УДК 002:34+004.056.5

к.т.н. **Мельник С.В.** (НА СБУ)
**Тихомиров О.О.** (НА СБУ)
**Лєнков О.С.** (ВІКНУ)

# ДО ПРОБЛЕМИ ФОРМУВАННЯ ПОНЯТІЙНО-ТЕРМІНОЛОГІЧНОГО АПАРАТУ КІБЕРБЕЗПЕКИ

***Стаття присвячена проблемі формування понятійно-термінологічного апарату кібербезпеки у сучасних умовах розвитку правової системи України. Її вирішення сприятиме гармонізації термінології національної та інформаційної безпеки і удосконаленню законодавства України.***

***Ключові слова: кібербезпека, кіберпростір, кіберзагроза, кіберзлочин, кібертероризм, кібервійна.***

***Статья посвящена проблеме формирования понятийно-терминологического аппарата кибербезопасности в современных условиях развития правовой системы Украины. Ее решение будет способствовать гармонизации терминологии национальной и информационной безопасности, а также усовершенствованию законодательства Украины.***

***Ключевые слова: кибербезопасность, киберпространство, киберугроза, киберпреступление, кибертерроризм, кибервойна.***

***The article is devoted to the problem of forming of concept-terminology vehicle of cybersecurity in the modern terms of development of the legal system of Ukraine. Its decision will be instrumental in harmonization of terminology of national and informational security, and also improvement of legislation of Ukraine.***

***Keywords: cybersecurity, cyberspace, cyberthreat, cybercrime, cyberterrorism, cyberwar.***

**Постановка проблеми.** Важливою теоретичною складовою будь-якої соціально значущої діяльності є напрацювання понятійно-термінологічного апарату, що забезпечує належний рівень галузевої та загальної комунікації суб'єктів цієї діяльності. Сьогодні широкого розповсюдження набули терміни кіберпростір, кіберзлочин, кібератака, кіберзброя та інші, що належать до особливо динамічної специфічної сфери діяльності людини, пов'язаної з обміном та обробкою електронних даних у глобальних інформаційно-комунікаційних мережах. Терміни з приставкою «кібер-» ще не отримали сформованого загальновизнаного значення ні на науковому, ні на нормативно-правовому рівні і залишаються предметом відкритої дискусії. Незважаючи на це, сфера до якої належать явища позначені цими термінами (кіберсфера) завдяки їх суспільній значущості, наприкінці 20 сторіччя стала об'єктом уваги на державному та міжнародному рівнях, а також об'єктом актуальних наукових досліджень.

Сучасні тенденції розвитку кіберсфери свідчать про невпинне збільшення її значення для подальшого розвитку суспільства, що зумовлює віднесення окремих груп суспільних відносин кіберсфери до сфери правового регулювання. Особливо актуально дана проблема постає відносно забезпечення національної безпеки та суспільно небезпечних діянь, які повинні набути статусу правопорушень у кіберсфері і тягнути за собою юридичну відповідальність. Можна стверджувати, що постає проблема формування правового понятійно-термінологічного апарату кіберсфери.

Означені чинники створюють гостру необхідність у законодавчому закріпленні основних понять кіберсфери з урахуванням сучасних та перспективних можливостей України, особливостей її правової системи, а також вимог, що висуваються до юридичної термінології та мови закону. Основними з цих вимог вважаються наступні: до термінологічного апарату – однозначність, адекватність, системність термінології, а також єдність її використання; до дефініцій та тлумачень понять – ясність і простота, точність і повнота, лаконічність, послідовність викладення [1, с. 18-34].

З метою адекватного змістовного наповнення понятійно-термінологічного апарату кіберсфери доцільно, по-перше, звернутись до джерела виникнення приставки «кібер-» – кібернетики та ґенези її значення, по-друге, встановити групу термінів, що будуть мати ключове значення для всього термінологічного апарату.

