УДК 004.056.347.77 **Стельмаховська О.І., Шорошев В.В. (ДУІКТ)**

МІЖНАРОДНІ НОРМИ ЩОДО ЗАХИСТУ АВТОРСЬКИХ І СУМІЖНИХ ПРАВ В МЕРЕЖІ INTERNET

В даній роботі висвітлюються чотири групи суспільно небезпечних діянь, які вимагають міжнародного співробітництва і контролю: злочинів проти конфіденційності, цілісності і доступності комп'ютерних даних і систем; злочинів, пов'язаних з використанням комп'ютерів, з порушенням авторських і суміжних прав на інтелектуальну власність та злочинів, пов'язаних з дитячою порнографією. Пропонується модель загроз для комп'ютерних даних і систем з урахуванням рекомендацій Конвенції Ради Європи про кіберзлочинність.

Тенденція до розширення міжнародного співробітництва у боротьбі зі злочинністю в галузі високих технологій відзначається у діяльності багатьох міжнародних організацій. Однією з них є Рада Європи, яка вважає, що без державного контролю комп'ютерних мереж обійтися не можна, а законодавче регулювання кіберпростору в одній окремо взятій країні навряд чи можливе. Тому зростання комп'ютерної злочинності вимагає узгодженого підходу держав до вироблення стратегії боротьби з нею. Очевидно, що дане протиріччя можна усунути тільки в рамках міжнародного права. Цій проблемі присвячено низку прийнятих Радою Європи рекомендацій, у яких зроблено спробу визначити поняття й окреслити коло "злочинів, пов'язаних з використанням комп'ютерних технологій та інтелектуальної власності на них". Однак рекомендаційний характер цих документів не сприяє вирішенню виникаючих на практиці колізій, для чого необхідні повноцінні міжнародно-правові документи.

Конвенція Ради Європи про кіберзлочинність являє собою комплексний документ, що містить норми, покликані вплинути на різні галузі права: карного, карно-процесуального, авторського, цивільного, нормативно-правового. Конвенція ґрунтується на головних принципах міжнародного права: поваги прав людини, співробітництва і сумлінного виконання зобов'язань за її рекомендаціями.

Норми права Конвенції спрямовані на імплементацію у нормативно-правові засади країн-учасниць Конвенції трьох основних блоків питань:

зближення кримінально-правової оцінки злочинів у сфері комп'ютерної інформації;

зближення національних карно-процесуальних заходів, спрямованих на забезпечення збору доказів при розслідуванні таких злочинів;

міжнародне співробітництво у карно-процесуальній діяльності, спрямоване на збирання доказів здійснення таких злочинів за кордоном.

Кримінально-правові питання. Нормами права Конвенції пропонується включити в законодавство країн-учасниць єдині норми про кримінальну відповідальність за "кіберзлочинність", перелік яких включає:

- діяння, спрямовані проти комп'ютерної інформації (як предмета злочинного зазіхання) і які використовують її в якості унікального знаряддя здійснення злочину;

- діяння, предметом зазіхання яких є інші охоронювані законом блага, а інформація, комп'ютери тощо є лише одним із елементів об'єктивної сторони злочину, наприклад, знаряддям його здійснення, складовою способу здійснення чи приховання злочину.

Об'єктом кіберзлочинів, відповідно до Конвенції, є широкий спектр охоронюваних нормами права суспільних відносин, що виникають при здійсненні інформаційних процесів з приводу виробництва, збору, обробки, накопичування, збереження, пошуку, передачі, поширення і споживання комп'ютерної інформації без порушення права на *інтелектуальну власність*, а також в інших галузях, де використовуються комп'ютери, комп'ютерні системи і мережі.

Серед них, з огляду на підвищену суспільну значимість, нормами права Конвенції вирізняються *правовідносини, що виникають у сфері забезпечення конфіденційності,*

цілісності і доступності комп'ютерних даних та систем, законного використання комп'ютерів і комп'ютерної інформації (даних), авторського та суміжного прав на інтелектуальну власність.

