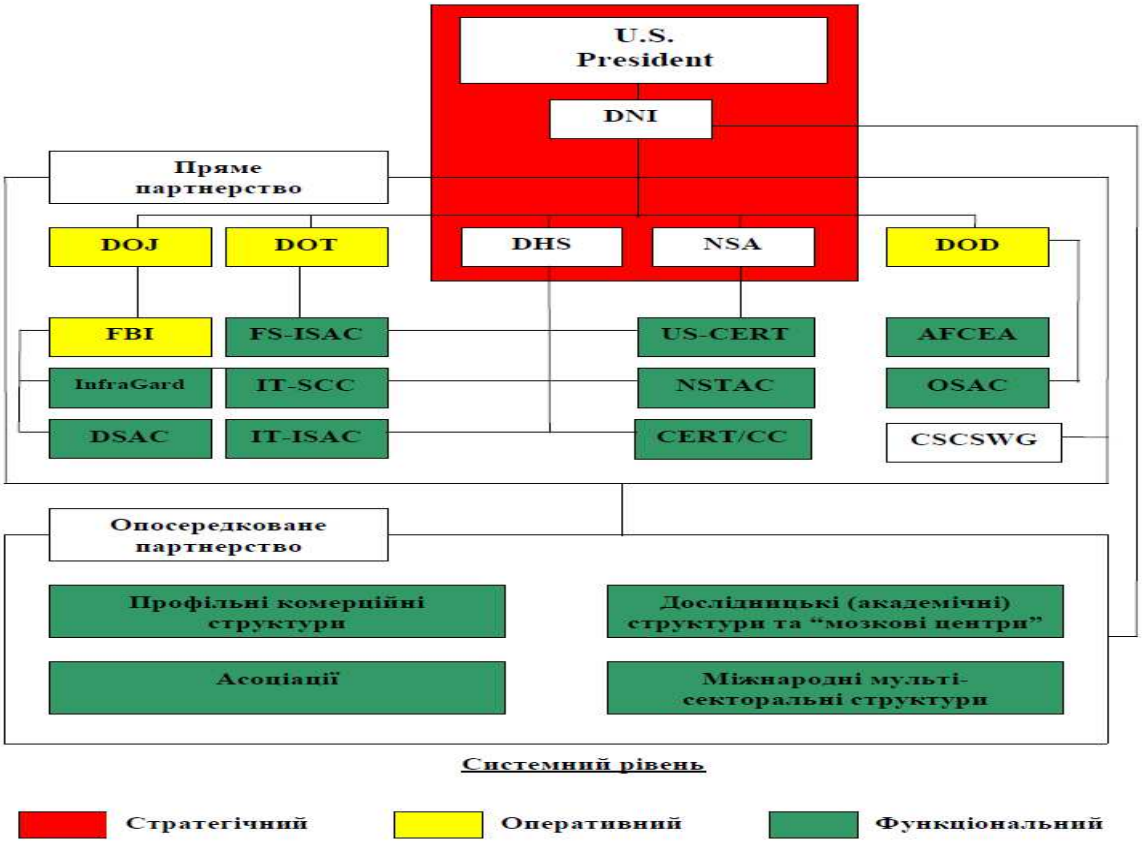

Рис. 2. Орієнтовна структурна схема взаємодії державного і недержавного секторів безпеки США

Опосередковане співробітництво державного сектору безпеки США з профільними недержавними структурами будується за предметно орієнтованим принципом. Наприклад, можна навести такі пріоритети опосередкованого співробітництва:

– з профільними структурами (Google Enterprise, McAfee, Symantec, Microsoft, AT&T тощо) – інноваційні технології отримання, упорядкування, пошуку інформації, зв'язку, обміну даними, автоматизації роботи з інформаційними ресурсами; розробка систем захисту комп'ютерних комплексів від існуючих кібератак, а також від нових поколінь загроз; управління потоками інформації, програмне забезпечення і сервісне обслуговування систем захисту від зовнішнього несанкціонованого втручання та ризиків кібератак; розширення соціальних та економічних можливостей суспільства у світі; системні рішення мережевої безпеки, управління ризиками, фільтрація та обробка веб-контенту;

– з дослідницькими структурами (REND Corporation, Berkman Center, CSIS, Sans Institute тощо) – дослідження тенденцій та динаміки розвитку кіберпростору з метою оцінки наявності загроз, необхідності запровадження санкцій, розробки відповідних норм і стандартів; ситуаційний аналіз, підготовка пропозицій для прийняття урядом рішень стратегічного рівня у міжнародних відносинах, у діалозі із суспільством, у частині взаємодії з приватним сектором економіки; сертифікація

інформаційних систем, методи раннього попередження Інтернет-атак;

– з асоціаціями (ITAA, ICASI, INSA тощо) – інформаційні технології, індустрія електронних засобів збирання, оброблення, передачі даних; практичний досвід захисту інформаційних систем; інноваційні розробки щодо їхньої практичної реалізації;

– з міжнародними мультисекторальними структурами (IETF, ICANN тощо) – еволюція Інтернет, технічні та конструкторські рішення систем управління його функціонуванням; аналіз інтересів Інтернет-спільноти [4–6].

