УДК 343.3/.7:004.056 (477)

БАТИРГАРЕЄВА В.С., *доктор юридичних наук, старший науковий співробітник,*
головний науковий співробітник ДНУ ІБП НАПрН України,
директор НДІ ВПЗ ім. академіка В.В. Сташиса НАПрН України.
ORCID: https://orcid.org/0000-0003-3879-2237.

ПРАВОВА ПЛАТФОРМА ДЛЯ ЗАБЕЗПЕЧЕННЯ В УКРАЇНІ ЕФЕКТИВНОГО ЗАХИСТУ ЦИФРОВИХ ТРАНСФОРМАЦІЙ СУСПІЛЬСТВА

Анотація. *У статті здійснено аналіз національних правових документів концептуально-стратегічного характеру, спрямованих на забезпечення в Українській державі захисту цифрових трансформацій суспільства з огляду на загрози й ризики, що зумовлюють потребу розробки й удосконалення таких документів. Крім того, наголошено на необхідності розв'язання низки завдань, що виникають у кримінальному праві та сутність яких випливає із запровадження інформаційно-комунікаційних технологій.*

Ключові слова: *інформаційний простір, цифрові трансформації, інформаційна безпеки, кіберзлочини, кримінально-правова охорона.*

Summary. *The article contains an analysis of national legal documents of a conceptual and strategic nature aimed at ensuring the protection of digital transformations of society in the Ukrainian state, taking into account the threats and risks that necessitate the development and improvement of such documents. In addition, the need to solve a number of problems that arise in criminal law and the essence of which follows from the introduction of information and communication technologies, is noted.*

Keywords: *information space, digital transformations, information security, cybercrime, criminal and legal protection.*

Аннотация. *В статье проведен анализ национальных правовых документов концептуально-стратегического характера, направленных на обеспечение в Украинском государстве защиты цифровых трансформаций общества с учетом угроз и рисков, которые обусловливают необходимость разработки и усовершенствования таких документов. Кроме того, отмечена необходимость решения ряда задач, которые возникают в уголовном праве и сущность которых вытекает из внедрения информационно-коммуникационных технологий.*

Ключевые слова: *информационное пространство, цифровые трансформации, информационная безопасность, киберпреступления, уголовно-правовая охрана.*

Постановка проблеми. На Другому Паризькому форумі миру, що відбувся у листопаді 2019 р., Генеральний секретар ООН А. Гутеріш серед п'яти сучасних загроз указав на розвиток технологій, які відкривають перед людством не лише нові можливості, а й водночас можуть призвести до зростання нерівності між державами і регіонами, що потягне за собою ще більш відчутний економічний, технологічний та геостратегічний розрив у світі [1]. Далі, розвиваючи думку про роль технологій у сучасному світі, Генеральний секретар ООН наголосив на спільному протистоянні таким загрозам, як кіберзлочинність та роботи-вбивці, додавши, що "автомати, які мають право і здатність чинити вбивства без участі людини, неприпустимі. Натомість, міжнародне співтовариство має прагнути до того, щоб штучний інтелект використовували у мирних цілях, для забезпечення гідного та мирного життя для всіх" [1].

Оскільки для сучасної цивілізації є характерним перехід від індустріального суспільства до суспільства інформаційного, що є проявом настання шостого технологічного (постіндустріального) укладу, при якому домінують біотехнології, що

ґрунтуються на результатах досліджень у галузі молекулярної біології та генної інженерії, нанотехнології, системи штучного інтелекту, глобальні інформаційні мережі й інтегровані високошвидкісні транспортні системи [2, с. 17], розробки реконструктивної хірургії та медицини та ін. [3], то лідируючі позиції серед новітніх досягнень, без сумніву, належать інформаційно-комп'ютерним технологіям. Ці технології присутні так чи інакше у структурі функціонування й застосування всіх інших технологій. Крім того, вони виступають й цілком самостійним феноменом, із приводу існування якого складаються відповідні суспільні відносини, кількість та інтенсивність розвитку котрих у теперішній час, без перебільшення, не поступаються масиву різноманітних відносин, що існують у виробничому, фінансовому, політичному, культурному та ін. сегментах життєдіяльності суспільства. Більше того, інтенсивність інформаційних відносин в останні 40 – 50 років настільки збільшилася, що інформація на початку XXI ст. перетворилася на одну з найбільш значущих у суспільстві цінностей. Без застосування інформаційно-комп'ютерних технологій не можна говорити й про цифрову трансформацію суспільства, яка зачіпає сьогодні, напевно, будь-яку сферу життєдіяльності суспільства та метою якої є створення суспільства саме інформаційного.

Інформаційне суспільство, до якого ведуть цифрові перетворення, пов'язується насамперед з явищем глобального інформаційного простору, буття якого, повторимося, зумовлюється розвитком високих інформаційно-комунікаційних технологій у цілому, застосуванням комп'ютерної техніки для обробки інформації та охопленням світу мережею Інтернету. Внаслідок цих процесів людство набуло своєрідного статусу жителів "глобального села", для якого географічні кордони втратили будь-яке принципове значення. До речі, термін "глобальне село" свого часу був уведений канадським культурологом, філософом і літературним критиком Маршаллом Маклюеном для розуміння ситуації, що виникла на планеті з появою електрики як засобу миттєвого зв'язку та похідних від нього електронних засобів комунікації. Учений, зокрема, описав те, як внаслідок появи якісних програмних продуктів електроніки Земна куля "стиснулася" до розмірів "села", і стала можливою миттєва інтерактивна передача повідомлень з однієї точки світу до будь-якої іншої [4, с. 254].