Вперше термін «кібернетика» введено в обіг древньогрецьким філософом Платоном для позначення мистецтва кормчого (у перекладі з грецької κυβερνητική – мистецтво управління). У 1834 французький вчений Андре Марі Ампер використав цей термін для позначення не існуючої ще у той час науки про управління суспільством. Офіційною датою народження кібернетики як окремої науки вважається рік опублікування книги Норберта Вінера «Кібернетика» (1947) у якій він визначив кібернетику як науку «про управління і зв'язок у тварині і машині».

У сучасному розумінні кібернетика – це наука про управління, зв'язок і переробку інформації. Об'єктом дослідження сучасної кібернетики є кібернетичні системи, які розглядаються абстрактно (безвідносно до їх реальної природи), що дозволяє проводити дослідження технічних, біологічних, соціальних систем загальними методами. Кібернетична система представляється у вигляді сукупності взаємопов'язаних об'єктів – елементів системи, що здатні запам'ятовувати, обробляти інформацію та обмінюватись нею з іншими елементами та зовнішнім світом. Система може змінювати структуру в результаті виникнення нових елементів, зникнення старих, а також зміни зв'язків між елементами. Прикладами таких систем є автопілот, електронна обчислювальна машина (комп'ютер), людський мозок, суспільство. Комп'ютер розглядається як універсальний перетворювач інформації, що здатний, запам'ятовуючи структуру іншої кібернетичної системи, виконувати її функції як перетворювача інформації. Саме ця якість робить його найфункціональнішою відомою кібернетичною системою та основним технічним засобом моделювання й вивчення інших кібернетичних систем будь якої природи [2].

Фундаментальне місце у термінологічному апараті кіберсфери доцільно віддати терміну «кіберпростір», що означає середовище, яке створює інтегративну основу всіх кіберявищ. І хоча його закріплення законодавством не є обов'язковим, встановлення герменевтичних особливостей кіберпростору сприятиме адекватному змістовному наповненню всього понятійно-термінологічного апарату кіберсфери.

Ґрунтуючись на сучасному розумінні кібернетики, кіберпростір можна розглядати як складну систему, що нерозривно поєднує у собі характеристики соціальних і технічних кібернетичних систем. Найсуттєвішими з цих характеристик відповідають рисам сучасних глобальних інформаційно-комунікаційних мереж (систем):

– широкі можливості управління, зв'язку та обробки інформації;

– реалізація за допомогою комп'ютерних систем;

– тісний зв'язок технології кіберпростору з розумом людини (технології виступають продовженням розуму на шляху ефективного досягнення мети);

– присутність як детермінованих закономірностей так і синергетичних та випадкових процесів;

– неосяжність меж розвитку і трансформації.

Враховуючи ті чи інші з означених характеристик можна сформувати широке та вузьке розуміння кіберпростору.

У широкому розумінні кіберпростір співпадає зі сферою використання комп'ютерів, автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку. На загальнонауковому рівні такий підхід може бути цілком припустимим. Однак, перехід у сферу правового регулювання привносить свій специфічний акцент. Право – універсальний соціальний регулятор, предметом його регулювання є суспільні відносини (поведінка суб'єктів). Виокремлення сфери суспільних відносин, пов'язаної з кіберпростором або кіберсферою, у якості предмета правового регулювання піднімає нові проблеми яким до цього часу не приділялося достатньої уваги. По-перше, важливим є розмежування нових для сфери правового регулювання видів поведінки суб'єкта, що належать до кіберпростору, та

вже регламентованої правовими нормами поведінки, що стосується комп'ютерних систем як об'єктів матеріального світу. По-друге, не менш важливим є усвідомлення змісту поведінки у кіберпросторі та її зовнішнього виразу.

Очевидно, що у межах широкого розуміння кіберпростору, вирішення цих проблем ускладнюється, оскільки діяння, пов'язані зі створенням, модифікацією, знищенням матеріальних компонентів комп'ютерних систем та мереж, а також фізичним втручанням у їх функціонування, можуть бути віднесені до діянь у кіберпросторі, при цьому не маючи безпосереднього зв'язку з використанням його технологічних можливостей.

Невирішеність даної проблеми простежується і у ратифікованій Україною Європейській Конвенції про кіберзлочинність, яка не передбачає обмеження способів та цілей протиправних діянь щодо комп'ютерних систем, мереж і даних, відносячи всі їх прояви до кіберзлочинів, тобто злочинів пов'язаних з кіберпростором [3].

