construction, alteration, repair of vehicles causes (causes) offensive to at least one of the socially dangerous consequences, under the provisions of this article.

Violation of existing transport rules may be committed not only one, but by several people, each of whom their action creates a set of conditions for the onset of serious consequences. The criminal legislation of Ukraine does not give the notion of accidental sharing of, and responsibility for the Commission of such a crime occurs on the same basis as for careless crimes.

In establishing causation in criminal responsibility for the crimes, which occurred in the case of violation of existing transport rules, you must fully consider and assess all the evidence in a criminal proceeding, install the required actions (or inaction), which should make the accident, completeness of implementation. Only after that you can install the direct cause, without which it would not have socially dangerous consequences and, if there are other signs of corpus delicti, to decide on the prosecution of the person.

The causal relationship of the crime stipulated in art. 291 of the Criminal Code, is characterized by the fact that a socially dangerous act committed that crime is immediate and sufficient cause of common socially dangerous consequences. With this necessary causal link can be both direct and indirect. It should be noted that, in some cases, to seek the development of causal link between the breach of the existing transport regulations and socially dangerous consequences, you must assign the trial of engineering and technical expertise.

Keywords: *criminal responsibility, objective side of crime, causal link, existing traffic rule.*

Надійшла до редакції 04.11.2014

Богатирьова О. І.
кандидат юридичних наук
Амелін О. В.
провідний науковий співробітник
(Національна академія прокуратури Україниии)

УДК 343.3/7

АНАЛІЗ ЧИННОГО ЗАКОНОДАВСТВА ПРО ЗЛОЧИНИ У СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРІВ, СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ

Проаналізовано чинне законодавство України у сфері використання комп'ютерів, систем та комп'ютерних мереж, а також з'ясовано окремі проблеми, які існують у даній сфері. Запропоновано відповідні напрями удосконалення правової бази із внесенням змін і доповнень до відповідних нормативно-правових актів.

Ключові слова*: злочини у сфері використання комп'ютерів, систем та комп'ютерних мереж, законодавство, кіберзлочинність, протидія.*

Постановка проблеми. Нині, як ніколи, соціально-економічний розвиток суспільства характеризується зростанням ролі інформаційної сфери, яка складається із сукупності інформаційної інфраструктури, інформаційних те-

хнологій, інформаційних ресурсів, суб'єктів, що здійснюють збір, формування, поширення і використання інформації, а також системи регулювання суспільних відносин, що при цьому виникають. Інформаційна сфера стає системоутворюючим фактором життя суспільства, безпосереднім чинником економічного зростання, сприяє забезпеченню обороноздатності країни, соціально-економічній стабільності та розвитку демократичних засад в управлінні державою. Як наслідок, роль інформаційної безпеки як складової національної безпеки будь-якої держави посилюється, при цьому з часом така залежність лише зростає.

На жаль, протягом усіх років незалежності України галузь інформаційних технологій розвивалася практично без жодного втручання з боку держави. Державне регулювання тут фактично зводилось до збору статистичних показників, які часто не відображали реального становища та основних тенденцій такої важливої у сучасному суспільстві сфери суспільних відносин.

Незважаючи на те, що Україна має висококваліфікований кадровий потенціал в інформаційній сфері, постійно зростаючий та поновлюваний парк комп'ютерної техніки, сучасні системи та засоби телекомунікацій, зв'язку, високий ступінь інформатизації банківської сфери, становлення інформаційного суспільства потребує вирішення численних проблем.

Аналіз публікацій, в яких започатковано розв'язання даної проблеми. Дослідженню вказаної проблематики присвятили свої праці такі науковці, як С. Бородін, О. Григор'єв, А. Гребеньков, В. Голубєв, Г. Долженков, М. Журба, І. Карась, О. Книженко, В. Карчевський, Ю. Ляпунов, П. Смагін, Л. Краснова, І. Клепицький, О. Користін, М. Литвинов, С. Спірина, В. Хахановський, однак питання аналізу законодавства у сфері використання комп'ютерів, систем та комп'ютерних мереж розглядалися ними лише фрагментарно.

Мета. Нині чинне законодавство про злочини у сфері використання комп'ютерів, систем та комп'ютерних мереж підлягає перегляду, оскільки не лише чинні норми Кримінального кодексу України вже не відповідають динаміці розвитку злочинності в цій сфері, а й існують інші прогалини у чинному законодавстві, вирішення яких дозволить змінити стан криміногенної обстановки у цій сфері на краще.