Ця думка не втратила своєї актуальності і через кілька десятиліть, коли українська вчена А.Б. Добровольська констатує, що "сучасні технології зв'язку стали імпульсом нової якості розвитку, створили передумову об'єднання людства в межах глобального інформаційного простору" [5, с. 63]. Але вже наші сучасники вперше зіштовхнулися із ситуацією, коли, здійснюючись головним чином в електронно-цифровій формі, циркуляція потоків інформації перетворилася на явище масштабного характеру, а формування правової оболонки упорядкованості та правомірності цієї циркуляції у вигляді відповідного законодавства все ще відстає від потреб нової інформаційної парадигми суспільства. У швидкоплинному світі, позначеному різною оцінкою наслідків глобалізації інформаційного простору, подібне запізнення рефлексії на небезпечні або принаймні неоднозначні явища інформаційного простору призводить як до виникнення й існування чималої кількості парадоксальних та неоднозначних ситуацій, що потребують унормування, так і до подальшого породження багатьох загроз і ризиків для прав і свобод суб'єктів такої комунікації. Тому і для нашої держави, що повною мірою включена до процесів цифрових трансформацій, пов'язаних із формуванням єдиного інформаційного простору, неабияке значення має проблема правового забезпечення інформаційної безпеки та захисту національних інтересів від реальних і потенційних небезпек.

Результати аналізу наукових публікацій. Над проблемою убезпечення цифрових трансформацій суспільства правовими засобами та підвищення їх ефективності працює

чимало зарубіжних і вітчизняних учених, що пояснюється, підкреслимо знов, глобальністю явища, яким є інформаційний простір, та масштабністю тих ризиків і загроз, що супроводжують цей процес і що, власне, визначають основні напрями захисту процесу подібної суспільної трансформації. Корисний доробок у цьому плані ми знаходимо у наукових працях вітчизняних учених В.М. Брижка, В.М. Бутузова, В.Д. Гавловського, І.В. Діордіца, О.Д. Довганя, І.М. Дороніна, Р.А. Калюжного, М.В. Карчевського, Ю.І. Когута, В.С. Куйбіди, В.А. Ліпкана, А.І. Марущака, В.М. Пасічника, В.Г. Пилипчука, О.Е. Радутного, К.В. Тітуніної, Т.Ю. Ткачука, В.М. Фурашева, М.Я. Швеця та багатьох інших [5 – 18]. Так само проблема убезпечення цифрових трансформацій знаходиться у фокусі уваги й зарубіжних дослідників (Л. Лесссіг (L. Lessig), В. Майер-Шонбергер (V. Mayer-Schunberger), М. Нілес (M. Nieles) at al., К. Лоу (K. Low) at al., Е. Сидоренко at al., Д. Валєєв (D. Valeev) at al. та ін.) [19 – 24].

Однак унаслідок великих темпів, що притаманні трансформації інформаційного простору, у цій площині виникають все нові й нові нагальні завдання, від успішного розв'язання яких залежить й успіх перетворення "звичайного" доцифрового формату цього простору на нову модель – цифрову. При цьому в Україні всі можливі ризики і небезпеки враховувати особливо важливо, оскільки, окрім, так би мовити, вже відомих і "традиційних" викликів, наш інформаційний простір "обтяжений" ще й проявами гібридної війни, яка ведеться проти України.

Метою статті є, по-перше, аналіз нормативно-правової бази, насамперед концептуально-стратегічного характеру, спрямованої на забезпечення в Україні ефективного захисту цифрових трансформацій суспільства з урахуванням тих загроз, що викликали необхідність її розробки; по-друге, окреслення завдань у галузі законодавства про кримінальну відповідальність, які необхідно розв'язати для ефективного правового захисту зазначеного процесу.

Виклад основного матеріалу. Наявність у сучасному світі необмеженої кількості загроз і ризиків для інформаційного простору і відповідно для самого процесу цифрової трансформації суспільства, без якої сьогодні неможливо уявити функціонування цього простору, потребує від держави активних дій щодо убезпечення цієї сфери. Недаремно у проекті Цифрової адженди України – 2020 ("Цифровий порядок денний" – 2020) було наголошено, що "цифровізація" України має супроводжуватися підвищенням довіри і безпеки при використанні інформаційно-комунікаційних технологій [25].

Одним із способів убезпечення тієї чи іншої сфери життєдіяльності суспільства є своєчасна правова рефлексія на існуючі загрози, а так само передбачення й запобігання виникненню нових. Під час розробки й подальшого вдосконалення в Україні правової платформи ефективного захисту суспільних відносин, пов'язаних із цифровою трансформацією, необхідно, по-перше, брати до уваги сутність захисту цих відносин, що зумовлюється завданням забезпечення інформаційної безпеки подібної трансформації і розкривається, власне, через це специфічне забезпечення; по-друге, враховувати складнощі, що пояснюються особливостями "матерії", яка вивчається, і що створюють ситуацію багатозадачності, з якою зіштовхуються як дослідники, так і законодавець разом із правозастосовниками, і, по-третє, провести ревізію того, що вже зроблено у площині правового регулювання певної сфери суспільних відносин. Водночас слід звернути увагу і на той факт, що розробка й удосконалення такої платформи мають проводитися з огляду на те, що, з одного боку, суспільні відносини із цифрової трансформації виникли порівняно недавно, а з другого, що ці відносини продовжують знаходитися у фазі активного розвитку. До того ж складність розв'язання конкретної проблеми зумовлюється низкою чинників, як-от: відсутність чіткого й однозначного

розуміння об'єкта правової охорони, у тому числі кримінально-правової, внаслідок розмитості меж охоронюваної сфери суспільних відносин та полідисциплінарності останніх; не розробленість термінологічного апарата, що позначає та описує найістотніші елементи розглядуваних суспільних відносин та питання, які виникають із цього приводу; недостатність досвіду законотворчої та правозастосовної діяльності під час захисту суспільних відносин із цифрової трансформації тощо.