Одним із шляхів вирішення означених проблем, а також проблеми гармонізації термінології може стати більш вузьке розуміння кіберпростору.

У вузькому розумінні сучасні дослідники ототожнюють кіберпростір з віртуальним простором, що відкидає його матеріальну (апаратну) складову. Віртуальний простір можна визначити як змодельований за допомогою комп'ютера інформаційний простір, у якому знаходяться відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому виді, що перебувають у процесі руху по локальним і глобальним комп'ютерним мережам, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі [4]. Іншими словами, кіберпростір виявляється у єдності інформаційних ресурсів, представлених у вигляді електронних комп'ютерних даних, та сукупності технології, що забезпечують можливості їх обміну та перетворення. Відповідно цьому підходу, до діянь у кіберпрострорі необхідно відносити лише ті діяння, що пов'язані з безпосереднім використанням технологічних можливостей кіберпростору, незалежно від наслідків які вони спричиняють.

Таким чином, ***кіберпростір*** – це простір, сформований інформаційно-комунікаційними системами, у якому проходять процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, представленої у вигляді електронних комп'ютерних даних. Ініціювання цих процесів та управління ними доцільно розглядати як зовнішній вираз поведінки суб'єкта у кіберпросторі, а сам кіберпростір обов'язково повинен розглядатися у якості засобу діяльності, хоча одночасно може виступати і її метою.

Особливо актуальною для правової системи України видається проблема формування та змістовного наповнення комплексу термінів, пов'язаних із протиправними діяннями у кіберсфері.

Науковцями пострадянського простору активно використовуються терміни «комп'ютерний злочин», «злочин у сфері комп'ютерної інформації», «злочин у сфері використання комп'ютерів», «злочин у сфері використання інформаційних технологій», «кіберзлочин» тощо. Більшість з них позначають правопорушення, що можуть виходити поза межі кіберпростору.

Так, наприклад, В.М. Бутузов, аналізуючи комп'ютерну злочинність, відносить до неї злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку і визначає їх як посягання на відносини у сфері комп'ютерної обробки інформації, на права власності фізичних та юридичних осіб на інформацію і доступ до неї [5, с. 94]. Очевидно, що у такому розумінні поняття комп'ютерного злочину є значно ширшим ніж поняття протиправного діяння у кіберсфері.

Більшою мірою сутність протиправних діянь у кіберсфері відображає поняття кіберзлочину, який на думку українських та російських фахівців може визначається як винне протиправне втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціоновану модифікацію комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, здійснені за допомогою комп'ютерів, комп'ютерних мереж і програм [4].

Зарубіжними фахівцями поняттям злочину, здійсненого у кіберпросторі, охоплюються будь-які протиправні діяння, що здійснюються за допомогою комп'ютерної системи або мережі, у рамках комп'ютерної системи або мережі або проти комп'ютерної системи або мережі. Такий підхід напрацьовано експертами Організації Об'єднаних Націй та Радою Європи у 2000-2001 роках [3; 6].

Загальні ознаки цих діянь, окреслені Конвенцією про кіберзлочинність, підписаною державами-членами Ради Європи у 2001 році і ратифікованою Україною у 2005 році. До них належать: незаконний доступ до комп'ютерної системи, нелегальне перехоплення даних, втручання у дані, втручання у систему, зловживання пристроями, підробка та шахрайство пов'язані з комп'ютерами; правопорушення, пов'язані з дитячою порнографією; правопорушення, пов'язані з порушенням авторських та суміжних прав [3].

Слід наголосити, що як Конвенцією про кіберзлочинність, так і більшістю наукових праць у цій сфері, протиправні діяння розглядаються безвідносно ступеня суспільної небезпеки (шкоди), але вимагається встановлення на рівні національних законодавств кримінальної відповідальності за них. Водночас, ст. 11 КК України визначає, що не є злочином дія або бездіяльність, яка хоча формально і містить ознаки будь-якого діяння, передбаченого КК України, але через малозначність не становить суспільної небезпеки, тобто не заподіяла і не могла заподіяти істотної шкоди фізичній чи юридичній особі, суспільству або державі.

