

УДК 351.75

DOI 10.33251/2707-8620-2021-5-185-194

**ТРОЯНСЬКИЙ Олександр Анатолійович**,  
кандидат юридичних наук, доцент,  
доцент кафедри права та правового  
регулювання авіаційної діяльності,  
Льотна академія  
Національного авіаційного університету  
ORCID 0000-0003-1420-9545

## ІНФОРМАЦІЙНА БЕЗПЕКА В УКРАЇНІ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

***Анотація.** У статті розглянуто проблемні питання інформаційної безпеки України на сучасному етапі її розвитку. Проаналізовано основні пріоритети державної політики з питань національної безпеки в інформаційній сфері, стан правового регулювання такої діяльності.*

*Розглянуто систему органів державної влади, які формують та реалізують державну інформаційну політику та покликані забезпечити інформаційну безпеку держави.*

*Визначено рівні забезпечення інформаційної безпеки та необхідність законодавчого закріплення таких понять, як інформаційна безпека держави, інформаційна безпека суспільства, інформаційна безпека організації (юридичної особи), інформаційна безпека людини.*

*Зазначено, що система інформаційної безпеки держави є складовою частиною системи національної безпеки країни і становить сукупність органів державної влади, місцевого самоврядування, недержавних структур і громадян, котрі повинні ефективно протистояти інформаційним загрозам за сучасних умов та узгоджено здійснювати діяльність по забезпеченню інформаційної безпеки на основі єдиних правових норм.*

***Ключові слова:** інформаційна безпека, інформаційна інфраструктура, державна інформаційна політика, загрози інформаційній безпеці, кібербезпека, національна безпека, стратегія національної безпеки.*

**Постановка проблеми.** Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни, її забезпечення в значній мірі сприяє успішному вирішенню завдань у безпековій, політичній, соціальній, економічній та інших сферах державної діяльності.

Проблема забезпечення інформаційної безпеки України багато в чому обумовлена неналежною координацією органів виконавчої влади при вирішенні завдань забезпечення інформаційної безпеки, а також пробілами в правовому регулюванні такої діяльності.

Відносини, пов'язані із забезпеченням інформаційної безпеки, як найважливіші сьогодні для суспільства та держави вимагають найшвидшого законодавчого врегулювання.

**Аналіз досліджень даної проблеми.** Проблематика інформаційної безпеки складна і багатоаспектна, що зумовлює необхідність вивчення й узагальнення наукових праць вчених-правників, фахівців з державного управління, безпекознавства, політичних, соціологічних та інших наук.

Окремі аспекти правового регулювання інформаційної сфери стали об'єктом наукового аналізу в працях вітчизняних дослідників, зокрема І. Арістової, І. Бачило, Р. Калюжного, Т. Костецької. Важливими для вивчення проблеми забезпечення інформаційної безпеки стали дослідження В. Гурковського, М. Гаврильців, М. Дмитренка, О. Золотар, Б. Кормича, В. Ліпкана, А. Марущак, В. Петрика, Г. Сашук.

**Метою даної статті** є дослідження основних напрямів державної інформаційної політики щодо забезпечення інформаційної безпеки держави на сучасному етапі розвитку, стан та перспективи її правового регулювання.

**Актуальність.** Швидкий розвиток інформаційних технологій, проникнення їх в усі сфери життя особистості, суспільства і держави привело до того, що в даний час усе більш актуального характеру викликають питання забезпечення інформаційної безпеки України як невід'ємного елемента національної безпеки, а захист громадян від негативного інформаційного впливу перетворюється в одне із пріоритетних державних завдань.

В умовах постійних світових конфліктів між державами, а також триваючого україно-російського протистояння, захист національного інформаційного простору від зовнішніх і внутрішніх інформаційних загроз, гарантування інформаційної безпеки та інформаційного суверенітету набувають особливого значення і стають чинниками функціонування України як суверенної та незалежної держави.