Про значущість проблеми нормативного регулювання з метою захисту розглядуваної сфери говорить хоча б той факт, що, наприклад, Dr. Ulrich Sieber, розглядаючи проблему унормування протидії так званим комп'ютерним злочинам (які, звісно ж, є негативним супутнім явищем цифрової трансформації суспільства як такої), ще наприкінці 90-х років XX ст. виділив шість основних етапів формування спрямованого на таку протидію законодавства, що приймалося у різних країнах із 1970-х рр.: а) захист даних та захист недоторканності приватного життя; б) кримінальне законодавство щодо боротьби з економічними злочинами, пов'язаними з використанням комп'ютерів; в) захист інтелектуальної власності; г) захист від протизаконного та шкідливого контексту; д) кримінально-процесуальне законодавство та f) правове регулювання захисних заходів, таких як криптографія та вимоги щодо автентифікації [26]. Як бачимо, Dr. Ulrich Sieber зробив експозицію цієї проблеми нібито у лінійному вимірі. Проте жоден із розглянутих ученим у ретроспективі аспектів, якими визначалася логіка відповідного нормотворчого процесу, й дотепер не втратив своєї актуальності. Це перший висновок, який можна зробити. І другий висновок полягає в тому, що сфера цифрової трансформації суспільства характеризується не лише виключно позитивними для соціуму ефектами, а й негативними проявами, до числа яких належать, зокрема, відповідні правопорушення. Саме цей аспект змушує знов і знов повертатися до проблеми протидії їм та проблеми створення нормативної платформи для надійного захисту інформаційних відносин від будь-яких правопорушень.

На теперішній час до правових засобів забезпечення в Українському суспільстві процесу цифрових трансформацій слід віднести: 1) положення державних документів концептуально-стратегічного характеру, які відбивають національні інтереси України в інформаційній сфері як такій та у зв'язку із пришвидшенням процесів діджиталізації нашого суспільства, а так само завдання, що постають через необхідність убезпечення відповідної сфери, виходячи із динаміки сучасних загроз і ризиків для останньої; 2) положення регулятивного законодавства, спрямованого на розвиток інформаційної сфери в цілому; 3) охоронні норми адміністративного та кримінально-правового характеру; 4) міжнародні стандарти.

У свою чергу, правова платформа саме захисту цифрових трансформацій нашого суспільства представлена насамперед положеннями відповідних законодавчих актів, у тому числі охоронних галузей права, тобто адміністративного та кримінального права, а так само документами засадничого характеру, тобто тими, що визначають доктринально-стратегічні підходи до убезпечення аналізованої сфери життєдіяльності суспільства. Неабияке значення мають й міжнародні стандарти. Саме на аналізі положень перелічених груп документів хотілося б зосередити увагу. Але спочатку наголосимо на одній принциповій для нашого дослідження тезі.

Важливою вимогою, що ставиться до процесу цифрових трансформацій, є вимога інформаційної безпеки. Щоб краще організувати захист зазначеного процесу, потрібно розуміти сутність інформаційної безпеки, яка проявляється у таких аспектах. По-перше, інформаційна безпека є самостійною складовою системного явища – національної безпеки, спрямованої на досягнення стану захищеності особи, суспільства та держави від

різноманітних внутрішніх і зовнішніх загроз та ризиків. По-друге, інформаційна безпека входить до складу будь-якої іншої сфери національної безпеки – зовнішньополітичної, державної, воєнної, економічної, енергетичної, соціально-гуманітарної, екологічної, науково-технічної та ін. По-третє, інформаційна безпека розглядається як об'єкт кримінально-правової охорони, тобто система суспільних відносин, що динамічно розвиваються та забезпечують існування й реалізацію інтересів особи, суспільства та держави в інформаційній сфері. Отже, аналізована категорія вирізняється наскрізним характером, що, власне, визначає й особливості правового захисту процесу цифрових трансформацій нашого суспільства.

За кількістю нормативно-правових документів і числом практичних заходів, що сьогодні вживаються в нашій країні у сфері захисту цифрової трансформації, навряд чи будь-яка країна пострадянського простору випереджає Україну. Так, на теперішній час прийнято і діє (або діяло) чимало важливих документів концептуально-стратегічного характеру, в яких інформаційній безпеці відведено чільне місце; за відомостями Державної служби спеціального зв'язку та захисту інформації України, лише у 2021 р., зафіксовано 41 млн. підозрілих подій інформаційної безпеки, опрацьовано 160 тис. критичних подій, зареєстровано 147 кіберінцидентів [27].

Як правильно підкреслюється у науковій літературі, державна політика національної безпеки формується на основі певних нормативно-правових актів, у підґрунтя системи яких має бути покладена концепція, доктрина і стратегія національної безпеки [15, с. 152]. Протягом останніх п'ятнадцяти років в Україні змінили один одного чотири документи стратегічного характеру, в яких особливим чином наголошується на інформаційній сфері як об'єкті національної безпеки. Йдеться про Стратегії 2007, 2012, 2015 та 2020 рр. [28 – 31], спрямовані, повторимося, на захист засад національної безпеки. Не вдаючись до аналізу цих документів, що "завдають загальну траєкторію руху до окресленої мети і зорієнтовані на довгострокову перспективу, яка формується на основі зіставлення національних інтересів та загроз національній безпеці" [15, с. 153], а так само до розгляду підходів щодо розуміння феномену національної безпеки, зазначимо лише про одне: в усіх згаданих стратегіях підкреслено роль інформаційної сфери та інформаційно-комунікаційних (комп'ютерних) технологій (інфраструктури, систем) у забезпеченні національної безпеки України[1]. Крім того, ще у 2007 р. зазначалося, що безпека інформаційно-комп'ютерних систем в галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо наближається до критичного стану [28]. У документі 2012 р. прямо наголошено на нездатності України протистояти новітнім викликам національній безпеці, пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам [29]. Тому серед першочергових засобів нейтралізації цих загроз робився акцент принаймні на забезпеченні безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури, а так само на розробці та впровадженні

[1] *Примітка*. Хоча в теорії права й вважається, що концепція національної безпеки містить певну керівну ідею, що розкривається у доктрині як певній системі принципів, поглядів, настанов та проблем забезпечення національної безпеки із подальшою деталізацією та конкретизацією у стратегії, див. [32, с. 249-250]). Проте аналіз концептуально-стратегічних підходів до захисту цифрової трансформації українського суспільства ми починаємо саме з розгляду стратегій національної безпеки, що за часом в Україні з'явилися дещо раніше за доктрини інформаційної безпеки.

національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними стандартами держав-членів ЄС, у тому числі згідно з вимогами Конвенції про кіберзлочинність [29].

У Стратегії 2015 р. серед актуальних загроз національній безпеці України окремо виділено загрози інформаційній безпеці, зумовлені веденням інформаційної війни проти України, відсутністю цілісної комунікативної політики держави, недостатнім рівнем медіа-культури суспільства, та загрози кібербезпеці і безпеці інформаційних ресурсів, проявом яких є уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [30].

Стратегія 2020 р. уперше згадує про те, що Україна має намір здійснити цифрову трансформацію, забезпечуючи надання адміністративних послуг через безпечне "єдине вікно" з використанням сучасних інформаційних технологій, та поширювати цифрову грамотність [31].

Не можна не згадати і про Стратегію розвитку інформаційного суспільства в Україні 2013 р., в якій на той час наголошувалося, що національна інформаційна сфера перебуває у стані активного становлення, гармонійного включення у глобальний світовий інформаційний простір та є основою розвитку інформаційного суспільства в Україні [33]. При цьому наочними показниками цих процесів мали б стати, зокрема, е-демократія, е-урядування, е-освіта, е-культура, е-медицина, інформаційна безпека та ін. [33] Є примітним, що про загрози інформаційній безпеці в наведеній Стратегії згадується лише мимохідь.

Наприкінці 2021 р. в Україні прийнято нову Стратегію здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та План заходів з її реалізації [34]. Зазначені документи прийняті для забезпечення якісної цифрової трансформації у певних сферах господарювання, пов'язаних з обігом матеріальних цінностей: як-от управління державними фінансами, діяльність із державного внутрішнього фінансового контролю, моніторингу та оцінки фіскальних ризиків, максимальна автоматизація бізнес-процесів та ін. У Стратегії як на окрему мету вказано на інформаційну безпеку в Єдиній інформаційно-телекомунікаційній системі Системи управління державними фінансами від сучасних кіберзагроз в умовах цифровізації управлінських процесів та необхідності обміну даними [34].

Разом із тим в Україні стали прийматися засадничі документи, які повністю присвячені питанням інформаційної безпеки. Так, у 2021 р. у цій сфері з'явилися одразу дві стратегії. Одна з них – Стратегія інформаційної безпеки, в якій визначаються поняття "інформаційна безпека" та "інформаційна загроза". У документі справедливо наголошується, що цифрова трансформація суспільства впливає на стан захищеності права особи на приватність внаслідок збільшення кількості соціальних мереж, їх інтегрованості з іншими соціальними сервісами повсякденного користування, а також внаслідок специфіки організації всесвітньої мережі Інтернет [35]. Уявляється, що перелік наведених у Стратегії внутрішніх і зовнішніх загроз дозволяє зрозуміти не лише можливі напрями захисту, а й домірність тих засобів, що сьогодні можуть бути запропоновані для нейтралізації цих загроз.

Другий документ стратегічного характеру, що був прийнятий у 2021 р., – Стратегія кібербезпеки України "Безпечний кіберпростір – запорука успішного розвитку країни" [36]. З огляду на чисельні для України загрози і виклики, якими насичений кіберпростір, в епоху цифрових трансформацій, до яких, ще раз підкреслимо, активно долучилася наша країна, підвищується значення й роль кібербезпеки. Як справедливо зазначається

Ю.І. Когутом, у період глобалізації швидкий розвиток інформаційних технологій, нових систем комунікаційних комп'ютерних мереж супроводжується зловживанням цими технологіями зі злочинною метою [14, с. 10]. Тому серед вагомих загроз кібербезпеці у Стратегії 2021 р. названа кіберзлочинність.

Дійсно, кіберпростір дедалі більше й більше стає поживним ґрунтом для вчинення, зокрема, злочинів проти основ національної безпеки України і громадської безпеки, громадського порядку та моральності, волі, честі та гідності особи, правопорушень, пов'язаних із незаконним обігом зброї, наркотичних засобів, легалізацією доходів, одержаних злочинним шляхом, тощо. Як бачимо, масштабність порушень кібербезпеки може бути різною – від завдання шкоди правам та інтересам окремої особи до завдання збитків великим суб'єктам господарювання, державним і громадським інституціям, нарешті, державі в цілому.

"Елементарним" прикладом порушення кібербезпеки може слугувати такий приклад із практики. Гр-н А., маючи практичні навички у сфері програмування та розуміючись на принципах інформаційної безпеки й кібербезпеки, отримав несанкціонований доступ до облікових акаунтів користувачів ігрової платформи "Steam" із метою контролю над цими акаунтами. У свою чергу, легітимні володільці акаунтів ігрової платформи "Steam" утрачали до них доступ. У подальшому А. за грошову винагороду передавав такі акаунти для користування третім особам, вчинивши своїми умисними діями кримінальне правопорушення, передбачене ч. 1 ст. 361 КК України, а саме: несанкціоноване втручання в роботу автоматизованих систем, комп'ютерних мереж, що призвело до втрати, підробки та блокування інформації [37].

Але ж трапляються й такі випадки, через які може бути спричинений колосальний збиток державі та суспільству. Наприклад, внаслідок кібератаки 14 січня 2022 р. втрачено низку зовнішніх інформаційних ресурсів моторного (транспортного) страхового бюро України. На щастя, реєстр, який містить персональні дані мільйонів українських автовласників, не ушкоджено. У цей самий день було здійснено хакерську атаку на урядові сайти, зокрема МЗС, МОН України тощо [38].

