РОЗДІЛ 6
КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ

УДК 343.1

ІСТОРИЧНИЙ РОЗВИТОК ЗАКОНОДАВСТВА УКРАЇНИ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

HISTORICAL DEVELOPMENT OF THE LEGISLATION OF COMBATING CYBERCRIME IN UKRAINE

Бельський Ю.А.,
ад'юнкт
Національна академія внутрішніх справ

У статті виділяються етапи розвитку законодавства України, що регулює відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Обґрунтовується необхідність виділення етапів розвитку законодавства у цій сфері з метою простеження тенденції розвитку та пошуку шляхів його подальшого вдосконалення.

Ключові слова: ЕОМ, етапи розвитку, протидія комп'ютерній злочинності.

В статье выделяются этапы развития законодательства Украины, которое регулирует ответственность за несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи. Обосновывается потребность выделения этапов развития законодательства в этой сфере с целью прослеживания тенденции развития и поиска путей его дальнейшего совершенства.

Ключевые слова: ЭВМ, этапы развития, противодействие компьютерной преступности.

The author of the article in result of analysis of legislation in area of combating of cybercrime determines the next periods:

1) soviet period as the period of Soviet legislation in Ukraine that regulate social relations in the field of information security;

2) post-Soviet period of the Law of Ukraine «On protection of information in automated systems» on July 5, 1994 № 80/94-BP which was first enshrined the basic concepts such as: access, lock, object, subject, protection and unauthorized actions on information;

3) the initial period of this period they were selected as the period when it was first enshrined in Article 198-1 of the Criminal Code of Ukraine from 1960 liability for intentional interference with operation of automated systems and distribution of software and hardware designed for illegal penetration into them;

4) early period which began with adoption of the new Criminal Code of Ukraine in 2001, in which «computer crime» has been allocated in separate section XVI «Crimes in the use of computers (computer) systems and computer networks», whose appearance was an objective necessity;

5) Period of implementation Convention of Cybercrimes in Ukrainian legislation should define the period after the signing of the Convention «On cybercrime» its provisions were largely reflected in national legislation;

6) the period of adaptation began in connection with the adoption of the Law of Ukraine «On State Program of Adaptation of Ukraine to the European Union» under which all subsequently adopted legislative acts were adopted with regard to compliance with European legislation. The adoption of this law determined the European direction of developing Ukrainian legislation;

7) current period began with the changes to Section XVI of the Criminal Code of Ukraine, as it was largely covered most of the concepts and types of attacks in the area of responsibility for crimes committed in the area of computer information;

8) information period started with the adoption of a number of acts that promote the establishment of information society in Ukraine and deepening international cooperation in combating computer crime.

Allocation periods of develop legislation in cyber crimes area allows to find the gaps in previous legal acts, and find the ways of improvement futures legal acts in this area.

Key words: computers, stages of development, combating computer crime.

В процесі розвитку нових засобів обчислювальної техніки та впровадження їх в повсякденне людське життя виникають також нові способи вчинення злочинів у цій сфері, що зумовлює необхідність своєчасної протидії. Досліджуючи історичний розвиток законодавства України про кримінальну відповідальність за несанкціоноване втручання в роботу ЕОМ, слід зауважити, що він нерозривно пов'язаний із розвитком самих ЕОМ, оскільки розвиток цієї категорії характеризувався спочатку виникненням ЕОМ, а потім подальшим виникненням законодавчого супроводження для встановлення регулювання у вказаній сфері.

По-перше, слід виділити радянський період формування законодавства у цій сфері. Перший злочин на території колишнього СРСР з використанням комп'ютерних технологій офіційно було зареєстровано у 1979 році у Вільнюсі. Від цього злочину збитки державі склали близько 80 тисяч рублів. Даний факт був занесений до міжнародного реєстру аналогічних правопорушень та є своєрідною точкою відліку виникнення «комп'ютерних злочинів» в СРСР [1, с. 73]. Якщо в СРСР комп'ютерні технології мали певний захист як майно, то з комп'ютерною інформацією, яка опрацьовувалася в самих машинах, ситуація була набагато гіршою. У радянському законодавстві існували окремі розрізнені норми і вони лише частково регулювали суспільні відносини у сфері комп'ютерної інформації. Хоча були певні нормативно-правові акти, в яких започатковані певні кроки на шляху до захисту комп'ютерної інформації. Це нерозголошення персональних даних про особу. Але такі акти не були достатньо ефективними, коли дані викрадались з комп'ютера, та виникали труднощі з кваліфікацією таких діянь. А якщо говорити про викрадення або привласнення інформації шляхом несанкціонованого копіювання, то діяння винної особи взагалі не можливо було

кваліфікувати як злочин. Оскільки в СРСР інформація, яка не відносилася до категорії, що захищається авторським правом, або стосовно якої не було встановлено режим користування з обмеженим доступом, не вважалась майном, тому не можливо було кваліфікувати подібне діяння як викрадення. З приводу цього Ю. М. Батурін висловився, що така інформація повинна бути захищена шляхом виділення її як самостійного предмету кримінально-правової охорони [2, с. 87].