З огляду на викладене, можна дійти висновку, що обрана у США методологія регулювання розвитку інформаційного простору, а також функціонування інформаційно-комунікаційної сфери, відповідає такій системно-пріоритетній парадигмі:

– забезпечення інформаційної безпеки суспільства та особи як важливішого сучасного пріоритету гарантування національної безпеки на всіх можливих напрямах внутрішніх і зовнішніх державних інтересів – політичних, економічних, культурних тощо;

– широкого залучення можливостей недержавних національних і транснаціональних інформаційно-комунікаційних структур як дієвого механізму досягнення власних цілей, підвищення авторитету, впливовості та конкурентоспроможності національних цінностей у зовнішньому середовищі.

Розкриваючи зарубіжний досвід, не можна не зупинитись на системі взаємодії правоохоронних органів з суб'єктами господарювання у процесі захисту інформації з обмеженим доступом, яка налагоджена в **Російській Федерації.**

Оскільки з Федеральних органів виконавчої влади найбільшою компетенцією у забезпеченні економічної та інформаційної безпеки Росії володіють Федеральна служба безпеки і МВС, доцільно зупинитися на проблемах взаємовідносин органів ФСБ і МВС з недержавними організаціями, у тому числі й з їх структурами безпеки, та можливих шляхах їх вирішення. Статтею 15 Закону Російської Федерації "Про Федеральну службу безпеки" [7] передбачається, що "органи федеральної служби безпеки здійснюють свою діяльність у взаємодії з федеральними органами державної влади, підприємствами, установами та організаціями незалежно від форм власності". У зазначеному Законі розкриваються окремі напрямки і форми такої взаємодії. Так, у тій же статті 15 говориться, що "з метою вирішення завдання забезпечення безпеки РФ військовослужбовці органів ФСБ можуть бути прикомандировані до державних органів, підприємств, установ і організацій незалежно від форм власності за згодою їх керівників у порядку, встановленому Президентом РФ".

У статті 12 зазначено на обов'язок органів ФСБ "брати участь у розробці та реалізації заходів щодо захисту відомостей, що становлять державну таємницю, здійснювати контроль за забезпеченням збереження відомостей, які становлять державну таємницю, в державних органах, на підприємствах, в установах і організаціях незалежно від форм власності". Серед прав (ст. 13), якими законодавець наділив ФСБ, є право на отримання безоплатно інформації від державних і недержавних органів, підприємств і організацій, необхідної для виконання покладених на ФСБ завдань, а також право на надання сприяння у розробці заходів щодо захисту комерційної таємниці та на здійснення підготовки кадрів для служб безпеки недержавних структур.

Правоохоронні органи Російської Федерації у порядку, визначеному законодавством, сприяють суб'єктам господарювання у проведенні таких заходів [8]:

– фізична охорона об'єктів і приватних осіб з використанням сучасних технічних засобів, вогнепальної зброї та спецзасобів;

– забезпечення безпеки об'єктів і приватних осіб за допомогою програмно-технічних комплексів захисту інформаційних систем;

– забезпечення інформаційної безпеки недержавних суб'єктів економічних відносин;

– інформаційно-аналітичне забезпечення підприємницького ризику і захист комерційної таємниці;

– превентивне консультування керівників новостворених підприємств та економічних структур з питань комплексної безпеки у формі консультацій, розробки практичних рекомендацій і т.д.;

– надання підприємницьким структурам гарантій у здійсненні комерційних угод і кредитоспроможності партнерів;

– забезпечення силами недержавного сектора охоронних послуг безпеки комерційних об'єктів міської інфраструктури;

– залучення недержавного сектору охоронних підприємств для забезпечення безпеки підприємств, для забезпечення безпеки проведених у містах, республіках міжнародних комерційних виставок, конгресів, симпозіумів, творчих фестивалів і т.д.;

– спільне з підрозділами патрульно-постової служби органів внутрішніх справ патрулювання в районах міста та громадських місцях у робочому режимі і під час проведення соціально значущих заходів і подій культурно-просвітнього характеру;

– забезпечення силами недержавного охоронного сектора порядку в місцях проведення масових культурно-спортивних і видовищних заходів;

– інша, передбачена законами діяльність.

В якості ***основних критеріїв*** при визначенні суб'єктів господарювання як об'єктів для сприяння розглядається:

– роль і місце охоронюваного ними об'єкта в економіці, наявність щодо нього реальних зовнішніх і внутрішніх загроз, які можуть завдати шкоди життєво важливим інтересам держави;

– ступінь участі приватного охоронного підприємства в державній політиці боротьби зі злочинністю;

– незалученість об'єкта в сферу кримінального бізнесу.

Чим вищий рівень системи, в якій збігаються інтереси держави і недержавного підприємства або організації, тим більш сприятливі умови повинні створюватися для їх взаємодії. На всіх зазначених рівнях державна політика забезпечення безпе-

ки конкретизується у вигляді концепцій, програм, планів діяльності суб'єктів системи безпеки, спрямованих на вирішення певних проблем (наприклад, щодо боротьби з дестабілізацією грошово-фінансової системи, з корупцією та організованою злочинністю, забезпечення безпеки інвестиційної політики і т. ін.).