Отже, збільшення кількості кіберзлочинів, що перетворилися вже на одну з глобальних "галузей" злочинності, є наслідком процесів цифрової трансформації суспільства. Нескладні розрахунки з огляду на знання про розміри латентної частини кіберзлочинів (до 90 %) та кількість всіх інших зареєстрованих злочинів дозволяють стверджувати, що число злочинів у кіберпросторі дорівнюються масиву кримінально караних правопорушень, учинених у режимі "офлайн" (!) Тому з абсолютною впевненістю можна сказати, що кіберзлочини є найдинамічнішою групою суспільно небезпечних діянь, адже з кожним роком кіберзлочини стають дедалі більш масовими й небезпечними [39]. Навіть стверджується, що на вершині кіберзлочинності знаходяться хакери, спонсоровані державою [40]. За оцінками міжнародної дослідницької та консалтингової компанії "International Data Corporation" у 2025 р. обсяг незахищених даних, що потребують захисту, становитиме майже половину від усього існуючого обсягу даних, тоді як ця ж величина для 2015 р. складала лише чверть [41].

Повертаючись до розгляду положень, які є засадничими для охорони цифрових трансформацій українського суспільства, зазначимо, що до Стратегії кібербезпеки 2021 р. уже діяла Стратегія кібербезпеки України 2016 р. [42]. Важливість цього документа зумовлена реалізацією, зокрема, таких завдань, як становлення й розвиток національної системи кібербезпеки, а так само розробка й прийняття у 2017 р. Закону України "Про основні засади забезпечення кібербезпеки України", в якому визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і

громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [43]. Цінним є те, що у Законі наводиться визначення кіберзлочину, або комп'ютерного злочину, під яким розуміється суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [43]. До речі, у національному правовому полі цей термін згадувався й у Стратегії національної безпеки України 2015 р. [30].

Ще одним видом документів, що має засадничий характер для захисту цифрових трансформацій від різного роду загроз і небезпек у контексті забезпечення національної безпеки як такої, є доктрина. Першу Доктрину інформаційної безпеки в Україні було прийнято у 2009 р. [44]. У зазначеному документі, по-перше, наведено перелік важливих в інформаційній сфері інтересів особи, суспільства і держави, по-друге, створено своєрідний каталог реальних і потенційних загроз інформаційній безпеці України, а, по-третє, визначено напрями державної політики в аналізованій сфері. Вже на той час у документі наголошувалося на існуванні негативних інформаційних впливів, спрямованих на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України, а так само на використанні ЗМІ та мережі Інтернет з метою пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками [44]. Крім того, згадано й про комп'ютерну злочинність і комп'ютерний тероризм (у подальшому щодо позначення цих явищ стали використовуватися терміни "кіберзлочинність" і "кібертероризм"). Разом із тим завданням доктрини не ставилося наведення конкретного плану з реалізації напрямів убезпечення інформаційного простору.

З розвитком суспільних відносин відбувається періодичний перегляд концептуальних підходів до забезпечення національної безпеки [45, с. 10]. Наступною у плані відповідної рефлексії на змінювану реальність стала Доктрина інформаційної безпеки України 2017 р. Фактично цей документ приймався в нових соціально-політичних умовах, тому його мета – уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни [46].

Як правильно зазначається українськими аналітиками, якщо Стратегія інформаційної безпеки розглядає дії країни-агресора проти України в інформаційній сфері лише як одну із загроз, то чинна Доктрина обмежує перелік основних загроз лише здійсненням з боку країни-агресора спеціальних інформаційних операцій, спрямованих на підрив обороноздатності України, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні, проведення спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі тощо [47].

Таким чином, проаналізовані вище концептуально-стратегічні правові документи визначають коло суспільних відносин, що потребують неабиякої уваги з боку державних інституцій та у відповідних випадках захисту, зокрема, кримінально-правовими засобами.

Разом із тим, і стратегії, і доктрини покликані визначати основні засади й принципи, на яких повинні базуватися законодавчі та всі інші нормативно-правові акти органів влади. Важливішими законами у сфері інформаційної безпеки на сьогоднішній день є закони України "Про національну безпеку України", "Про основні засади забезпечення кібербезпеки України", "Про захист інформації в інформаційно-телекомунікаційних

системах", а так само Кримінальний кодекс України та Кодекс України про адміністративні правопорушення. Водночас неабияке значення для ефективного захисту цифрових трансформацій суспільства має і нещодавно прийнятий Закон України "Про критичну інфраструктуру" [48], в якому згадується про такі категорії, як "критична інфраструктура", "кібербезпека", "кіберзахист", "кібертероризм", "кіберпростір", "кібератаки" та "інформаційна безпека". Це дозволяє зробити висновок, що існування об'єктів критичної інфраструктури є неможливим без належного кіберзахисту інформаційної "оболонки" їх функціонування. При цьому питання їх кіберзахисту є настільки важливим, що в самому нормативно-правовому акті наголошується на тому, що відносини щодо забезпечення кіберзахисту та кібербезпеки об'єктів критичної інфраструктури регулюються окремим законом [48].

Так само важливими для захисту цифрових трансформації є положення Закону України "Про основні засади забезпечення кібербезпеки України", в яких розкривається зміст кібербезпеки та кіберзахисту. Так, під кібербезпекою розуміється захищеність життєво важливих інтересів людини й громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі [43]. Водночас кіберзахист представляє собою сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості й надійності функціонування комунікаційних, технологічних систем [43]. Разом із тим кіберзахист інформаційного простору у такому розумінні, як воно наводиться в аналізованому Законі, на наш погляд, є дещо вужчим за правовий захист цифрових трансформацій, оскільки не охоплює, умовно кажучи, стадію правової реакції у вигляді юридичної відповідальності осіб, які вчинили ці кіберінциденти і кібератаки. Тому стосовно подібних суспільно небезпечних діянь застосування юридичної відповідальності насамперед кримінальної, стає крайнім доводом (*ultima ratio*) в арсеналі законодавця.