Наступним періодом розвитку законодавства у сфері захисту ЕОМ став пострадянський період розвитку вітчизняного законодавства у цій сфері.

На початку 90-х років XX ст. виникла нагальна потреба модернізації кримінального законодавства, оскільки діючі норми не відповідали потребам кримінально-правового регулювання не тільки у сфері використання ЕОМ, якої не було тоді взагалі, а й кримінального законодавства в цілому.

Для усунення цього недоліку Верховною Радою України у 1992 році було прийнято постанову про схвалення Концепції судово-правової реформи в Україні та створення першої робочої Комісії з питань розробки нового законодавства, зокрема реформування кримінального законодавства України [3].

Уперше визначення таких понять, як «користування», «доступ», «блокування», «об'єкт», «суб'єкт», «захист» та «несанкціоновані дії щодо інформації», було закріплено в Законі України «Про захист інформації в автоматизованих системах» від 05 липня 1994 року № 80/94-ВР [4] (на сьогодні після внесених змін від 31 травня 2005 року відомий як Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 2594-IV [5]). Хоча Закон і не містить норм про кримінальну відповідальність, він виступає певним інструментарієм Кримінального кодексу України 1960 та 2001 років, оскільки містить в собі визначення більшості основних понять, залишається чинним та актуальним і на сьогодні, та постійно змінюється і доповнюється, про що свідчать останні зміни до нього від 19 квітня 2014 року [6]. Саме на виконання вищезгаданого Закону 20 жовтня 1994 року Верховною Радою України був прийнятий Закон України «Про внесення змін і доповнень до Кримінального кодексу України та Кримінально-процесуального кодексу України» № 218/94 – ВР [7], який доповнив Кримінальний кодекс 1960 року ст. 1981 «Порушення роботи автоматизованих систем». Цьому Закону передували прийняті закони, які прямо чи опосередковано торкаються цієї сфери. Це Закон України «Про інформацію» від 02 жовтня 1992 року № 2657-XII [8], що встановлював гарантії та охорону для громадян права на інформацію і визначив правові форми міжнародного співробітництва в галузі інформації, закладав правові основи інформаційної діяльності в Україні, та Закон України «Про науково-технічну інформацію» від 25 червня 1993 року № 3322-XII [9], що визначив основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу країни.

Проте, враховуючи усі попередньо прийняті закони у цій сфері, Закон України «Про внесення змін і доповнень до Кримінального кодексу України та Кримінально-процесуального кодексу України» так і не був узгоджений належним чином із законами що передували його прийняттю, та не охопив повною мірою ті поняття, які були закріплені в них, а лише відобразив у єдиній ст. 1981 Кримінального кодексу України (далі – КК України) тільки поняття автоматизованих систем [10].

Стаття 1981 КК України також передбачила відповідальність за дві самостійні форми злочинних дій:

1) умисне втручання у роботу автоматизованих систем, що призвело до перекручення чи знищення інформації або носіїв інформації;

2) розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручення або знищення інформації чи то носіїв інформації [7].

Саме закріплення вперше в КК України відповідальності за умисне втручання у роботу автоматизованих систем та розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в них, становить собою початковий період розвитку законодавства України про кримінальну відповідальність за злочини у сфері несанкціонованого втручання в роботу ЕОМ.

Такі вчені, як М. С. Вертузаєв, В. О. Голубєв, О. І. Котляревський та О. М. Юрченко зазначали, що зазначення в одній статті про «умисне втручання у роботу автоматизованих систем» та «розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи» було недоцільним, оскільки, на їх думку, ці дві частини статті являли собою два окремих самостійних склади злочинів та мали бути відображені в окремих нормах Кримінального кодексу 1960 року [11, с. 19-20]. Так, В. В. Лісовий зазначав, що у ст. 1981 Кримінального кодексу 1960 року передбачалися не «комп'ютерні» злочини, а злочини, що порушували роботу автоматизованих систем, та стверджував, що автоматизованою може визнаватися лише система з групи засобів обчислювальної техніки [12, с. 274]. Таку ж позицію висловлював М. С. Вертузаєв. Він вважав, що в зазначеній статті мова йшлася лише про автоматизовану систему, та вважав суттєвою різницю між окремим комп'ютером та автоматизованою системою [11, с. 207].