**Виклад основного матеріалу.** Сучасний стан забезпечення національної та інформаційної безпеки України потребує розробки науково обґрунтованої державної політики та стратегії в цій галузі, визначення системи національних цінностей, життєво важливих інтересів особистості, суспільства та держави, визначення зовнішніх і внутрішніх загроз цим інтересам, розвитку інформаційної інфраструктури, пошуку ефективних заходів для забезпечення безпеки в усіх її сферах життєдіяльності, налагодження ефективної взаємодії державних органів та належного законодавчого закріплення.

Головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку [1, с. 69].

Відповідно до ст. 3 Закону України «Про національну безпеку України» [2] державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо. Загрози національній безпеці України та відповідні пріоритети державної політики у сферах національної безпеки і оборони визначаються у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки і оборони, які схвалюються Радою національної безпеки і оборони України і затверджуються указами Президента України.

Необхідно зазначити, що даний законодавчий акт не визначає державної політики щодо інформаційної безпеки та не передбачає Стратегії інформаційної безпеки.

До прийняття вказаного вище закону, 25 лютого 2017 року Указом Президента України була затверджена Доктрина інформаційної безпеки України [3], яка визначила національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в цій сфері. Її метою є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни.

Пріоритети державної політики в інформаційній сфері закріплені у даному документі за наступними напрямками: забезпечення інформаційної безпеки; забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію; забезпечення відкритості та прозорості держави перед громадянами; формування позитивного міжнародного іміджу України.

Інформаційна безпека передбачає, перш за все, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Досягнення належного рівня національної безпеки сучасної держави неможливе без реалізації ефективної інформаційної політики [4].

Основні напрями державної політики з питань національної безпеки в інформаційній сфері також визначені у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [5], Стратегії національної безпеки України [6] та в інших нормативно-правових документах.

Відповідно до п. 13 Основних засад розвитку інформаційного суспільства в Україні на 2007-2015 роки [5] вирішення проблеми інформаційної безпеки має здійснюватися 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.

Інформаційна інфраструктура – комплекс програмно-технічних засобів, організаційних систем та нормативних баз, який забезпечує організацію взаємодії інформаційних потоків, функціонування та розвиток засобів інформаційної взаємодії та інформаційного простору країни або організації. Важливим фактором впливу на стан інформаційної інфраструктури країни є наявність відповідної конструктивної державної політики в цій галузі, яка має стимулювати її розвиток.

З метою розвитку інформаційної інфраструктури у вересні 2019 року було створено Міністерство цифрової трансформації України, яке є центральним органом виконавчої влади та забезпечує формування та реалізацію державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації; у сфері впровадження електронного документообігу; у сфері розвитку цифрових навичок та цифрових прав громадян; у сферах відкритих даних, розвитку національних електронних інформаційних ресурсів та інтероперабельності, розвитку інфраструктури ширококутвого доступу до Інтернету та телекомунікацій, електронної комерції та бізнесу; у сфері надання електронних та адміністративних послуг; у сферах електронних довірчих послуг та електронної ідентифікації; у сфері розвитку ІТ-індустрії [7].

Ефективно протистояти інформаційним загрозам у сучасних умовах може лише добре організована державна система забезпечення інформаційної безпеки, що повинна здійснюватися при повній взаємодії всіх державних органів, недержавних структур і громадян [8, с. 40].

На сьогодні в Україні триває процес становлення урядових і стратегічних систем комунікацій. У державі функціонує низка органів центральної виконавчої влади та відомств (Міноборони, МВС, Міністерство культури та інформаційної політики, Міністерство закордонних справ, Служба безпеки України, розвідувальні органи та ін.), які формують та реалізують державну інформаційну політику та вживають заходів щодо забезпечення інформаційної безпеки. Координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері відповідно до законодавства покладено на Раду національної безпеки і оборони України.

Кабінет Міністрів України забезпечує здійснення інформаційної політики держави, фінансування програм, пов'язаних з інформаційною безпекою, спрямовуватиме і координуватиме роботу міністерств, інших органів виконавчої влади у цій сфері.