Об'єктивна сторона кіберзлочинів характеризується виокремленням чотирьох груп суспільно небезпечних діянь, успішна протидія яким можлива тільки за широкого міжнародного співробітництва країн-членів, що подписали Конвенцію Ради Європи. Для вироблення відповідної політики безпеки та її гармонізації з досягнутим міжнародним досвідом (рис.1) пропонується для порівняльного аналізу і використання модель потенційних загроз комп'ютерним даним і системам, регламентованих за нормами права Конвенції Ради Європи про кіберзлочинність. Розглянемо запропоновану в моделі класифікацію і зміст чотирьох груп суспільно небезпечних злочинів.

1. Злочини проти конфіденційності, цілісності і доступності комп'ютерних даних та систем.

Протизаконний доступ – одержання доступу до комп'ютерної системи загалом або до будь-якої її частини без права на те, що може розглядатися як злочин, якщо це вчинено в обхід заходів безпеки і з наміром заволодіти комп'ютерними даними чи з іншим безчесним наміром (особливо плагіат), або щодо комп'ютерної системи, з'єднаної з іншою комп'ютерною системою.

Протизаконне перехоплення комп'ютерних даних, якщо його здійснено з використанням технічних засобів перехоплення без права на це і для непублічних передач комп'ютерних даних у комп'ютерну систему, з неї чи всередині такої системи, в т.ч. електромагнітні випромінювання комп'ютерної системи, що несуть такі комп'ютерні дані, а також якщо це вчинено в обхід заходів безпеки і з наміром заволодіти комп'ютерними даними чи іншим безчесним наміром (досить поширене на цей час через Internet порушення права *інтелектуальної власності*) щодо комп'ютерної системи, з'єднаної з іншою комп'ютерною системою.

Порушення цілісності даних – ушкодження, стирання, псування, зміна або блокування комп'ютерних даних без права на це, у тому числі винятково у випадках, які призвели до серйозних наслідків.

Втручання в роботу (функціонування) системи – створення без права на це серйозних перешкод роботі комп'ютерної системи шляхом уведення, передачі, ушкодження, стирання, псування, зміни чи блокування комп'ютерних даних.

Протиправне використання пристроїв:

виробництво, продаж, придбання для використання, імпорт, оптовий продаж чи інші форми надання в користування: (1) пристроїв, у т.ч комп'ютерні програми, розроблені чи адаптовані, насамперед для цілей здійснення злочинів; (2) комп'ютерних паролів, кодів доступу або інших подібних даних, за допомогою яких може бути отриманий несанкціонований доступ до комп'ютерної системи загалом чи до будь-якої її частини, з наміром використовувати їх з метою здійснення злочинів;

володіння одним із предметів, що згадуються вище, з наміром використовувати його з метою здійснення злочинів .

2. Злочини, пов'язані з використанням комп'ютерів (рис. 1, друга колонка).

Підробка з використанням комп'ютерів – уведення, зміна, стирання чи блокування комп'ютерних даних, що призводять до порушення автентичності даних з наміром, щоб вони розглядалися або використовувалися в юридичних цілях та начебто вони залишаються справжніми, незалежно від того, чи ці дані читаються безпосередньо, чи зрозумілі.

Шахрайство з використанням комп'ютерів – позбавлення іншої особи його власності (у тому числі *інтелектуальної власності*) шляхом уведення, зміни, стирання чи приховання комп'ютерних даних або втручання у функціонування комп'ютера або системи з метою неправомірного одержання економічної вигоди для себе чи для іншої особи.

3. Злочини, пов'язані з порушенням авторських і суміжних прав (рис.1, третя колонка).

*Порушення авторського права***,** передбаченого нормами внутрішньо державного законодавства, з урахуванням вимог Паризького акту від 24 липня 1971 р. до Бернської Конвенції про захист творів літератури і мистецтва, Угоди про пов'язані з торгівлею аспекти прав на *інтелектуальну власність* і Договори про авторське право **Всесвітньої організації інтелектуальної власності (ВОІВ)**, за винятком будь-яких моральних прав, наданих цими Конвенціями, коли такі дії навмисне відбуваються в комерційному масштабі і за допомогою комп'ютерної системи.