Виходячи з позицій науковців з цього приводу, визначення у Законі України «Про захист інформації в автоматизованих системах» та з позиції ст. 1981 Кримінального кодексу 1960 року можна дійти висновку, що у Кримінальному кодексі 1960 року передбачалися лише відносини, пов'язані із порядком використання та втручання в роботу автоматизованих систем. Такою позицією в нормі законодавець охопив лише захист порядку роботи автоматизованих систем, при цьому недостатньо охопивши захист комп'ютерної інформації. Тоді, якщо викрадалась інформація з комп'ютера, який не був обладнаний засобами зв'язку, тобто не знаходився в мережі та не являв собою складову автоматизованої системи, то такі злочинні дії не підпадали під ознаку злочину, передбаченого ст. 1981 Кримінального кодексу 1960 року.

Наступним періодом розвитку законодавства у сфері протидії комп'ютерній злочинності став період оновлення, або новітній період, після прийняття нового КК України. КК України 2001 року містив у собі цілий розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж», поява якого була об'єктивною необхідністю. Спочатку у ньому було 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». На сьогоднішній день розділ XVI зазнав певних змін та доповнень, які в основному вносилися у 2003–2005 роках. Зокрема у 2003 році сам розділ та ст. 361 КК України було доповнено Законом України «Про внесення змін до Кримінального кодексу України щодо відповідальності за незаконне втручання в роботу мереж електрозв'язку» від 05 червня 2003 року № 908-IV [613] нормою, що передбачає кримінальну відповідальність за втручання у роботу мереж електрозв'язку. Сьогодні назва розділу XVI має наступну назву: «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж

електрозв'язку». Певні зміни відбулись у ст. 361 КК України, яка була викладена в новій редакції. У ній була встановлена кримінальна відповідальність за втручання в роботу мереж електрозв'язку, змінена санкція, а ч. 2 статті була доповнена приміткою.

Внесені зміни можна вважати становленням сучасного періоду розвитку законодавства, оскільки було значною мірою охоплено більшість понять та видів посягань у галузі відповідальності за злочини, що вчиняються у сфері використання комп'ютерної інформації.

Питання захисту телекомунікаційних мереж та інформації, що в них обробляється, було відображено у Законі України від 18 листопада 2003 року «Про телекомунікації». У Законі надається визначення інформаційної безпеки телекомунікаційних мереж як здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації. Цей Закон передбачає, що оператори телекомунікацій зобов'язані забезпечувати захист технічних засобів від несанкціонованого доступу.

У ст. 33 Закону вказані обов'язки споживачів телекомунікаційних послуг не допускати дій, що можуть створювати загрозу для безпеки експлуатації мереж телекомунікацій, підтримки цілісності та взаємодії мереж телекомунікацій, захисту інформаційної безпеки мереж телекомунікацій, електромагнітної сумісності радіоелектронних засобів, ускладнювати чи унеможливлювати надання послуг іншим споживачам. Встановлено захист персональних даних споживачів телекомунікаційних послуг, а ст. 34 передбачає відповідальність за збереження відомостей щодо споживача оператором, провайдером телекомунікацій, отриманих при укладенні договору наданих телекомунікаційних послуг, у т. ч. отримання послуг, їх тривалості, змісту, маршрутів передавання тощо, та розголошення цієї інформації без згоди споживача [13].

Одним із основних документів у сфері захисту від комп'ютерної злочинності є Конвенція Ради Європи з кіберзлочинності, яку було підписано Україною 23 листопада 2001 року у Будапешті [14]. Вона була прийнята для протидії комп'ютерним злочинам та для співробітництва та координації діяльності правоохоронних органів різних держав. Підписання Конвенції про кіберзлочинність можна вважати новим періодом у формуванні національного законодавства та відповідальності за злочини у сфері ЕОМ. Його слід назвати післяконвенційним періодом, оскільки положення Конвенції про кіберзлочинність здебільшого знайшли своє відображення у національному законодавстві, проте не в повному обсязі, а в основному щодо положень матеріального права. Проаналізувавши перелік діянь, вказаних у Конвенції, які відносяться до кіберзлочинів, можна дійти висновку, що цей перелік є дещо ширшим, ніж діяння, передбачені розділом XVI КК України.