Аналіз законодавства про адміністративні правопорушення дозволяє констатувати, що арсенал адміністративно-правових засобів протидії правопорушенням у сфері цифрових трансформацій на сьогодні є достатньо обмеженим (ст. 163-14 "Порушення порядку здійснення операцій з електронними грошима", ст. 163-15 "Порушення порядку проведення готівкових розрахунків та розрахунків з використанням електронних платіжних засобів за товари (послуги)" та деякі інші), адже весь "захисний упор" робиться на можливості кримінального права.

Будь-які цифрові трансформації суспільства завжди пов'язані із циркуляцією інформації, що є матрицею будь-яких інформаційних відносин. Як ми раніше писали, "особливістю нинішньої моделі захисту інформаційних відносин є те, що відповідні норми містяться у різних розділах Особливої частини законодавства про кримінальну відповідальність" [49, с. 112]. Однак, тут важливо нагадати, що йдеться не лише про кіберпростір як середовище, створюване інформаційними системами, об'єднаними в локальні або глобальні комп'ютерні мережі або реалізованими на окремих комп'ютерах та інших пристроях [50, с. 191], а й взагалі про обіг інформації, з використанням якої може пов'язуватися вчинення злочину. Тому, роблячи акцент на захисті цифрових трансформацій, ми повинні брати до уваги той сегмент інформаційних потоків, "життєдіяльність" яких зумовлюється саме кіберпростором. Так би мовити, традиційними прикладами порушення законодавства в інформаційному просторі є комп'ютерні злочини,

відповідальність за які встановлено у Розділі XVI Особливої частини КК України. Водночас цифрова трансформація суспільства може нести загрози правам та інтересам окремих громадян, які убезпечуються від кримінальних правопорушень нормами Розділу V ("Кримінальні правопорушення проти виборчих, трудових та інших особистих прав і свобод людини і громадянина") Особливої частини КК України. Йдеться, наприклад, про внесення неправдивих відомостей або будь-яке втручання у роботу баз даних державних реєстрів (ст. 158 КК України), порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 162 КК України), та ін. Із процесами цифрових трансформацій можуть бути пов'язані загрози громадській безпеці та основам національної безпеки, про що наголошувалося вище, господарській діяльності країни, моральності суспільства тощо. Навіть погроза вбивством та доведення до самогубства можуть здійснюватися шляхом використання досягнень інформаційно-комунікаційних технологій.

У цьому зв'язку не можна не зазначити, хоча б пунктиром, про деякі проблеми кримінально-правового захисту суспільних відносин, що породжені процесами цифрових трансформацій.

По-перше, серед основних причин, що потребують вдосконалення кримінального законодавства, можна виділити дві найпомітніші: зміни в об'єкті кримінально-правової охорони та зміни у способі посягання [51, с. 6]. Інформація, будучи одним із найпоширеніших предметів суспільних відносин, якими, власне, й опосередковується буття трансформаційних процесів та на які сьогодні посягають чимало злочинних діянь, й досі не отримала достатнього осмислення як певної ознаки складу злочину з позиції її природи. Причому йдеться не про будь-яку інформацію, а лише про ту її частину, що пов'язана із кіберпростором як таким (тобто ту, що генерується, змінюється, існує, руйнується, навіть підтримує функціональність цього простору тощо). У цьому разі говорять про кібернетичну, або комп'ютерну інформацію [52, с. 159-163]. Підвищення ефективності кримінально-правового захисту цифрових трансформацій потребує принаймні відходу у розумінні предмета злочину від його "матеріальності", котра традиційно пов'язується з належністю цієї категорії виключно до будь-яких матеріальних субстанцій. Уявляється, що зміна парадигми світу означає й зміни у розумінні, здавалося б, усталених категорій кримінально-правової науки.

Цікаве спостереження наводить С. Дарбінян. Так він пише: "Я впевнений, що величезна кількість реальних злочинів залишається за бортом. Наприклад, йдеться про ситуації, коли у користувача викрадають "танчик" (танк в онлайн-грі World of Tanks) ціною в кілька тисяч доларів або за допомогою вірусів викрадають особисті паролі від криптогаманців і викрадають потім Etherium або Bitcoin. Про такі злочини не заявляють, їх кількість ніхто не відслідковує, щодо них не порушуються кримінальні справи" [53].

По-друге, мають рацію ті дослідники, які зазначають, що у кримінальному законодавстві при значній кількості інформаційних об'єктів як предметів кримінально-правової охорони є відсутнім системний підхід до охорони суспільних відносин у даній сфері [54, с. 213]. Така ситуація призводить до застосування різних підходів до класифікації злочинів, що посягають на відповідні відносини. Однак зазначена проблема має не лише суто теоретичний, а й прагматичний характер, оскільки сьогодні від ставлення до градації правопорушень, що виявляються негативними наслідками процесу цифрових трансформацій суспільства, залежить "абрис" структури майбутнього законодавства про кримінальну відповідальність, над яким триває напружена робота. Тут лише зауважимо, що певне уявлення про класифікацію цих правопорушень дає Конвенція про кіберзлочинність 2001 р., підготовлена Радою Європи та ратифікована Україною у

2005 р. У зазначеному документі міститься інформація про чотири різновиди кримінальних правопорушень, а саме про: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання в дані та втручання в систему); 2) правопорушення, пов'язані з комп'ютерами (підробка та шахрайство, пов'язані з комп'ютерами); 3) правопорушення, пов'язані зі змістом (дитяча порнографія); 4) правопорушення, пов'язані з порушенням авторських та суміжних прав [55].

По-третє, вже зараз можна стверджувати, що у майбутньому зазнають змін способи реалізації положень деяких інститутів кримінального права. Так, наприклад, вже сьогодні викликає неабиякий інтерес відповідь за запитання: чи можна сплати, наприклад, штраф віртуальною валютою або чи можна конфіскувати в особи витвори цифрового мистецтва, NFT-токени, що використовуються кількома цифровими платформами для підтвердження факту володіння цифровими активами та права на їх використання та ін.?