При Раді національної безпеки і оборони України діє Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки як консультативно-дорадчий орган. До

основних її завдань, зокрема, належить аналіз стану і можливих загроз національній безпеці України в інформаційній сфері та узагальнення міжнародного досвіду щодо формування та реалізації інформаційної політики [9]/

У березні поточного року відповідно до Указу Президента України від 19 березня 2021 року № 106 [10] створено Центр протидії дезінформації, який є робочим органом Ради національної безпеки і оборони України та забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою [11]. 31 березня 2021 року відбулася презентація Центру стратегічних комунікацій та інформаційної безпеки (ЦСКІБ), створеного при Міністерстві культури та інформаційної політики, діяльність якого спрямована на об'єднання зусиль громадських організацій та влади у боротьбі із дезінформацією, швидке реагування на фейки, а також на промоцію українських нарративів [12].

Для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань діє Державна служба спеціального зв'язку та захисту інформації України [13].

У п. 66 Стратегії національної безпеки України [6] визначено, що вона є основою для розроблення п'ятнадцяти основних документів щодо планування у сферах національної безпеки і оборони, які визначатимуть шляхи та інструменти її реалізації, зокрема в інформаційній сфері – це Стратегія кібербезпеки України та Стратегія інформаційної безпеки.

Необхідно зазначити, що питання забезпечення кібербезпеки України є більше врегульованими у нормативно-правових актах України чим питання інформаційної безпеки. Так, 15 березня 2016 року Указом Президента України № 96 була затверджена Стратегія кібербезпеки України [14], 5 жовтня 2017 року був прийнятий Закон України «Про основні засади забезпечення кібербезпеки України» [15].

26 серпня 2021 року Указом Президента уведено в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» [16]. У новій Стратегії кібербезпеки зазначається, що діяльність суб'єктів національної системи кібербезпеки залишається недостатньо скоординованою і такою, що спрямована на виконання лише поточних завдань. За результатами експертних оцінок, стан реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96, за визначеними показниками не перевищує 40 відсотків. Невирішеними залишилися питання оперативного обміну інформацією про кіберзагрози, ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства. Недостатніми є організація і проведення наукових досліджень у сфері кібербезпеки.

Указом Президента України від 26 серпня 2021 року № 446/2021 введено в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави», яким Кабінету Міністрів України доручено невідкладно здійснити комплекс заходів з метою створення у системі Міністерства оборони України кібервійськ та набуття ними відповідних спроможностей [17].

15 вересня поточного року Кабінет Міністрів України ухвалив проект Стратегії інформаційної безпеки до 2025 року [18] (далі – Стратегія), але його ще має схвалити Рада національної безпеки і оборони України та увести в дію своїм Указом Президент України.

Дана Стратегія визначає засади забезпечення інформаційної безпеки України, протидії загрозам національній безпеці в інформаційній сфері, захисту прав осіб на інформацію та захист персональних даних.

Інформаційна безпека – це такий стан захищеності життєво важливих інтересів, а, отже, й інформаційної озброєності держави, суспільства, особистості, за якого ніякі інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів [19].

За об'єктною ознакою в теорії права виділяють такі види інформаційної безпеки: людини; юридичних осіб; суспільства; держави (національна інформаційна безпека); міжнародного співтовариства [2; 11] та запропоновані поняття даних термінів [19].

Віокремлюють наступні рівні забезпечення інформаційної безпеки:

– рівень особи (формування раціонального, критичного мислення на основі принципів свободи вибору);

– суспільний рівень (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, які належать вітчизняним власникам);

– державний рівень (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, система захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам) [21, с. 318].

Необхідно також виділити рівень організації (інформаційно-аналітичне забезпечення діяльності організації (юридичної особи), система захисту конфіденційної інформації, протидія зовнішнім загрозам).

Законодавче визначення інформаційної безпеки зафіксоване в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр.»: «інформаційна безпека – стан 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» [5].

У проекті Стратегії інформаційної безпеки поняття інформаційної безпеки викладене як стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій.