Виклад основного матеріалу. Провідні країни світу, переглянувши пріоритети інформаційної державної політики, нині розробляють і впроваджують державні стратегії та програми розвитку інформаційного суспільства, які є основою запобігання злочинності та спрямовані на:

- створення глобального інформаційного простору, здатного забезпечити нову якість життя;
- збільшення питомої ваги інформаційно-комунікаційних технологій (далі – ІКТ), продуктів і послуг у валовому внутрішньому продукті країни;
- появу якісно нових електронних комунікацій та ефективної інформаційної взаємодії людей на засадах зростаючого доступу до національних і світових інформаційних ресурсів;

- подолання інформаційної нерівності та прогресуюче задоволення людських потреб в інформаційних продуктах і послугах.

Аналіз таких стратегій і програм у країнах Європейського Союзу, Балтійського регіону Європи, Японії, США та інших країн світу показує, що їх основною метою є досягнення лідируючих позицій в економічній та соціальній складових державного розвитку через широке використання ІКТ – електронної комерції, електронного уряду, електронного бізнесу тощо – не як ізольованих сфер діяльності, а як інтегрованої і взаємозалежної сукупності цих технологій.

Зокрема, такі програми реалізуються у:

– Сполучених Штатах Америки («План дій адміністрації США в галузі Національної інформаційної інфраструктури»);

– країнах ЄС («Європа 2020: стратегія розумного, стійкого і всеосяжного зростання»; у Федеративній республіці Німеччина – «Шлях Німеччини до інформаційного суспільства», Королівстві Данія – «Державна програма переходу до інформаційного суспільства», Королівстві Швеція – Національна програма становлення інформаційного суспільства «Інформаційне суспільство Швеції»);

– Королівстві Норвегія (Програма «eNorge» і Програма становлення і переходу до інформаційного суспільства «Краще використання інформаційної технології у Норвегії»);

– Республіці Корея (Програма «Корейська інформаційна інфраструктура») [2, с. 5-6].

Україна не є винятком з цього загального процесу. Реалізація державної політики у вказаній сфері знайшла своє відображення у низці законодавчих актів, в тому числі прийнятих в останні роки, серед яких:

– Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», який визначає пріоритетним напрямком державної політики розвиток національної інфраструктури інформаційних технологій, державну підтримку для нових «електронних» секторів економіки, застосування ІКТ у всіх сферах життя (зокрема в уряді та засобах масової інформації) і поліпшення ситуації у сфері безпеки інформаційних технологій;

- закони України «Про доступ до публічної інформації», «Про адміністративні послуги», «Про інформацію», «Про захист персональних даних», «Про державну підтримку розвитку індустрії програмної продукції», «Про державну таємницю», «Про інформаційні агентства», Конвенція про кіберзлочинність від 23 листопада 2001 р., ратифікована Україною 7 вересня 2005 р., тощо [1, с. 119-122];

- зміни до Податкового кодексу України щодо особливостей оподаткування підприємств, які працюють у галузі виробництва програмного забезпечення;

- Стратегія розвитку інформаційного суспільства в Україні;

- Концепція розвитку електронного урядування;

- Міжнародна ініціатива «Партнерство „Відкритий уряд”»;

- Концепція Державної цільової програми створення та функціонування інформаційної системи надання адміністративних послуг на період до 2017 року;

- План заходів зі створення Єдиного державного порталу адміністративних послуг.

Водночас з розвитком інформаційно-комунікаційних технологій зростають загрози та ризики їх використання з метою протиправної діяльності. Сьогодні кіберзлочинність вийшла за межі сфери контролю правоохоронних органів однієї держави та переросла в серйозну міждержавну та транснаціональну проблему. Так, у доповіді Палати громад Сполученого Королівства Великої Британії та Північної Ірландії зазначається, що доходи від злочинної діяльності, пов'язаної з використанням мережі загального користування Інтернет, становлять 388 мільярдів доларів США щорічно і вже перевищили прибутки злочинних угруповань від наркобізнесу (288 мільярдів доларів США). Зокрема, зазначено, що «хакерська атака на об'єкти інфраструктури Великобританії може спричинити тяжчі наслідки, ніж використання зброї масового знищення» [4].

За результатами спільних досліджень компанії ,,McAfee" та Центру стратегічних і міжнародних досліджень (CSIS), збитки від кібератак у 2013 р. у світовому масштабі склали близько 3 трлн. доларів США., де найбільших з них зазнали Німеччина, Китай та США (по 200 млн.) [5, с. 9].

