

УДК 351.746.1

DOI <https://doi.org/10.32840/pdu.2021.2.19>

**І. В. Кукін**

кандидат наук з державного управління,  
докторант кафедри прикордонної безпеки  
Національної академії Державної прикордонної служби України  
імені Богдана Хмельницького

## **ДОСЛІДЖЕННЯ АКТУАЛЬНИХ ПРОБЛЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИСТОСТІ У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ЇЇ ПРИКОРДОННОМУ СЕКТОРІ**

*У статті розглянуто окремі питання та шляхи удосконалення правового регулювання щодо забезпечення інформаційної безпеки особистості у системі національної безпеки та її прикордонному секторі. Акцентовано увагу на зростанні за умов ведення інформаційних війн впливу інформаційної безпеки на стан національної безпеки та зумовлений ефектом синергії її зв'язок із реальним станом інформаційної безпеки особистості.*

*Зазначено, що інформаційна безпека характеризує стан захищеності особи, суспільства, держави, усуває можливе нанесення їм суттєвої шкоди від небезпечних інформаційних впливів і забезпечує їх сталий розвиток. Публічне управління щодо її забезпечення неможливе без зміцнення інформаційної безпеки особистості шляхом застосування державою механізмів публічного управління, які включають методи правового регулювання.*

*Наведено основні пріоритети інформаційної політики держави. Показано проблеми юридичної невизначеності критеріїв легітимності посадових осіб органів публічного управління, недостатнього розуміння населенням держави основних термінів і норм міжнародного гуманітарного права, що створює підґрунтя для маніпулювання інформацією за умов ведення проти України інформаційних війн.*

*Зазначено, що стан забезпечення інформаційної безпеки особистості досягається усуненням проблем інформаційної невизначеності в законодавчій базі, дотриманням персоналом органів публічного управління та іншими особами меж правової поведінки, розвитком правосвідомості у суспільстві. Наведено приклади недостатнього врахування у нормативно-правових актах України факторів соціальної справедливості й економічної доцільності.*

*З метою удосконалення публічного управління інформаційною безпекою особистості у сфері прикордонної безпеки та її прикордонному секторі запропоновано створення міжнародної та міждержавних систем забезпечення інформаційної безпеки особистості, розробку відповідної концепції, удосконалення заходів щодо доведення та роз'яснення населенню термінології та змісту норм міжнародного гуманітарного права. Також показана можливість використання об'єктів історичної та культурної спадщини для зміцнення стану інформаційної безпеки особистості, популяризації теорії та історії публічного управління.*

**Ключові слова:** інформаційна безпека, правове регулювання, інформаційна безпека особистості, національна безпека, прикордонна безпека.

**Постановка проблеми.** Людина є основним елементом соціальної системи. Без обміну інформацією будь-яка її діяльність у соціумі неможлива. Скоєння правопорушень, розвиток соціальних конфліктів певною мірою зумовлені помилково сприйнятою людьми інформацією.

Сучасні системи інформаційної безпеки правовими, економічними, політичними, силовими, технічними засобами створю-

ють над суспільством певний купол для захисту від зовнішніх шкідливих інформаційних впливів. Водночас українське суспільство продовжує відчувати негативний вплив інформаційної агресії з боку Російської Федерації. Інформаційні загрози національній і прикордонній безпеці залишаються актуальними. Це зумовлює необхідність удосконалення правового регулювання питань інформаційної

безпеки особистості, що зменшує загрози та ризики поширення шкідливої інформації в середині соціальної системи.

**Аналіз останніх досліджень і публікацій.** Питання забезпечення інформаційної безпеки держави наведені у роботах М.В. Банчука, А. Кречетнікова, А.В. Ландіної, Д.С. Мельника, О.А. Панченка, О.Б. Панченка, В.М. Петрика, М.М. Присяжнюка, Г. Рожкової, А.І. Семенченка, В.Ю. Степанова. Водночас недостатньо дослідженим залишається правове регулювання питань забезпечення інформаційної безпеки особистості у сфері національної безпеки та її прикордонному секторі.

**Мета статті** – на основі аналізу результатів досліджень механізмів правового регулювання забезпечення інформаційної безпеки особистості в системі національної безпеки та її прикордонному секторі виявити суперечності, недоліки та запропонувати шляхи їх усунення.

**Виклад основного матеріалу.** Інформаційна безпека характеризує стан захищеності особи, суспільства, держави, що усуває можливе нанесення їм суттєвої шкоди від небезпечних інформаційних впливів і забезпечує їх сталий розвиток. Зазначені об'єкти інформаційного впливу тісно зв'язані між собою [1, с. 8]. На думку О.Б. Панченка та М.В. Банчука, сфера інформаційного права забезпечує: розвиток понятійного апарату; визначення структури та змісту зазначеної галузі; встановлення властивостей інформаційних об'єктів; систематизацію джерел права; реалізацію інформаційних прав, свобод, обов'язків, правовий захист учасників соціальних комунікацій; прогнозування розвитку інформаційної сфери; проведення науково-дослідної діяльності; розвиток міжнародної співпраці [2, с. 133].