Порушення суміжних прав, пов'язаних з авторським правом:

порушення, передбачені нормами внутрішньо державного законодавства, з урахуванням вимог Міжнародної конвенції про захист прав виконавців, виробників звукозаписів і радіомовних організацій (*Римська конвенція*);

порушення угод щодо пов'язаних з торгівлею аспектів прав *інтелектуальної власності* і Договори ВОІВ про виконавців і звукозаписи, за винятком будь-яких наданих цими Конвенціями моральних прав, коли такі дії відбуваються навмисне в комерційному масштабі і за допомогою комп'ютерної системи.

Установлення як обов'язкової ознаки більш важких наслідків (матеріального збитку, протиправного використання отриманої комп'ютерної інформації тощо) Конвенцією залишено на розсуд держав-учасниць. Загалом норми Конвенції не передбачають обов'язковість настання шкідливих наслідків.

4. Злочин, пов'язані зі змістом даних (рис.1, четверта колонка)**.**

Правопорушення, пов'язані з дитячою порнографією (порнографічними матеріалами, що візуально відображають участь неповнолітньої чи удаваної повнолітньою особи в сексуально відвертих діях, а також реалістичні зображення, що представляють неповнолітніх, які беруть участь у сексуально відвертих діях), а саме:

виробництво з метою поширення через комп'ютерні системи;

пропозиція чи надання через комп'ютерні системи;

розповсюдження чи передача через комп'ютерні системи;

придбання через комп'ютерну систему для себе чи для іншої особи;

володіння дитячою порнографією, що знаходиться в комп'ютерній системі або в середовищі для збереження комп'ютерних даних.

Суб'єктом кіберзлочинів може бути фізична особа, яка скоїла зазначені вище дії.

Виходячи з практики, що складається в різних країнах, норми Конвенції вимагають установлення відповідальності юридичних осіб за правопорушення, передбачені нею. Умовами настання відповідальності юридичної особи є: (1) здійснення дії (2) з метою одержання вигоди на користь юридичної особи (3) його посадовою особою, що займає керівну посаду, (4) з використанням його повноважень по представленню юридичної особи, прийняттю рішень або здійсненню контролю за його діяльністю.

Крім того, Конвенція наказує установлювати відповідальність юридичних осіб також у випадках здійснення протиправних дій іншим працівником під керівництвом особи, що займає керівну посаду, з метою одержання вигоди на користь юридичної особи.

Суб'єктивна сторона кіберзлочинів. Усі злочини, згадані в нормах Конвенції, передбачають відповідальність тільки у випадку їх здійснення навмисне. У деяких статтях Конвенції, що встановлюють злочинність "традиційних" злочинів, вчинених з використанням комп'ютера чи комп'ютерної інформації, передбачено, що навмисна форма провини має характеризувати не лише саме діяння, а й протиправне їх використання, хоч це і є кваліфікуючою ознакою таких злочинів (приміром, ст. 8 – шахрайство з використанням комп'ютера). Поряд зі вчиненими злочинами в Конвенції передбачається необхідність установлення відповідальності за замах, співучасть чи підбурювання до його здійснення.

Відповідно до норм Конвенції встановлення конкретних санкцій за здійснення зазначених діянь віднесено ***до ведення держав країн-членів***, що підписали Конвенцію. На їх розсуд може встановлюватися ***кримінальна*** відповідальність для фізичних осіб, а також ***карна, цивільно-правова*** або ***адміністративна*** відповідальність юридичних осіб. Передбачені внутрішньодержавним законодавством санкції мають бути ефективними, пропорційними і переконливими.

Карно-процесуальні аспекти. Однієї з головних особливостей Конвенції є те, що в ній запропоновано виходити з того положення, що головна роль у регулюванні карного процесу розслідування злочинів у сфері комп'ютерної злочинності належить національному законодавству. У силу цього Конвенція включає гл. 2 "Заходи, що слід прийняти на національному рівні", якою передбачено включення в національний карний процес норм щодо процесуальних дій, специфічних для розслідування і судового розгляду по справах про комп'ютерні злочини.