Збитки від кібератак поділяються на шість основних категорій:

1. недоотримана вигода правовласників;
2. безпосередні збитки від кіберзлочинів;
3. збитки, спричинені незаконним заволодінням інформацією, що становить службову, банківську або комерційну таємницю;
4. збитки, спричинені державним і громадським підприємствам, установам і організаціям у результаті перешкоджання здійсненню законної діяльності;
5. витрати на забезпечення кібербезпеки;
6. моральні збитки від кіберзлочинів.

Протидія кіберзлочинам в Україні фактично розпочалась із прийняттям у 2001 р. Кримінального кодексу України, де діянням у сфері інформаційної безпеки було присвячено окремий розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж", який містив усього три статті: ст. 361 «Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж»; ст. 362 «Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем» та ст. 363 «Порушення правил експлуатації автоматизованих електронно-обчислювальних систем».

Законом України від 5 червня 2003 р. № 908-IV були внесені зміни до вказаного Кодексу, відповідно до яких назву розділу XVI змінено на «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів),

систем та комп'ютерних мереж і мереж електрозв'язку»; статтю 361 було викладено у новій редакції, згідно з якою встановлювалася кримінальна відповідальність за втручання в роботу мереж електрозв'язку; змінено санкцію ч. 2 ст. 361; вказану статтю доповнено приміткою про визначення розміру значної шкоди, заподіюваної злочинами, передбаченими цією статтею.

Пізніше Законом України від 23 грудня 2004 р. № 2289-IV було істотно змінено редакцію ст. 361-363 КК. Крім того, Кримінальний закон було доповнено трьома новими статтями 361-1, 361-2 та 363-1.

Отже, чинним КК передбачено кримінальну відповідальність за:

1) несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361);

2) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1);

3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2);

4) несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362);

5) порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363).

6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1).

Враховуючи викладене, виникає запитання: чи є підстави вважати, що чинне вітчизняне законодавство вже містить достатню кількість дієвих правових норм, спрямованих на правову охорону інформаційної безпеки України?

Можливо, проблеми, які виникають у вказаній сфері, є не стільки результатом відсутності необхідної законодавчої бази, скільки результатом недостатньо ефективної діяльності відповідних державних органів, уповноважених забезпечувати захист інформації у процесі використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку?

Звернімося до офіційних даних Державної служби статистики України щодо динаміки таких злочинів, зареєстрованих органами внутрішніх справ протягом 2009-2013 рр. Так, починаючи з 2010 р. спостерігається тенденція щодо їх зменшення (на 12,4% порівняно з 2009 р.). Ця тенденція посилилася

у 2011 р., оскільки було зареєстровано 131 злочин, на відміну від 190 у 2010 р. У 2012 р. зареєстровано 138 злочинів, що свідчить про їх незначне збільшення (7%). У 2013 р. зареєстровано 595 таких злочинів. Зростання цього виду злочинності обумовлено щорічним зростанням кількості користувачів Інтернет-ресурсу в Україні. Зокрема, згідно з даними Київського міжнародного інституту соціології, у вересні 2013 р. 49,8% дорослого населення України користувалися Інтернетом. Темп приросту протягом лютого 2012 р. по жовтень 2013 р. склав 16%, що трохи поступається рекордному стрибку в 34% у період з березня 2011 р. до лютого 2012 р.

Територіальний розподіл злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку свідчить про їх концентрацію у великих містах. Так, протягом 2009-2012 рр. найбільше злочинів було зареєстровано у Дніпропетровській, Донецькій, Запорізькій областях. Дещо змінилася ситуація у 2013 році, коли першість серед реєстрації цієї категорії злочинів одержала столиця України – Київ (163), далі – Одеса (67), Дніпропетровськ (47). За перше півріччя 2014 р. найбільше їх обліковано у місті Києві (37), Одеській (25), Львівській (27), Рівненській (19) та Миколаївській (15) областях. Найменше – у Закарпатській (2) та Вінницькій (2) областях. Таке становище передусім пов'язано із диспропорцією проникнення Інтернету в населені пункти різної величини. За даними Київського міжнародного інституту соціології, на даний момент значно відстає у поширенні Інтернету сільська місцевість через обмеження в технічних можливостях підключення малонаселених пунктів.

У структурі злочинності за період, що аналізується, найбільш поширеним є несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України). Так, в 2009 р. їх було зареєстровано 96 випадків, 2010 р. – 87, 2011 р. – 67, 2012 р. – 83, 2013 р. – 408.