Проте, наведені визначення, на нашу думку, містять низку оціночних формулювань, які потребують уточнення і додаткового тлумачення.

Зокрема, потребує додаткового вивчення та чіткого визначення використані у даних поняттях терміни «негативний інформаційний вплив», «негативний інформаційно-психологічний вплив». Також необхідно пояснити, що розуміється під «негативними наслідками застосування інформаційних технологій». Крім того, є потреба в законодавчому закріпленні таких понять, як інформаційна безпека держави, інформаційна безпека суспільства, інформаційна безпека організації (юридичної особи), інформаційна безпека людини (фізичної особи).

Цілком логічним було б дати визначення даних термінів у базовому Законі України «Про інформацію» або Законі України «Про основні засади забезпечення кібербезпеки України». Адже відсутність однозначного розуміння вказаних формулювань може призвести до їх довільного тлумачення і таким чином створити умови для можливих зловживань під час застосування Стратегії на практиці, запровадження цензури та обмеження діяльності

ЗМІ, Інтернету, соціальних мереж та створити інші посягання на свободу слова, що вже викликає занепокоєння громадськості.

Правовий характер Стратегії, так само як і чинної Доктрини, не передбачає норм прямої дії – посилаючись на Стратегію не можна притягувати до кримінальної відповідальності, поширювати права державних органів. Для реальних правових наслідків мають бути прийняті спеціальні нормативні акти: нові закони, укази Президента, постанови КМУ, рішення інших органів влади. Як Доктрина, так і Стратегія – визначають основні засади і принципи, на яких мають базуватися ці закони та інші нормативно-правові акти.

Фіксуючи стан свободи слова в Україні через Барометр свободи слова, Інститут масової інформації відмічає, що основною проблемою в захисті суспільства від впливу шкідливої інформації є не стільки відсутність законодавчої бази, скільки невиконання чинного законодавства з боку посадових осіб органів влади, бездіяльність уповноважених органів, неналежне реагування або реагування в неправовий спосіб. Також проблемою є відсутність координації дій між різними органами влади, поставлення особистих амбіцій вище за загальну користь, непрофесійність і безвідповідальність посадових осіб при виконанні ними своїх обов'язків [22].

Важливість проблеми розвитку законодавства у сфері інформації та інформаційної безпеки, становлення інформаційного суспільства визначається тією обставиною, що норми законів цієї сфери суттєво впливають на законодавче регулювання відносин суб'єктів у всіх сферах життя держави [23].

**Висновки.** Враховуючи викладене вище, необхідно зазначити, що окремі питання інформаційної безпеки потребують подальшого законодавчого врегулювання. Крім того, керівництву держави потрібно вжити належних заходів щодо дотримання вимог чинного законодавства посадовими особами органів влади, виключення випадків бездіяльності уповноважених органів, їх належне реагування на виклики сьогодення у правовий спосіб, а також покращення координації дій між органами державної влади, місцевого самоврядування, недержавними структурами і громадянами з питань забезпечення інформаційної безпеки.

Перспективами подальших досліджень у цьому напрямі є розкриття основних понять та категорій для їх використання при розробці прикладних проблем інформаційної безпеки. Адже саме розмежування основних понять у цій сфері, їх уніфіковане застосування у процесі нормотворчої діяльності сприятиме однозначному розумінню основних завдань забезпечення інформаційної безпеки особи, юридичних осіб, суспільства, держави.

#### Список використаних джерел

1. Боднар І. Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. № 1. URL: <https://core.ac.uk/download/pdf/141443493.pdf> (дата звернення: 10.10.2021).
2. Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#n355> (дата звернення: 10.10.2021).
3. Доктрина інформаційної безпеки України: затв. Указом Президента України від 25 лютого 2017 р. № 47/2017. URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> (дата звернення: 10.10.2021).
4. Печенюк А. В. Інформаційна безпека України як складова національної безпеки. НДІ фіскальної політики: URL: <https://www.ndifp.com/1561/> (дата звернення: 12.10.2021).
5. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр. : Закон України від 09 січня 2007 р. № 537-V. URL: <https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=537-16#Text> (дата звернення: 10.10.2021).
6. Стратегія національної безпеки України: затв. Указом Президента України від 14 вересня 2020 р. № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#n7> (дата звернення: 10.10.2021).