У коло процесуальних норм, запропонованих у Конвенції для включення в національне законодавство, входять, насамперед, відомі слідчі дії, доповнені певними особливостями, пов'язаними зі специфікою, властивостями доказової інформації у формі комп'ютерних даних:

якщо під час обшуку є підстави думати, що шукані дані зберігаються в іншій комп'ютерній системі чи її частині і коли такі дані доступні з першої системи або можуть бути отримані з її допомогою, компетентні органи вправі негайно "поширити" вироблений обшук на цю іншу систему;

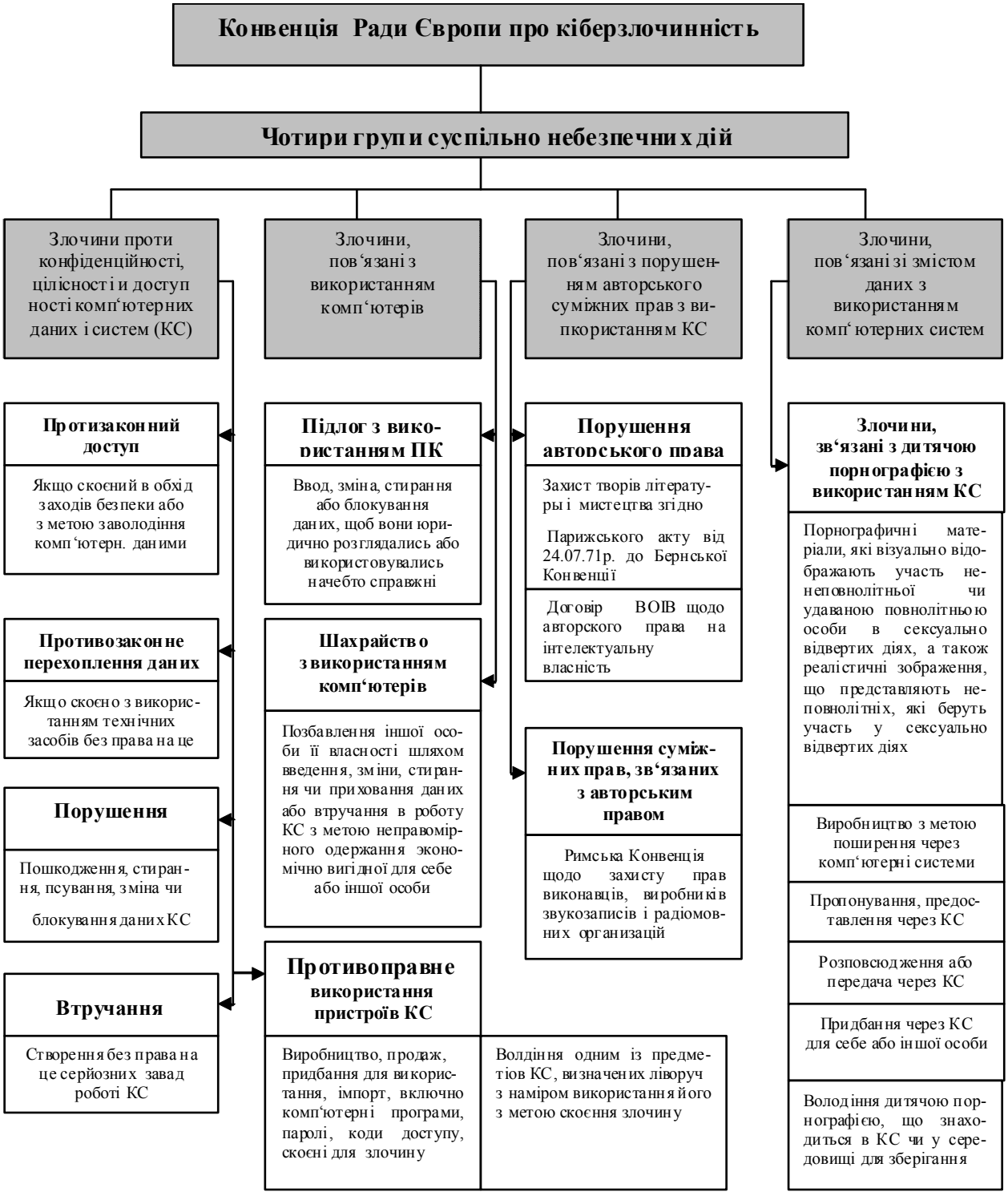
при виявленні шуканих комп'ютерних даних компетентні органи вправі: (a) зробити виїмку обчислювальної системи, її частини чи середовища для збереження комп'ютерних даних або іншим подібним чином накласти арешт на них; (b) виготовити і зберегти копії відповідних комп'ютерних даних; (c) забезпечити збереження цілісності стосовних до справи збережених комп'ютерних даних; (d) зробити ці комп'ютерні дані в комп'ютерній системі, доступ до якої був отриманий, недоступними або видалити їх з неї.