Друге місце посіли несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК). За перше півріччя 2014 р. обліковано 26 таких кримінальних правопорушень. Їх кількість у 2013 р. складала 152 злочини на противагу 105, зареєстрованим у 2009 р.

До найменш поширених серед цієї категорії злочинів належать: перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК) та порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК). Такі злочини зафіксовано в одиничних випадках, а в окремі роки (2009-2010) вони навіть не реєструвалися.

Згідно із вказаними статистичними даними частка злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку в загальній структурі злочинності все ще є незначною, становлячи менше 1%. Вказане можна пояснити тим, що злочини у сфері комп'ютерної інформації належать до високолатентних. Проведені кримінологічні дослідження, засновані на опитуванні працівників правоохоронних органів та спеціалістів в галузі інформаційних технологій, показали, що за межами статистичних обліків залишаються до 90% кіберзлочинів [3]. Високу латентність таких злочинів пов'язують з небажанням потерпілих подавати заяви до органів внутрішніх справ; недосвідченістю працівників правоохоронних органів у розслідуванні цих злочинів; труднощами в кваліфікації; відсутністю спеціалізованих експертиз для розслідування комп'ютерних злочинів; труднощами збирання доказів; відсутністю комп'ютерної культури.

Та чи можна виправдати низький рівень протидії комп'ютерним злочинам їх високою латентністю? Мабуть, ні. На нашу думку, з метою ефективного запобігання вказаним злочинам необхідно значно удосконалювати чинне законодавство, зокрема такими шляхами:

1) з метою суттєвого покращення рівня виявлення, документування, розкриття та розслідування злочинів, що вчинюються з використанням комп'ютерних систем та телекомунікаційних мереж, необхідно чітко розмежувати компетенцію підрозділів боротьби з кіберзлочинністю МВС та контррозвідувального забезпечення інформаційної безпеки держави Служби безпеки України, які при виконанні службових обов'язків часто дублюють функції один одного;

2) потребує термінового вирішення питання законодавчого визначення статусу підприємств, установ, організацій, що надають доступ до мережі загального користування Інтернет, оскільки дотепер не розмежовано суб'єктів ринку телекомунікацій за послугами, які ними надаються, та не передбачено відповідальності за порушення вимог чинного законодавства. Діяльність постачальників інтернет-послуг не підлягає ліцензуванню та обов'язковій державній реєстрації, відсутні правові та організаційні основи ефективного співробітництва з суб'єктами ринку телекомунікацій та громадськістю у напрямку запобігання кіберзлочинності;

3) канали обміну інформацією про злочини цієї категорії з правоохоронними органами інших держав (Національний контактний пункт з обміну інформацією та реагування на кіберзлочини, Робочий апарат Укрбюро Інтерполу, Генеральна прокуратура та Міністерство юстиції України) категорично не задовольняють потреби сьогодення, оскільки унеможливлюють оперативне вирішення завдань з документування та розслідування кіберзлочинів, зокрема через неможливість первинної ідентифікації;

4) специфічність кіберзлочинів потребує залучення лише відповідних фахівців, що володіють необхідними навичками та знаннями, тому існує необхідність підвищення професійного рівня службових осіб різних відомств

правоохоронних органів та суддів. Крім того, необхідно вирішити питання щодо утворення у структурі Генеральної прокуратури та Головної судової адміністрації спеціалізованих підрозділів щодо здійснення нагляду за додержанням законів та розгляду кримінальних проваджень про кіберзлочини.

Також потребують удосконалення нормативно-правові акти, які закладають фундамент єдиної державної політики забезпечення інформаційної (кібернетичної) безпеки та її реалізації.

Першим кроком до здійснення цієї мети є визначення кібернетичної безпеки самостійною сферою національної безпеки, загроз, основних напрямів державної політики. Вказане надасть можливість формувати засади державної політики у сфері забезпечення кібернетичної безпеки України через визначення основних реальних і потенційних загроз національній безпеці кібернетичного характеру, основних напрямів державної політики та основних функцій суб'єктів щодо забезпечення національної безпеки в цій сфері.

Другим кроком є внесення змін до чинних нормативно-правових актів, які б визначали такі основоположні поняття, як «кібернетична безпека» («кібербезпека»), «кібернетичний простір» («кіберпростір»), «кібернетична злочинність» («кіберзлочинність») тощо.