7. Положення про Міністерство цифрової трансформації України: затв. постановою К-ту міністрів України від 18 вересня 2019 р. № 856 URL: <https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text> (дата звернення: 14.10.2021).
8. Дмитренко М. А. Проблемні питання інформаційної безпеки України. Міжнародні відносини. Серія Політичні науки. 2017. № 17. С. 236–243.
9. Положення про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України: затв. Указом Президента України від 22 січня 2002 р. № 63/2002 URL: <https://zakon.rada.gov.ua/laws/show/63/2002#Text> (дата звернення: 14.10.2021).
10. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: затв. Указом Президента України від 19 березня 2021 р. № 106/2021 URL: <https://zakon.rada.gov.ua/laws/show/106/2021#n5> (дата звернення: 14.10.2021).
11. Положення про Центр протидії дезінформації: затв. Указом Президента України від 7 травня 2021 р. № 187/2021 URL: <https://zakon.rada.gov.ua/laws/show/187/2021#Text> (дата звернення: 14.10.2021).
12. Презентовано Центр стратегічних комунікацій та інформаційної безпеки. Урядовий портал: веб-сайт. URL: <https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informatsijnoyi-bezpeki> (дата звернення: 14.10.2021).
13. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 р. № 3475-IV. URL: <https://zakon.rada.gov.ua/laws/show/3475-15#Text> (дата звернення: 14.10.2021).
14. Стратегія кібербезпеки України: затв. Указом Президента України від 15 березня 2016 р. № 96/2016. URL: <https://zakon.rada.gov.ua/laws/show/96/2016#n11> (дата звернення: 10.10.2021).
15. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 10.10.2021).
16. Стратегія кібербезпеки України: затв. Указом Президента України від 26 серпня 2021 р. № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n7> (дата звернення: 10.10.2021).
17. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави»: Указ Президента України від 26 серп. 2021 р. № 446/2021. URL: <https://zakon.rada.gov.ua/laws/show/446/2021#Text> (дата звернення: 14.10.2021).
18. Стратегія інформаційної безпеки: проект / Кабінет Міністрів України URL: <http://materialy.kmu.gov.ua/d08bb830/docs/cd2d9166/Dodatok.pdf> (дата звернення: 10.10.2021).
19. Сашук Г. Інформаційна безпека в системі забезпечення національної безпеки. Інтернет архів Waybackmachine. 2015.: веб-сайт. URL: [https://web.archive.org/web/20151110042232/http://journ.univ.kiev.ua/trk/publikacii/satshuk\\_public.php](https://web.archive.org/web/20151110042232/http://journ.univ.kiev.ua/trk/publikacii/satshuk_public.php) (дата звернення: 14.10.2021).
20. Золотар О. О. Класифікація інформаційної безпеки. Інформація і право. 2011. № 2. URL: [http://nbuv.gov.ua/UJRN/Infpr\\_2011\\_2\\_19](http://nbuv.gov.ua/UJRN/Infpr_2011_2_19) (дата звернення: 14.10.2021).
21. Кузьменко А. М. Особливості проблем законодавчого забезпечення інформаційної безпеки держави, суспільства і громадянина в умовах інформаційно-психологічного протидорства. Часопис Київського університету права. 2010. № 4. С. 317–321.
22. Сафаров А. Аналіз Стратегії інформаційної безпеки в порівнянні з чинною Доктриною інформаційної безпеки. Інститут масової інформації: веб-сайт. URL: <https://imi.org.ua/monitorings/analiz-strategiyi-informatsijnoyi-bezpeky-v-porivnyanni-z-chynnoyu-doktrynoyu-informatsijnoyi-i38852> (дата звернення: 10.10.2021).

23. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки. Юридичний науковий електронний журнал. 2020. №2. URL: <https://54.pdf> (lsej.org.ua). (дата звернення: 14.10.2021).

### References

1. Bodnar, I.R. (2014). *Informacijna bezpeka yak osnova nacionalnoyi bezpeky [Information security as a basis of national security]. Mexanizm regulyuvannya ekonomiky – The mechanism of regulation of the economy*, 1. Retrieved from: <https://core.ac.uk/download/pdf/141443493.pdf> [in Ukrainian].
2. Pro nacionalnu bezpeku Ukrayiny: Zakon Ukrayiny vid 21 cherv. 2018 r. № 2469-VIII [On National Security of Ukraine: Law of Ukraine of June 21, 2018 № 2469-VIII]. (n.d.). [zakon.rada.gov.ua](http://zakon.rada.gov.ua). Retrieved from: <https://zakon.rada.gov.ua/laws/show/2469-19#n355> [in Ukrainian].
3. Doktryna informacijnoyi bezpeky Ukrayiny: zatv. Ukazom Prezydenta Ukrayiny vid 25 lyut. 2017 r. № 47/2017 [Doctrine of information security of Ukraine: approved. By the Decree of the President of Ukraine of February 25, 2017 № 47/2017]. (n.d.). [zakon.rada.gov.ua](http://zakon.rada.gov.ua). Retrieved from: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> [in Ukrainian].
4. Pechenyuk, A.V. *Informacijna bezpeka Ukrayiny yak skladova nacionalnoyi bezpeky [Information security of Ukraine as a component of national security]*. NDI fiskalnoyi polityky` – Research Institute of Fiscal Policy : veb-sajt. (n.d.). Retrieved from: <https://www.ndifp.com/1561/> [in Ukrainian].
5. Pro Osnovni zasady rozvytku informacijnogo suspilstva v Ukrayini na 2007–2015 r.r. : Zakon Ukrayiny vid 09 sich. 2007 r. № 537-V [On the Basic Principles of Information Society Development in Ukraine for 2007–2015: Law of Ukraine of January 9, 2007 № 537-V]. (n.d.). [zakon.rada.gov.ua](http://zakon.rada.gov.ua). Retrieved from: <https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=537-16#Text> [in Ukrainian].
6. Strategiya nacionalnoyi bezpeky Ukrayiny: zatv. Ukazom Prezydenta Ukrayiny vid 14 ver. 2020 r. № 392/2020 [National Security Strategy of Ukraine: approved. By the Decree of the President of Ukraine of September 14, 2020 № 392/2020]. (n.d.). [zakon.rada.gov.ua](http://zakon.rada.gov.ua). Retrieved from: <https://zakon.rada.gov.ua/laws/show/392/2020#n7> [in Ukrainian].
7. Polozhennya pro Ministerstvo cyfrovoyi transformaciyi Ukrayiny: zatv. postanovoyu Kabinetu ministriv Ukrayiny vid 18 ver. 2019 r. № 856 [Regulations on the Ministry of Digital Transformation of Ukraine: approved. Resolution of the Cabinet of Ministers of Ukraine of September 18, 2019 № 856]. (n.d.). [zakon.rada.gov.ua](http://zakon.rada.gov.ua). Retrieved from: <https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text> [in Ukrainian].
8. Dmytrenko, M.A. (2017). *Problemni pytannya informacijnoyi bezpeky Ukrayiny [Problematic issues of information security of Ukraine]*. *Mizhnarodni vidnosyny – International relations*, 17, 236-243 [in Ukrainian].
9. Polozhennya pro Mizhvidomchu komisiyu z pytan informacijnoyi polityky ta informacijnoyi bezpeky pry Radi nacionalnoyi bezpeky i oborony Ukrayiny : zatv. Ukazom Prezydenta Ukrayiny vid 22 sich. 2002 r. № 63/2002 [Regulations on the Interdepartmental Commission on Information Policy and Information Security under the National Security and Defense Council of Ukraine: approved. By the Decree of the President of Ukraine of January 22, 2002 № 63/2002]. (n.d.). [zakon.rada.gov.ua](http://zakon.rada.gov.ua). Retrieved from: <https://zakon.rada.gov.ua/laws/show/63/2002#Text> [in Ukrainian].
10. Pro rishennya Rady nacionalnoyi bezpeky i oborony Ukrayiny vid 11 bereznya 2021 roku "Pro stvorennya Centru protydyi dezinformaciyi": zatv. Ukazom Prezydenta Ukrayiny vid 19 ber. 2021 r. № 106/2021 [On the decision of the National Security and Defense Council of Ukraine of March 11, 2021 "On the establishment of the Center for Countering Disinformation": approved. By the Decree of the President of Ukraine of March 19, 2021 № 106/2021]. (n.d.). [zakon.rada.gov.ua](http://zakon.rada.gov.ua). Retrieved from: <https://zakon.rada.gov.ua/laws/show/106/2021#n5> [in