Для забезпечення виїмки необхідних комп'ютерних даних компетентні органи вправі зобов'язати будь-яку особу, яка володіє знаннями про функціонування відповідної комп'ютерної системи чи застосовувані заходи захисту, надати відповідну допомогу.

Поряд з цим у Конвенції передбачається необхідність формування на внутрішньодержавному рівні ***правових основ нових процесуальних дій***. До них також належать:

По-перше, негайне забезпечення схоронності збережених комп'ютерних даних, зокрема дані про потоки інформації, що були генеровані і збережені за допомогою комп'ютерної системи, коли маються підстави вважати, що ці дані особливо піддано ризику втрати чи модифікації. Воно має здійснюватися на підставі розпорядження компетентних органів, відданого будь-якій особі, у володінні чи під контролем якої знаходяться комп'ютерні дані. Конкретний термін збереження Конвенцією не встановлений, але позначений як "адекватний період часу, що дозволить компетентним органам домогтися розкриття цих комп'ютерних даних". Це означає, що запропонований процесуальний інститут не дає правових підстав для прямого доступу органів влади до комп'ютерної інформації, а лише створює передумови для нього, будучи мірою попереднього характеру.

При цьому під схоронністю даних слід розуміти залишення їх у тому вигляді, в якому вони вже зберігаються в ЕОМ, захистивши від будь-яких зовнішніх впливів;



Примітка: ВОІВ – всесвітня організація інтелектуальної власності;
КС – комп'ютерні данні і системи.

Рис. 1. Модель потенційних загроз комп'ютерним даним і системам за нормами права Конвенції Ради Європи про кіберзлочинність

По-друге, негайне забезпечення схоронності і часткове розкриття даних про потоки інформації. Воно відрізняється від попереднього тим, що підлягає застосуванню у випадках, коли йдеться про необхідність збереження зведень щодо повідомлення електрозв'язку, переданих по комп'ютерним мережам. Це має дозволити негайно зберігати

дані про потоки інформації "незалежно від того, один чи більше число постачальників послуг були втягнуті в передачу відповідного повідомлення", а з іншого - негайно розкривати ці дані компетентним органом в обсягах, достатніх, щоб "ідентифікувати постачальників послуг і шлях, яким передавалося повідомлення", тобто фактично для того, щоб оперативно відстежити проходження комп'ютерної інформації в мережах від місця введення до кінцевого адресата;

По-третє, віддача розпорядження про пред'явлення. Таке розпорядження може бути віддано (1) особі – про пред'явлення комп'ютерних даних, підконтрольних особі, що зберігаються в комп'ютерній системі або в іншому середовищі для збереження комп'ютерних даних, (2) постачальнику послуг – зведень про його абонентів. До останнього належить будь-яка наявна у постачальникові послуг інформація про користувачів, виражена як у формі комп'ютерних даних, так і в будь-якій іншій формі (за винятком даних про потоки чи зміст інформації), за допомогою якої можна установити: тип використаного зв'язку, його технічні умови і час здійснення; особистість користувача, його адреса, номери телефонів та інших засобів доступу, зведення про виставлені йому рахунки і зроблені їм платежі; будь-які інші зведення про місце установки комунікаційного устаткування. Слід зазначити, що норми Конвенції допускають застосування даного виду нових повноважень строго на індивідуальній основі для вирішення завдань розслідування конкретних кримінальних справ. У зв'язку з цим слід розуміти, що ці нові повноваження не повинні використовуватися з метою змусити всіх постачальників послуг постійно накопичувати і зберігати зведення про всіх своїх абонентів, усю передану ними комп'ютерну інформацію тощо;