Висновки. Все зазначене може створити правову основу для подальшої нормотворчої діяльності, спрямовану на розробку та вдосконалення національної системи кібернетичної безпеки, протидії кібернетичній злочинності тощо. Зокрема, потребують змін та доповнень закони:

– «Про оборону України» – щодо підготовки Збройних Сил України до відбиття агресії в кіберпросторі;

– «Про інформацію» – щодо статусу інформації, яка циркулює в ІТС та АСУ критичної інформаційної інфраструктури;

– «Про телекомунікації» – щодо приведення Закону у відповідність до Конвенції РЄ про кіберзлочинність;

– «Про боротьбу з тероризмом» – щодо боротьби з кібертероризмом;

– «Про ліцензування певних видів господарської діяльності» – щодо ліцензування обладнання та програмного забезпечення для застосування в ІТС об'єктів інформаційної інфраструктури;

– «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру» – щодо кіберзахисту об'єктів підвищеної небезпеки;

– «Про Збройні Сили України», «Про Службу безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України» – щодо уточнення компетенції та повноважень у зв'язку зі створенням Єдиної загальнодержавної системи кібернетичної безпеки.

Бібліографічні посилання

1. *Амелін О. В.* Електронна (комп'ютерна) інформація: нормативно-правове визначення в законодавстві України / О. В. Амелін // Вісник Національної академії внутр. справ. – 2014. – № 2 (91). – С. 117-127.

2. Кабінет Міністрів України. Інформативно-аналітичні та довідкові матеріали на

виконання п. 2 Постанови ВР України „Про проведення парламентських слухань на тему „Законодавче забезпечення розвитку інформаційного суспільства в Україні" від 11.03.2014 № 860-VII : Лист від 20.05.2014 № 6370/0/2-14.

3. *Спирина С.* Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации / С. Спирина [Электронный ресурс] – Режим доступа : http://www.dissercat.com/content/kriminologicheskie-i-ugolovno-pravovye-problemy-prestuplenii-v-sfere-kompyuternoi-informatsi.

4. *Ronald Noble.* The globalization of crime a transnational organized crime threat assessment [Електронний ресурс]. – Режим доступу : http://www.unodc.org/documents/data-and-nalysis_Report_2010_low_res.pdf.

5. Losses: Estimating the Global Cost of Cybercrime. – 2014 [Електронний ресурс]. – Режим доступу : http://www.mcafee.com/ca/resources/reports/economic-impact cybercrime2.pdf.

Богатырёва О. И., Амелин А. В. Анализ действующего законодательства о преступлениях в сфере использования компьютеров, систем и компьютерных сетей. Проанализировано действующее законодательство Украины в сфере использования компьютеров, систем и компьютерных сетей, а также выяснены отдельные проблемы, существующие в данной сфере. Предложены соответствующие направления совершенствования правовой базы путем внесения изменений и дополнений в конкретные нормативно-правовые акты в исследуемой сфере.

Ключевые слова: преступления в сфере использования компьютеров, систем и компьютерных сетей; законодательство; киберпреступность, противодействие.

Bogatyryova O., Amelyn O. Analysis by applicable law crime in use computers systems and computer networks. Threats and risks of their use grow with development of informatively-communication technologies. For today a cybercrime went out of the sphere of control of law enforcement authorities of one state and outgrew in a serious intergovernmental and transnational problem.

Revising the leading countries of the world priorities of informative public policy, presently develop and inculcate state strategies and programs of development of informative society, that are basis of prevention of criminality.

Unfortunately, during all years of independence of Ukraine, industry of information technologies developed practically without every interference from the side of the state. Government control of this industry was actually taken to collection of statistical indexes that did not represent the real position and basic tendencies of such important in modern society sphere of public relations often.

Presently operating legislation about crimes in the field of the use of computers, systems and computer networks is subject to the revision as not only operating norms of the Criminal code of Ukraine already do not answer the dynamics of development of criminality in this sphere but also there are other blanks in a current legislation, the decision of that will allow to change the state of criminogenic situation in the field of it on the best.

Taking into account marked, in the article the current legislation of Ukraine is analysed in the field of the use of computers, systems and computer networks, and also separate problems that exist in the field of given are found out. Offer corresponding directions of improvement of legal base in the field of marked, by making alteration and adding to the certain normatively-legal acts in the field of investigated. A dynamics, territorial distribution, is considered, structure of criminality in the field of indicated for period 2009–2013 and basic steps necessary for the substantial improvement of level of counteraction are certain.

***Keywords**: crimes in the field of the use of computers, systems and computer networks; legislation; cybercrime; counteraction.*

Надійшла до редакції 22.12.2014