Проте, незважаючи на прийняті акти та значні кроки щодо протидії злочинності в цій сфері, у Комплексній програмі профілактики злочинності на 2001–2005 роки про комп'ютерні злочини та захист інформації не згадувалося [15].

У 2004 році було прийнято Закон України «Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу» [16]. Прийняття цього Закону можна вважати періодом адаптації законодавства у сфері захисту інформаційних комп'ютерних технологій, адже в подальшому прийняття всіх наступних актів обов'язково узгоджувалося із відповідністю законодавству Європейського Союзу, що визначило подальший вектор розвитку вітчизняного законодавства. Саме як логічне продовження цього Закону для подальшого розвитку законодавства у сфері адаптації вітчизняного законодавства до світових норм та удосконалення законодавства у сфері комп'ютеризованої обробки інформації 20 жовтня 2005 року було прийнято Указ Президента України № 1497/2005 «Про першочергові завдання щодо впровадження новітніх інформаційних технологій», яким було передбачено розроблення до 2010 року нормативно-правових актів та здійснення заходів, спрямованих на запобігання злочинності в сфері використання ЕОМ [17].

У Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 9 січня 2007 року [18] передбачено визначення поняття «інформаційна безпека» як стану захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Законом передбачається також вирішення проблеми інформаційної безпеки шляхом: створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів; підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань; вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері; розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Таким чином, можна зробити висновок, що на законодавчому рівні було закріплено прагнення до встановлення інформаційного суспільства в Україні та розширеного тлумачення поняття інформаційної безпеки, що передбачило не тільки технічний захист, а й захист від недостовірної «шкідливої» інформації та недопущення знищення, викривлення, перекручення інформації, що спричинили негативні наслідки застосування інформаційних технологій. Саме законодавче закріплення цього прагнення можна виділити як інформаційний період.

Для розвитку інформаційного суспільства в Україні, сприяння створенню умов для відкритого і прозорого державного управління, автоматизації адміністративних послуг та функцій органів державної влади було прийнято Розпорядження Кабінету Міністрів України від 13 грудня 2010 року № 2250-р, яким було схвалено Концепцію розвитку електронного урядування в Україні. Відповідно до Розпорядження, електронне урядування – це форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян [19]. По суті впровадження системи електронного урядування являє собою створення електронної системи взаємодії між державними органами, а також між ними та громадянами у разі надання адміністративних послуг. Така система на сьогодні потребує встановлення законодавчого захисту від стороннього впливу, тому на сьогодні існує потреба в модернізації закону про кримінальну відповідальність в частині посилення кримінальної відповідальності за несанкціоноване втручання в роботу ЕОМ що перебувають у користуванні органів державної влади. Слід відмітити, що кіберзахист державних електронних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури було визначено пріоритетними об'єктами охорони

Стратегією кібербезпеки України від 15 березня 2016 року [20]. На виконання положень Стратегії кібербезпеки було прийнято Положення про Національний координаційний центр кібербезпеки від 07 червня 2016 року, яким створено робочий орган Ради національної безпеки і оборони України, серед завдань якого визначено аналіз стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури [21]. Також Рекомендаціями парламентських слухань на тему: «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України» від 31 березня 2016 року, якими надано рекомендації щодо розроблення проектів державних програм економічного і соціального розвитку України, проектів законів України та нормативно-правових актів, що стосуються галузі інформаційно-комунікаційних технологій (далі – ІКТ) та інформаційного простору України. Зазначеними Рекомендаціями визначаються заходи та напрямки розвитку законодавства у зазначеній сфері. Серед яких Кабінету Міністрів України рекомендовано забезпечити переклад та запровадження в Україні міжнародних стандартів та кращих практик з ІКТ та кібербезпеки та розробити й запровадити механізми державно-приватного партнерства для управління кіберзахистом критичної інформаційної інфраструктури у запобіганні кіберзагрозам та в умовах кризових ситуацій, надзвичайного стану, в особливий період [22]. Зазначені рекомендації можна визначити як дороговказ для майбутнього розвитку законодавства в інформаційній сфері.

Аналізуючи законодавство України про кримінальну відповідальність за несанкціоноване втручання в роботу ЕОМ від радянського періоду до сьогодні можна дійти висновку, що прийняті норми не завжди узгоджувались між собою, інколи були суперечливими в розумінні існуючої проблеми, якими вони оперували та потребували суттєвого доопрацювання.