По-четверте, збір і запис із застосуванням технічних засобів у режимі реального часу даних ***про потоки інформації, передані через комп'ютерні системи.***

Нормами Конвенції передбачено наділення повноваженнями здійснювати цю діяльність як компетентними органами держави, так і за їх указівкою постачальників послуг. Даний вид діяльності розрахований на застосування тощо зведень про повідомлення, переданих мережами електрозв'язку, що формуються (створюються) безпосередньо в момент реалізації таких повноважень. При цьому здійснюється передача нематеріальних об'єктів (наприклад, у формі електромагнітних імпульсів), а їх збір і запис не заважають проходженню самого повідомлення мережами електрозв'язку до адресата.

По-п'яте, перехоплення (збирання і запис) даних про зміст повідомлень, переданих за допомогою комп'ютерних систем, здійснюване як компетентними органами держави, так і постачальниками послуг за їх указівкою. Даний інститут аналогічний попередньому, але стосується безпосередньо змістовної частини повідомлень, переданих мережами електрозв'язку.

Хоча в нормах Конвенції детально і не прописано механізм правового регулювання реалізації двох останніх способів збирання комп'ютерної інформації, наявний досвід і співвіднесеність з нормами законодавства інших країн дозволяють стверджувати, що вони, імовірно, у даний час підлягають використанню шляхом проведення оперативно-розшукових заходів.

Запропонована модель потенційних загроз для комп'ютерних даних і систем з урахуванням рекомендацій Конвенції Рад Європи про кіберзлочинність та її тлумачення можуть бути корисними для фахівців при створенні захищених комп'ютерних систем, а також для гармонізації внутрішньодержавних законодавчих актів України як країни-учасниці щодо сумлінного виконання рекомендацій цієї Конвенції.

Література

1. Голубєв В.О. Розслідування комп'ютерних злочинів // Конвенція про кіберзлочиність: Монографія. – Запоріжжя: Запорізьк. інст. держ. та муніціп. управл., 2003.

2. Шорошев В.В., Близнюк И.Л., Балина С.Н. Классификация угроз для компьютерных данных и систем по рекомендациям Конвенции Совета Европы о киберпреступности // Бизнес и безопасность. №1, 2005. С.36-39.

3. С.Н.Соколов А.В., Степанюк О.М. Защита от кмпьютерного терроризма. Справочное пособие – СПб.: БХВ – Петербург; Арлит, 2002. – 496 с.

4. Близнюк І.Л., Шорошев В.В. Способи вчинення злочинів з використанням комп'ютерних систем та мереж.\\ Науковий вісник НАВСУ. – К., 2004. - № 6. С.118-132.

5. Шорошев В.В. Модель угроз для локальних вычислительных сетей по рекомендаціям Конвенции Сонета Европы о кибеопреступности. Науково-виробничий журнал Державної адміністрації зв'язку та інформатизації України "Зв'язок" № 4, 2005. С. 37-42.

6. А.Ю. Ільніцький, В.В.Шорошев, І.Л.Близнюк. Монографія "Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах органів внутрішніх справ України" (шифр "Торсіон-1"). Свідоцтво Державного департаменту інтелектуальної власності Міносвіти і науки України про реєстрацію авторського права на твір № 14446 від 20.11.2005 у вигляді програмного продукту "Торсіон-1". – К.: Видавництво НАВСУ, 2003р. – 316с.

7. Прогалини законодавства України щодо захисту авторських прав в Інтернет / Т.В. Курило, Н.В. Вербова // Наук. Вісн. Львів. Держ. Ун-ту внутрішніх справ. – 2008. - №1. – с.119-124.

8. Ступак С, Жучка О. Авторське право і суміжні права в інформаційному суспільстві в Європейських спільнотах і в Україні/ Юридична газета. – 2006. - №5.

Надійшла: 04.03.11

Рецензент: д.т.н., проф. Петров О.С.