По-четверте, у світлі цифрових трансформацій потрібно починати замислюватися з приводу діджиталізації процесу відправлення правосуддя, окремі елементи якої вже сьогодні впроваджені у нас у країні.

Що ж стосується міжнародних стандартів цифрових трансформацій суспільного життя, які відіграють неабияку роль у цьому процесі, то цей блок документів є достатньо об'ємним, тим самим заслуговуючи на окремий розгляд. Тут лише зазначимо, що міжнародні інституції опікуються ходом цифрових трансформацій у достатній мірі – приймають правові документи, готують аналітику, проводять науково-практичні форуми, надають грантову підтримку національним дослідницьким школам і громадським організаціям.

Висновки.

Новітня історія свідчить, що від моменту виникнення нових суспільних відносин до моменту, коли формується більш-менш одноманітна юридична практика їх захисту, проходить від п'яти до восьми років [54, с. 218]. Розвиток інформаційного суспільства є настільки стрімким, що інколи просто не вистачає часу, щоб адекватно зреагувати на виникнення все нових і нових загроз і ризиків. У такій ситуації система захисту має дещо хаотичний характер. Тому щоб завдати правильний вектор у діяльності із побудови цього захисту, виникає необхідність, по-перше, якомога скоріше оцінити наявні негативні прояви цифрових трансформацій, по-друге, негайно реагувати на виявлені ризики шляхом своєчасної розробки й прийняття ефективного законодавства, спрямованого на нейтралізацію останніх, по-третє, синхронізувати вітчизняні напрацювання у цій сфері з міжнародними стандартами, по-четверте, здійснити своєрідну ревізію застарілих доктринальних уявлень про ті чи інші категорії й інститути кримінального права.

Що стосується науки і галузі кримінального права, то тут принаймні необхідно розв'язати низку завдань, як-от: переосмислити теоретичні підходи до предмета злочину; взяти за основу класифікацію злочинів ту ідею, що відбиватиме логіку цифрових трансформацій та забезпечуватиме надійний захист цих процесів засобами кримінального права; переглянути шляхи реалізації деяких інститутів кримінального права, насамперед пов'язаних із кваліфікацією вчиненого та реалізацією кримінальних покарань.

Використана література

1. Multilateralism must weather 'challenges of today and tomorrow' Guterres tells Paris Peace Forum. UN News. *Global perspective Human storie.* 11 November 2019. Peace and Security. URL: https://news.un.org/en/story/2019/11/1051081

2. Нанотехнологии как ключевой фактор нового технологического уклада в экономике / под ред. С.Ю. Глазьева и В.В. Харитонова. Москва: Тровант, 2009. 304 с.

3. Alekseieva K., Novikova I., Bediukh O., Kostyuk O. Technological Orders' Change Caused by the Pandemics: Digitalization in the Internationalization of Technology Transfer. *Problems and Perspectives in Management.* 2021. Is.19 (3). P. 261-275.

4. Molinaro M., McLuhan C., Toye W. (eds.). *Letters of Marshall McLuhan.* Toronto, Oxford & New York: Oxford University Press, 1987. 562 p.

5. Добровольська А.Б. Інформаційний простір: проблеми становлення нової якості національного росту. *Наука України у світовому інформаційному просторі:* зб. наук. праць. Вип. 3. Київ: Академперіодика, 2010. С. 61-70.

6. Брижко В., Базанов Ю. та ін. е-майбутнє та інформаційне право. 2-ге вид., доп. Київ: НДЦПІ АПрН України. 2006. 305 с.; Пилипчук В.Г., Брижко В.М. Проблеми становлення і розвитку інформаційного законодавства в контексті євроінтеграції України. *Інформація та право.* № 1(1)/2011. С. 7-15; Брижко В.М. Основи систематизації інформаційного законодавства: теоретичні та правові засади: монографія. Київ: ТОВ "ПанТот", 2012 р. 304 с.

7. Гавловський В.Д., Бутузов В.М., Тітуніна К.В. Комп'ютерна злочинність: міжнародний досвід боротьби і перспективи для України. *Правова інформатика.* № 1(21)/2009. С. 72-77.

8. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право.* 2017. Вип. 5. С. 174-180.

9. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право.* № 1(24)/2018. С. 89-103.

10. Доронін І.М. Цифровий розвиток та національна безпека у контексті правових проблем. *Інформація і право.* № 1(28)/2019. С. 29-36.

11. Швець М., Калюжний Р., Гавловський В. та ін. Інформаційне законодавство України: концептуальні основи формування. *Право України.* 2001. № 7. С. 88-91.

12. Протидія злочинам у сфері використання комп'ютерних технологій інтегрований навч.-практ. посібник / за ред. М.В. Карчевського. Харків: Право, 2019. 188 с.

13. Карчевський М.В. Кримінально-правова охорона інформаційної безпеки України: монографія / МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. 528 с.

14. Когут Ю.І. Кібервійни, кіберзлочинність (концепції, стратегії, технології): практ. посібник. Київ: Консалтингова компанія "СІДКОН"; ВД "Дакор", 2022. 284 с.

15. Куйбіда В.С., Пасічник В.М. Засади державної політики національної безпеки України: монографія / за заг. ред. В.С. Куйбіди. Київ: НАДУ, 2020. 488 с.

16. Марущак А.І. Пріоритети розвитку інформаційного права України. *Інформація і право.* № 1(1)/2011. С. 20-24.

17. Радутний О.Е. Кримінальна відповідальність штучного інтелекту. *Інформація і право.* № 2(21)/2017. С. 124-132.

18. Фурашев В.М. Законодавче забезпечення інформаційної безпеки України. *Інформація і право.* № 1(10)/2014. С. 59-67.

19. Lessig L. The Path of Cyberlaw. *The Yale Law Journal.* 1995. T. 104. Is. 7. P. 1743-1755.

20. Mayer-Schunberger V. Generational Development of Data Protection in Europe. In: Agre P., Rotenberg M. (eds.). Technology and Privacy: the New Landscape. Cambridge: MIT Press, 1997. P. 219-242.