Висновки. З огляду на викладене, можна дійти висновку, що обрані у США та Російській Федерації системи взаємодії правоохоронних органів з суб'єктами господарювання у процесі захисту інформації є налагодженими та результативними. На основі їх аналізу можна зробити наступні висновки для України.

1. Напрямком взаємодії правоохоронних органів України з суб'єктами господарювання має стати захист не тільки державної, але й комерційної таємниці. Сьогодні складається ситуація, коли державна таємниця, поряд з комерційною, може існувати і в приватному секторі. Це пов'язано, насамперед, з акціонуванням підприємств, можливим розміщенням держзамовлень на оборонну продукцію на приватизованих підприємствах, і т.д.

2. Основні форми взаємодії у сфері захисту інформації з обмеженим доступом, розголошення якої може завдати шкоди життєвоважливим інтересам держави:

– надання з боку органів СБ України консультативної допомоги суб'єктам господарювання, на яких передбачається розмістити державне замовлення на стратегічну продукцію, в створенні на них необхідних умов для отримання ліцензії на право проведення секретних робіт;

– спільна участь у профілактичних заходах та ін.

Такий рівень взаємодії передбачає, перш за все, взаємний обмін інформацією з досить широкого кола питань, пов'язаних із захистом інформації.

3. Що стосується організації роботи щодо захисту комерційної таємниці, то треба мати на увазі два аспекти цієї проблеми:

а) коли в якості замовника продукції, що має властивості комерційної таємниці, виступає держава;

б) коли комерційна таємниця є власністю тільки підприємця.

У першому випадку механізм взаємодії державних і недержавних служб безпеки повинен бути аналогічний механізму взаємодії із захисту державної таємниці, у другому – органи СБ України можуть лише сприяти підприємцю в забезпеченні комерційної таємниці; а ініціативи мають виходити від керівництва підприємства, зацікавленого у збереженні своїх комерційних секретів.

Сприяння може мати такі форми:

надання методологічної та практичної допомоги в організації роботи щодо захисту комерційної таємниці;

інформування керівництва підприємств про факти, що потрапили в поле зору органів СБ України, які свідчать про витік комерційних секретів;

підготовка фахівців для недержавних служб безпеки і т.д.

У сфері захисту комерційної таємниці відкривається широке поле для взаємодії з урахуванням також і того, що при виході на закордонного партнера наші підприємці стикаються як з різного виду промисловим шпигунством, так і з здійснюваної під прикриттям зарубіжних фірм розвідувальною діяльністю спецслужб іноземних держав. Найбільш серйозним стримуючим фактором взаємодії у цій діяльності є відсутність Закону "Про комерційну таємницю".

Дослідження дієвих механізмів зарубіжного досвіду та впровадження його в практику взаємодії правоохоронних органів України із суб'єктами господарювання в процесі захисту інформації з обмеженим доступом, вироблення на цій основі пропозицій та рекомендацій для удосконалення існуючої правової бази, будуть відображені в подальших роботах автора.

Список використаних джерел

1. Соколов В. Консорциум за мир в киберпространстве [Электронный ресурс] / В. Соколов. – Режим доступа : http://www.rian.ru/analytics/20100504/230220288.html.

2. US Intelligence and Security Agencies / [Electronic resource]. – Mode of access : http://www.fas.org/irp/official.html.

3. Андрейчук В. С. Взаємодія державного та недержавного секторів США у сфері інформаційної безпеки: досвід для України / Віталій Степанович Андрійчук // Інформаційна безпека: людини, суспільства, держави. – 2012. – № 2 (9). – Ст. 53–63.

4. United States Intelligence Community / [Electronic resourse]. – Mode of access : http://en.wikipedia.org/wiki/United_States_Intelligence_Community.

5. Супян В. Б. "Мозговые центры" США: их роль и эволюция как независимых исследовательских организаций / В. Б. Супян // США и Канада: экономика – политика – культура. – 2010. – № 1. – С. 4–16.

6. Диксон П. Фабрики мысли / П. Диксон. – М. : Прогресс, 1976. – 430 с.

7. О Федеральной службе безопасности [Электронный ресурс] : Федеральный закон от 22 февраля 1995 года. – Режим доступа : http://www.fsb.ru/fsb/npd/more.htm!id=10340801@fsbNpa.html.

8. Ипполитов К. Х. О роли и месте НСБ в обеспечении безопасности предпринимательства и личности киберпространстве [Электронный ресурс] / К. Х. Ипполитов. – Режим доступа : http://mail.guardinfo.ru/.

В статье рассматриваются вопросы изучения и внедрения иностранного опыта (на примере США и Российской Федерации) в построение системы взаимодействия правоохранительных органов Украины с субъектами хозяйствования в процессе защиты информации с ограниченным доступом.

The article deals with the study and implementation of foreign experience (for example, the United States and the Russian Federation) to build a system of interaction between the law enforcement agencies and the business entities in the protection of information with limited access.

Стаття надійшла до редакції журналу 4 червня 2014 року.