Ukrainian].

11. Polozhennya pro Tsentr protydyi dezinformatsiyi : zatv. Ukazom Prezydenta Ukrayiny vid 7 trav. 2021 r. № 187/2021 [*Regulations on the Center for Counteracting Disinformation: approved. By the Decree of the President of Ukraine of May 7. 2021 № 187/2021*]. (n.d.). zakon.rada.gov.ua. Retrieved from: <https://zakon.rada.gov.ua/laws/show/187/2021#Text> [in Ukrainian].

12. Prezentovano Tsentr stratehichnykh komunikatsiy ta informatsiynoi bezpeky [*The Center for Strategic Communications and Information Security was presented*]. www.kmu.gov.ua. Retrieved from: <https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoi-bezpeki> [in Ukrainian].

13. Pro Derzhavnu sluzhbu spetsialnoho zv'yazku ta zakhystu informatsiyi Ukrayiny : Zakon Ukrayiny vid 23 lyut. 2006 r. № 3475-IV [*On the State Service for Special Communications and Information Protection of Ukraine: Law of Ukraine of 23 February. 2006 № 3475-IV*]. (n.d.). zakon.rada.gov.ua. Retrieved from: <https://zakon.rada.gov.ua/laws/show/3475-15#Text> [in Ukrainian].

14. Stratehiya kiberbezpeky Ukrayiny: zatv. Ukazom Prezydenta Ukrayiny vid 15 ber. 2016 r. № 96/2016 [*Cybersecurity strategy of Ukraine: approved. By the Decree of the President of Ukraine of March 15. 2016 № 96/2016*]. (n.d.). zakon.rada.gov.ua. Retrieved from: <https://zakon.rada.gov.ua/laws/show/96/2016#n11> [in Ukrainian].

15. Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny: Zakon Ukrayiny vid 5 zhovt. 2017 r. № 2163-VIII [*On the basic principles of cybersecurity in Ukraine: Law of Ukraine of October 5. 2017 № 2163-VIII*]. (n.d.). zakon.rada.gov.ua. Retrieved from: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> [in Ukrainian].

16. Stratehiya kiberbezpeky Ukrayiny: zatv. Ukazom Prezydenta Ukrayiny vid 26 serp. 2021 r. № 447/2021 [*Cybersecurity strategy of Ukraine: approved. By the Decree of the President of Ukraine of August 26. 2021 № 447/2021*]. (n.d.). zakon.rada.gov.ua. Retrieved from: <https://zakon.rada.gov.ua/laws/show/447/2021#n7> [in Ukrainian].

17. Pro rishennya Rady natsional'noyi bezpeky i oborony Ukrayiny vid 14 travnya 2021 roku "Pro nevidkladni zakhody z kiberoborony derzhavy": Ukaz Prezydenta Ukrayiny vid 26 serp. 2021 r. № 446/2021 [*On the decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On urgent measures for cyber defense of the state": Decree of the President of Ukraine of August 26. 2021 № 446/2021*]. (n.d.). zakon.rada.gov.ua. Retrieved from: <https://zakon.rada.gov.ua/laws/show/446/2021#Text> [in Ukrainian].