У законодавстві України та позиціях науковців досі немає чіткого розмежування між злочинами у сфері комп'ютерної інформації, злочинами з використанням ЕОМ, чи проникненням в ЕОМ. Незважаючи на дискусійність цієї проблеми, ми пропонуємо поняття комп'ютерного злочину як злочину, вчиненого щодо комп'ютерної інформації, який посягає на її захист та цілісність, і комп'ютерної інформації як інформації (відомостей), що відображені у формі, придатній для її обробки засобами ЕОМ.

Слід зауважити, що й досі не передбачено кримінальну відповідальність за посягання на урядові телекомунікаційні системи, комп'ютерні мережі та об'єкти критичної інформаційної інфраструктури, хоча на це міститься посилання в деяких нормативних актах, зокрема Стратегії кібербезпеки від 15 березня 2016 року та у Річній національній програмі співробітництва «Україна – НАТО» на 2016 рік.

ЛІТЕРАТУРА

1. Комп'ютерна злочинність : навчальний посібник / [П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін.]. – К. : Атіка, 2002. – 240 с.
2. Батурин Ю. М. Компьютерные правонарушения : криминализация, квалификация, раскрытие / Ю. М. Батурин, А. М. Жодзишский // Советское государство и право. – 1990. – № 12. – С. 86–94.
3. Про Концепцію судово-правової реформи в Україні : Постанова Верховної Ради України від 28 квітня 1992 року № 2296-XII // Відомості Верховної Ради України. – 1992. – № 30. – Ст. 426.
4. Про захист інформації в автоматизованих системах : Закон України від 05 липня 1994 року № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.
5. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 31 травня 2005 року № 2594-IV // Відомості Верховної Ради України. – 2005. – № 26. – Ст. 347.
6. Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації»» : Закон України від 27 березня 2014 року № 1170-VII // Урядовий кур'єр. – 2014. – № 74.
7. Про внесення змін і доповнень до Кримінального кодексу України та Кримінально-процесуального кодексу України : Закон України від 20 жовтня 1994 року № 218/94 // Відомості Верховної Ради України. – 1994. – № 45. – Ст. 409.
8. Про інформацію : Закон України від 02 жовтня 1992 року № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
9. Про науково-технічну інформацію : Закон України від 25 червня 1993 року № 3322-XII //Відомості Верховної Ради України. – 1993. – № 33. – Ст. 345.
10. Безпека комп'ютерних систем : злочинність у сфері комп'ютерної інформації та її попередження / [Вертузаєв М. С., Голубєв В. О., Котляревський О. І., Юрченко О. М.]. – Запоріжжя : ПВКФ «Павел», 1998. – 315 с.
11. Вертузаєв М. С. Комп'ютерна злочинність в Україні : міфи та реальність / М. С. Вертузаєв // Науковий вісник Української академії внутрішніх справ. – 1997. – Вип. 1. – С. 203–213.
12. Лісовий В. В. Порівняльний аналіз кримінального законодавства щодо комп'ютерних злочинів / В. В. Лісовий // Науковий вісник Національної академії внутрішніх справ України. – 2001. – Вип. 4. – С. 274–278.
13. Про телекомунікації : Закон України від 18 листопада 2003 року № 1280-IV // Голос України. – 2003. – № 244.
14. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07 вересня 2005 року № 2824-IV [Електронний ресурс]. – Режим доступу :
http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi
15. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні : Указ Президента України від 31 липня 2000 року № 28/2000 // Офіційний вісник України. – 2000. – № 31. – Ст. 1300.
16. Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу : Закон України від 18 березня 2004 року № 1629-IV // Урядовий кур'єр. – 2004. – № 74.
17. Про першочергові завдання щодо впровадження новітніх інформаційних технологій : Указ Президента України від 20 жовтня 2005 року № 1497/2005 // Урядовий кур'єр. – 2005. – № 207.
18. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09 січня 2007 року № 537-V // Голос України. – 2007. – № 21.
19. Про схвалення Концепції розвитку електронного урядування в Україні : Розпорядження Кабінету Міністрів України від 13 грудня 2010 року № 2250-р // Урядовий кур'єр. – 2011. – № 1.
20. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 року № 96/2016 // Урядовий кур'єр. – 2016. – № 52.
21. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07 червня 2016 року № 242/2016 // Урядовий кур'єр. – 2016. – № 108.
22. Про Рекомендації парламентських слухань на тему: «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України» : Постанова Верховної Ради України від 31 березня 2016 року № 1073-VIII // Голос України. – 2016. – № 71.