Зазначене свідчить про необхідність інтерпретації протиправних діянь у кіберсфері крізь призму принципів правової системи України, згідно яким виділяється дві загальні групи правопорушень: злочини (найбільш суспільно небезпечні діяння, визначені КК України) та проступки (менш небезпечні діяння передбачені іншими нормативно-правовими актами України). Тоді доцільним видається введення родового для неправомірних діянь у кіберсфері поняття – «кіберправопорушення», що забезпечить формування загального уявлення щодо них.

***Кіберправопорушення*** – це суспільно небезпечне винне діяння, що здійснюється з використанням технологій перетворення (створення, зберігання, обміну, обробки та знищення) інформації, представленої у вигляді комп'ютерних даних, і тягне за собою юридичну відповідальність. Кіберправопурушення має всі загальні ознаки правопорушення, що виділяються у теорії права та вирізняється лише факультативною частиною юридичного складу, у якому кіберпростір виступає як засіб або мета здійснення правопорушення.

Відповідно, до ***кіберзлочинів*** слід віднести найбільш небезпечні кіберправопорушення за які встановлюється кримінальна відповідальність. А до ***кіберпроступків*** – всі інші кіберправопорушення, що не несуть суттєвої суспільної небезпеки, за які передбачається юридична відповідальність інших видів, насамперед адміністративна.

Враховуючи сучасні тенденції розуміння інформаційної безпеки, кіберправопорушення можна розглядати у вузькому і широкому розумінні. У вузькому – це протиправні діяння, що призвели до порушення конфіденційності, цілісності, авторства та доступності інформації в інформаційно-телекомунікаційних системах у рамках їх технологічних функцій. У широкому розумінні до кіберправопорушень додатково можна віднести протиправні діяння, що призвели до реалізації деструктивних інформаційно-психологічних впливів на свідомість, психологічний та психічний стан людей, здійснених з використанням можливостей сучасних інформаційно-телекомунікаційних систем.

Слід зазначити, що технологічна складова всіх кіберправопорушень є однаковою – це використання технічних недоліків механізмів безпеки сучасних інформаційно-комунікаційних систем, методів соціальної інженерії та сучасних технологічних можливостей впливу на цільову аудиторію через кіберпростір, що робить його незрівнянно дієвим засобом досягнення різноманітних злочинних цілей. Крім того, доцільно зважати на технологічні можливості побудови прихованих каналів зв'язку та управління в інформаційно-телекомунікаційних системах (стеганосистем), що можуть бути використані

для організації противоправної діяльності, у тому числі розвідувально-підривного і терористичного характеру.

Саме тому посиленої уваги сьогодні потребують злочини проти основ національної безпеки, які завдяки ефективності кіберпростору як засобу здійснення, можуть набути загрозливих масштабів. До них у першу чергу належать тероризм, шпигунство, державна зрада, публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної та влади, а також дискредитація органів влади та держави на міжнародній арені. Найнебезпечнішим з них є сучасний прояв тероризму – кібертероризм.

У загальному розумінні ***кібертероризм*** уявляється як суспільно небезпечна діяльність, що полягає у свідомому, цілеспрямованому залякуванню населення та органів влади і здійснюється з використанням інформаційно-телекомунікаційних систем з метою досягнення злочинних цілей.

Тероризм має багато проявів та складових. Законом України «Про боротьбу з тероризмом» визначено низку протиправних діянь, що можуть мати місце в ході терористичної діяльності [7]. В першу чергу до них належать злочинні діяння, що відповідають ст. 112, 147, 258-260, 443, 444 КК України. Всі вони в окремих випадках, можуть бути віднесені до кіберзлочинів та терористичної діяльності у кіберпросторі. Однак квінтесенцією терористичної діяльності є терористичний акт (ст. 258 КК України), який у взаємозв'язку з кіберпростором, доцільно виділити окремим поняттям – «кібертерористичний акт». Для його дефініції можна скористатись визначенням кібертероризму сформульованим А. Щетиловим, що вдало відображає сутність «кіберскладової» цього явища, та законодавчою дефініцією терористичного акту, закріпленою ст. 258 КК України [8; 9].