21. Nieles M., Dempsey K., Pillitteri V.-Y. An Introduction to Information Security. Gaithersburg: National Institute of Standards and Technology, 2017. 91 p.

22. Low K., Mik E. Pause the Blockchain Legal Revolution. *International and Comparative Law Quarterly.* 2020. Is. 69(1). P. 135-175.

23. Sidorenko E.L., von Arx P. Transformation of Law in the Context of Digitalization: Defining the Correct Priorities. *DigItal Law Journal.* 2020. Vol. 1. No 1. P. 24-38.

24. Valeev D.K., Nuriev A.G. Digitization of Law: Some Problematic Aspects. *Journal of Politics and Law*. 2019. Vol. 12. No. 5. Pp. 135-139.

25. Цифрової адженди України – 2020 ("Цифровий порядок денний" – 2020). URL: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf

26. Sieber U. Legal Aspects of Computer-Related Crime in the Information Society: Comcrime Study (1 January 1998). Würzburg: Julius-Maximilians-Universität Würzburg, 1998. P. 24-31.

27. "41 млн підозрілих подій та 147 кіберінцидентів": річний звіт ДЦКЗ. URL: https://cip.gov.ua/ua/news/321f4bf8

28. Стратегія національної безпеки України: Указ Президента України від 12.02.07 р. № 105/2007. *Офіц. вісник України.* 2007. № 11. Ст. 389.

29. Стратегія національної безпеки України "Україна у світі, що змінюється": в ред. Указу Президента України від 08.06.12 р. № 389/2012. URL: https://zakon.rada.gov.ua/laws/show/105/2007#Text

30. Стратегія національної безпеки України: Указ Президента України від 26.05.15 р. № 287/2015. URL: https://www.president.gov.ua/documents/2872015-19070

31. Стратегія національної безпеки України "Безпека людини – безпека країни": Указ Президента України від 14.09.20 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037

32. Ситник Г.П., Олуйко В.М., Вавринчук М.П. Національна безпека України: теорія і практика: монографія / за заг. ред. Г.П. Ситника. Київ: "Кондор", 2007. 669 с.

33. Стратегія розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15.05.13 р. № 386-р. *Офіц. вісник України.* 2013. № 44. Ст. 1581.

34. Стратегія здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року: Розпорядження Кабінету Міністрів України від 17.11.21 р. № 1467-р. URL: https://zakon.rada.gov.ua/laws/show/1467-2021-р#n15

35. Стратегія інформаційної безпеки: Указ Президента України від 28.12.21 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069

36. Стратегія кібербезпеки України "Безпечний кіберпростір – запорука успішного розвитку країни": Указ Президента України від 26.08.21 р. № 447/2021. URL: //www.president.gov.ua/documents/4472021-40013

37. Вирок Приморського районного суду м. Одеси від 20.02.20 р. (кримінальне провадження № 1-кп/522/798/20).

38. Інформація з баз даних МТСБУ не втрачена – реєстр відновить свою роботу найближчим часом. URL: https://cip.gov.ua/ua/news/informaciya-z-baz-danikh-mtsbu-ne-vtrachena-reyestr-vidnovit-svoyu-robotu-naiblizhchim-chasom

39. Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606

40. В 2021 году зафиксировано рекордное число атак с использованием 0Day-уязвимостей. URL: https://www.securitylab.ru/news/525058.php

41. Киберпреступность в цифрах. URL: https://www.aktiv-company.ru/analitics/articles/cybercryme.html

42. Стратегія кібербезпеки України: Указ Президента України від 15.03.16 р. № 96-2016. URL: https://www.president.gov.ua/documents/962016-19836

43. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.

44. Доктрина інформаційної безпеки України: Указ Президента України від 08.07.09 р. № 514/2009. *Офіц. вісник України*. 2009. № 52. Ст. 1783.

45. Резнікова О.О. Розробка стратегії національної безпеки з урахуванням принципів національної стійкості. *Стратегічна панорама*. 2018. № 2. С. 5-11.

46. Доктрина інформаційної безпеки України: Указ Президента України від 25.02.17 р. № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374

47. Сафаров А. Аналіз Стратегії інформаційної безпеки порівняно з чинною Доктриною інформаційної безпеки. URL: https://imi.org.ua/monitorings/analiz-strategiyi-informatsijnoyi-bezpeky-v-porivnyanni-z-chynnoyudoktrynoyu-informatsijnoyi-i38852

48. Про критичну інфраструктуру: Закон України від 16.11.21 р. № 1882-IX. *Офіц. вісник України*. 2021. № 98. Ст. 6341.

49. Батиргареєва В.С. Щодо концептуальної моделі захисту інформаційного простору України засобами кримінального права. *Інформація і право*. № 1(32)/2020. С. 110-119.

50. Попова Т.В., Ліпкан В.А. Стратегічні комунікації (словник) / за ред. В.А. Ліпкана. Київ: ФОП С. Ліпкан, 2016. 416 с.

51. Букалерова Л.А., Пикуров Н.И. Уголовно-правовая охрана оборона официальной информации. *Правовые вопросы связи*. 2005. № 1. С. 6-8.

52. Кузьмін С.А. Комп'ютерна (кібернетична) інформація, як предмет учинення злочину (кримінально-правовий аспект). *Інформація і право.* № 3(6)/2012. С. 159-163.

53. Киберпреступлений становится все больше, однако их раскрываемость уменьшается. URL: https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvae most-umenshaetsya

54. Елин В.М., Жарова А.В. О выделении информационных объектов в самостоятельную категорию объекта преступления. *Труды Института государства и права РАН*. 2009. № 5. С. 205-229.

55. Конвенція про кіберзлочинність від 2001 р.: ратифікована Законом України "Про ратифікацію Конвенції про кіберзлочинність" від 07.09.05 р. № 2824-IV *Відомості Верховної Ради України.* 2006. № 5-6. Ст. 71.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~