18. Stratehiya informatsiynoi bezpeky: proekt / Kabinet Ministriv Ukrayiny [*Information security strategy: project / Cabinet of Ministers of Ukraine*]. (n.d.). materialy.kmu.gov.ua. Retrieved from: <http://materialy.kmu.gov.ua/d08bb830/docs/cd2d9166/Dodatok.pdf> [in Ukrainian].

19. Sashchuk, H. (2015). Informatsiyna bezpeka v systemi zabezpechennya natsional'noyi bezpeky [*Information security in the system of national security*]. Internet arkhiv Waybackmachine – Waybackmachine online archive. Retrieved from: [https://web.archive.org/web/20151110042232/http://journ.univ.kiev.ua/trk/publikacii/satshuk\\_public.php](https://web.archive.org/web/20151110042232/http://journ.univ.kiev.ua/trk/publikacii/satshuk_public.php) [in Ukrainian].

20. Zolotar, O.O. (2011). Klasyfikatsiya informatsiynoi bezpeky [*Classification of information security*]. *Informatsiya i pravo – Information and law*, 2. Retrieved from: [http://nbuv.gov.ua/UJRN/Infpr\\_2011\\_2\\_19](http://nbuv.gov.ua/UJRN/Infpr_2011_2_19) [in Ukrainian].

21. Kuzmenko, A.M. (2010). Osoblyvosti problem zakonodavchoho zabezpechennya informatsiynoi bezpeky derzhavy, suspilstva i hromadyanyna v umovakh informatsiyno-psykholohichnoho protyborstva [*Features of problems of legislative maintenance of information security of the state, society and the citizen in the conditions of information and psychological confrontation*]. *Chasopys Kyivskoho universytetu prava – Journal of Kyiv University of Law*, 4, 317-321. [in Ukrainian].

22. Safarov, A. (2021). Analiz Stratehiyi informatsiynoi bezpeky v porivnyanni z

chynnoyu Doktrynoyu informatsiynoyi bezpeky [Analysis of the Information Security Strategy in comparison with the current Information Security Doctrine]. Instytut masovoyi informatsiyi – Institute of Mass Media. imi.org.ua. Retrieved from: <https://imi.org.ua/monitorings/analiz-strategiyi-informatsijnoyi-bezpeky-v-porivnyanni-z-chynnoyu-doktrynoyu-informatsijnoyi-i38852> [in Ukrainian].

23. Havryltsiv, M.T. (2020). Informatsiyna bezpeka derzhavy v systemi natsionalnoyi bezpeky [Information security of the state in the system of national security]. Yurydychnyy naukovyy elektronnyy zhurnal – Legal scientific electronic journal, 2. lsej.org.ua. Retrieved from: <https://54.pdf> (lsej.org.ua) [in Ukrainian].

**TROYANSKY Oleksandr**, Candidate of Law, Associate Professor, Associate Professor of Law and Legal Regulation, Flight Academy of the National Aviation University.

### INFORMATION SECURITY IN UKRAINE: PRESENT STATE AND DEVELOPMENT PROSPECTS

**Abstract.** *The article deals with the problematic issues of information security in Ukraine at the present stage of its development. The main priorities of government policy on issues of national security in the information sphere and the state of legal regulation of such activities are analyzed.*

*The system of public authorities that form and implement the government information policy and which are designed to ensure the information security of the state is considered.*

*The levels of ensuring information security and the need to legally consolidate such concepts as information security of the government, information security of society, information security of an organization (legal entity), and information security of a person were determined.*

*It is noted that the information security system of the government is an integral part of the national security system of the country. This system is a set of authorities, local government, non-state structures and citizens, which must effectively confront information threats in modern conditions and consistently carry out the activities to ensure information security based on common legal norms.*

**Key words:** *information security, information infrastructure, government information policy, threats to information security, cybersecurity, national security, national security strategy.*

*Одержано редакцією: 29.10.2021 р.  
Прийнято до публікації: 09.11.2021 р.*