Отже, ***кібертерористичний акт*** – це втручання в роботу компонентів інформаційно-телекомунікаційних систем та їх програмного забезпечення або несанкціонована модифікація комп'ютерних даних, що викликає дезорганізацію роботи критично важливих елементів інфраструктури держави й створює небезпеку для життя чи здоров'я людини або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів.

Сучасний період державотворення України відзначений поступовим формування комплексних підходів до національної безпеки, серед яких забезпечення інформаційної безпеки займає одне з провідних місць. Ст. 17 Конституції України інформаційна безпека визнана однією з найважливіших функцій держави, а Доктриною інформаційної безпеки України визначена невід'ємною складовою кожної зі сфер національної безпеки та, водночас, важливою самостійною сферою забезпечення національної безпеки [10; 11]. Активно розгортаються процеси розробки відповідних нормативно-правових актів, що створять правове підгрунтя державної діяльності щодо її забезпечення у всіх напрямках. Не мине уваги законодавця і нова на нормативно-правовому рівні, але важлива складова інформаційної безпеки – кібербезпека (кібернетична безпека). Актуальність даної проблеми вимагає першочергового поповнення понятійно-термінологічного апарату сфери національної безпеки України низкою термінів та понять концептуального рівня, що окреслять особливості безпеки у кіберсфері або кіберпросторі. До них можна віднести кібербезпеку, кіберзахист, кіберзагрозу, кібервійну, кіберзброю, кібератаку та запропонувати наступне їх визначення.

У контексті нормативно-правового розуміння національної та інформаційної безпеки ***кібербезпека*** може визначатися як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства,

своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері функціонування інформаційно-телекомунікаційних систем. У технологічному контексті кібербезпека – це процесс захисту кіберпростору від реальних та потенційних кіберзагроз. На філософсько-соціологічному рівні осмислення кібербезпеку можна інтерпретувати через сукупність умов функціонування суб'єкта у кіберпросторі, що забезпечують його оптимальний інформаційний розвиток.

***Кіберзагроза*** – дестабілізуючий фактор (чинник) негативного впливу на об'єкт безпеки, що здійснюється шляхом використання технологічних можливостей кіберпростору. До кіберзагроз відносяться загрози порушення конфіденційності, цілісності, авторства, спостережності та доступності інформації, також загрози деструктивних інформаційно-психологічних впливів на свідомість, психологічний та психічний стан людини.

***Кіберзахист*** – комплекс заходів правового, організаційного, економічного, технологічного, ідеологічного характеру тощо, спрямованих на забезпечення належного рівня нівелювання кіберзагроз.

***Кібервійна*** у загальному розумінні – це активне протистояння між суб'єктами, що передбачає застосування наступальних (оборонних) дій у кіберпросторі з метою нанесення (протидії нанесенню) шкоди будь-якого характеру. На міжнародному рівні кібервійна – це спосіб вирішення протиріч між державами та націями засобами деструктивного впливу через кіберпростір.

***Кіберзброя*** – сукупність інформаційно-телекомунікаційних технологій, що використовується для досягнення злочинних цілей та нанесення шкоди через кіберпростір.

***Кібератака*** – одна з наймасштабніших кіберзагроз сучасності. Кібератака може розглядатися і як самостійне явище, і як квінтесенція ведення кібервійни або здійснення терористичної діяльності у кіберпросторі. У такому контексті проглядаються паралелі між кібератакою та кібертерористичним актом, а оскільки ці поняття повністю не співпадають, то виникає необхідність напрацювання правової дефініції кібератаки як злочину.

Кібератака (кібернапад) у загальному розумінні – це використання технічних недоліків механізмів безпеки сучасного кіберпростору з метою дезорганізації роботи його елементів. З кримінологічної точки зору кібератака повинна виражатися у формі діяння, яке полягає у втручанні в роботу компонентів інформаційно-телекомунікаційних систем та їх програмного забезпечення або несанкціонованої модифікації комп'ютерних даних, що здійснюється через інформаційно-телекомунікаційні мережі з метою дезорганізації роботи їх елементів.

Світові тенденції посилення чинників негативного впливу, до яких крім розгортання активної терористичної діяльності належать ще й масштабні природні катаклізми, техногенні катастрофи, збройні та інформаційні протистояння, привертають особливу увагу до безпеки держави як провідного суб'єкта організації суспільного життя. Надійне та ефективне функціонування кожного з елементів механізму держави є важливим підґрунтям як національної безпеки загалом, так і безпеки кожного громадянина. Тому актуальним видається також розгляд таких нових понять сфери безпеки держави як кібербезпека держави, кіберінфраструктура держави та критична кіберінфраструктура держави.

***Кіберінфраструктура держави*** – це сукупність інформаційно-телекомунікаційних систем та мереж (обчислювальних засобів, каналів обміну даними, систем зберігання даних, засобів комутації та управління інформаційними потоками), що забезпечують функціонування механізму держави. Причому у широкому розумінні до кіберінфраструктури держави необхідно віднести також і організаційні структури та нормативно-правові механізми, що забезпечують належне функціонування інформаційно-телекомунікаційних систем та мереж.

***Критична кіберінфраструктура держави*** – кіберінфраструктура мінімального рівня розвитку, що забезпечує оптимальне функціонування елементів механізму держави у кіберпросторі та конкурентоспроможність держави на міжнародній арені. Критерієм віднесення до критичної кіберінфраструктури держави може виступати приналежність інформаційно-телекомунікаційних систем до таких, що мають загальнодержавний,

галузевий, відомчий або регіональний статус, або ж впроваджених на підприємствах, що мають стратегічне значення для держави.

**Висновки.** Кіберсфера (сфера обміну та обробки інформації, представленої у вигляді електронних комп'ютерних даних) відіграє все більшого значення у процесах розвитку українського суспільства. Негативні явища кіберсфери набувають загрозливих масштабів, що зумовлює необхідність охоплення її регулятивними та охоронними функціями права, а також підвищує увагу до кібербезпеки як до окремої складової національної безпеки України. У таких умовах важливим є системний підхід до формування понятійно-термінологічного апарату кібербезпеки, який забезпечить адекватне його змістовне наповнення, відповідність вимогам, що висуваються до правової термінології, а також гармонізацію з термінологією діючого українського законодавства та міжнародних актів.

ЛІТЕРАТУРА:

1. Пиголкин А.С. Язык закона / [под. ред. А.С. Пиголкина]. – М.: Юрид. лит., 1990. – 192 с.

2. Кибернетика // Украинская советская энциклопедия, т. 5. – К.: Главная редакция украинской советской энциклопедии, 1981. – С.7-8.

3. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 №2824-IV // Відомості Верховної Ради України. – 2006. – № 5-6. – Ст. 71.

4. Тропина Т.Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате // Сборник научных трудов международной конференции «Информационные технологии и безопасность». Выпуск 3. – К.: Национальная академия наук Украины, 2003. – С. 173 – 181.

5. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В.М. Бутузов. – К.: КИТ, 2010. – 408 с.

6. Преступления, связанные с использованием компьютерной сети / Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями //A / CONF. 187/10. [Електронний ресурс]. – Режим доступу: http://www.uncjin.org/Documents/congr10/10r.pdf

7. Про боротьбу з тероризмом: Закон України від 20.03.2003 №638-IV [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=638-15

8. Щетилов А. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом [Електронний ресурс]. – Режим доступу: http://www.crime-research.ru/library/chetilov.htm

9. Кримінальний Кодекс України: Закон України від 05.04.2001 №2341-III [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341-14

10. Конституція України: Закон України від 28.06.1996 №254к/96-ВР [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=254%EA%2F96-%E2%F0

11. Про Доктрину інформаційної безпеки України: Указ Президента України від 8 липня 2009 року №514/2009 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=514%2F2009

**Рецензент: д.т.н., проф. Лєнков С.В.**