Основні принципи інформаційних відносин: гарантування прав на інформацію; відкритість, доступність, свобода обміну інформацією; об'єктивність, достовірність, повнота, точність інформації; забезпечення законності її обігу [2, с. 139]. Правова держава утворюється: укладанням публічно-правового союзу народу; легітимізацією суспільством правових норм; встановленням політичної відповідальності держави перед народом; забезпечен-

ням верховенства права; поділом влади; створенням системи противаг; юридичною формою діяльності органів державної влади [3, с. 102].

Механізм публічного управління створюється системою взаємодіючих нормативно визначених органів, організацій, які наділені повноваженнями для реалізації суспільно корисних завдань у відповідних сферах діяльності [3, с. 67].

У США завдання забезпечення інформаційної безпеки розподілені між державними органами, котрі забезпечують захист комп'ютерів та інформаційних систем, здійснюють інформаційні операції, ведуть інформаційні війни, досліджують спектри електромагнітних випромінювань, розробляють стандарти та технології, проводять науково-дослідні роботи [1, с. 47].

Функції Офісу зв'язку Великої Британії визначаються виключно законодавчими актами. Законодавством острова Мен і Нормандських островів йому також делеговано низку повноважень. Це сприяє єдності й узгодженості інформаційної політики регіону та створенню більш ефективною системи колективної безпеки. До сфери повноважень Офісу зв'язку як регулятора використання електронних мереж також належать питання: мовлення; телевізійних і радіопослуг; друкованих засобів масової інформації; кримінального провадження [4].

Принциповою відмінністю розроблених у Великій Британії «Норм управління інформаційною безпекою» є врахування потреб малих і середніх фірм, які раніше не приймалися проблемами захисту інформації. Це свідчить про наявність проблем щодо усвідомлення суспільством важливості підтримання необхідного стану інформаційної безпеки [1, с. 74].

У Франції пріоритетами забезпечення інформаційної безпеки визначені: військова та громадська діяльність; юриспруденція; оборонна промисловість; якість продуктів харчування та водопостачання; охорона здоров'я; енергетика; фінансовий сектор; транспорт; соціальні комунікації; мовлення; промисловість; використання космічного простору; наукова діяльність. Правове регулювання щодо використання Інтернет-мереж включає: свободу

комунікацій і вільного доступу до інформаційних ресурсів; регламентацію обов'язків постачальників послуг і правового статусу доменів; захист інтелектуальної власності; запобігання розповсюдженню шкідливого контенту; захист персональних даних [1, с. 118].

Регуляторна політика аудіовізуальних комунікацій спрямовується на: повагу до людської гідності; попередження дискримінації; запобігання шкідливої поведінки; усунення загроз вчинення фізичної, психічної, моральної шкоди особам, які не досягли 18 років; протидію використанню неповнолітніх для переконання батьків або інших осіб купувати або орендувати товари чи послуги, використанню довіри неповнолітніх до батьків, вчителів чи інших осіб або безпідставному залишенню їх у небезпечних ситуаціях [5].

Пріоритети інформаційної політики країн Європейського Союзу: забезпечення прозорості; удосконалення знань, вмінь і навичок населення держави; розширення інструментів обробки інформації; дотримання принципів плюралізму думок; проведення наукових досліджень [6]. Точність і неупередженість інформації забезпечують: об'єктивність фактів; сприяння обміну думками; дотримання принципів журналістики й етики; відокремлення думок від новин; обов'язкове зазначення автора інформації; запобігання спробам навмисної омани аудиторії [7].

Національні інтереси Російської Федерації з питань інформаційної безпеки включають: дотримання конституційних прав осіб; духовне оновлення населення; збереження культурних цінностей і традицій; інформаційне забезпечення політики; вільний доступ громадян до відкритої інформації; розвиток технологій; підтримку внутрішнього ринку; підвищення ефективності використання інформації; захист інформації; забезпечення безпеки інформаційних систем [1, с. 202].

За своєю сукупністю законодавство Російської Федерації щодо забезпечення інформаційної безпеки відповідає концепціям побудови демократичної держави. Водночас реальний стан її економіки обмежує розробку та виробництво нових видів зброї, якими можна ефективно про-

тидіяти збройним силам країн-членів НАТО. Це примушує тоталітарну владу Росії обирати технології ведення інформаційних війн як основний спосіб досягнення геополітичних цілей.

Питання забезпечення інформаційної безпеки включені до окремих норм міжнародного права. Так, Конвенцією про захист прав людини й основоположних свобод в інформаційній сфері гарантується свобода думки, совісті та релігії, вираження поглядів, одержання і передача інформації, ідей, без втручання органів державної влади і незалежно від кордонів. Водночас держава може встановлювати законами певні формальності, умови, обмеження або санкції в інтересах забезпечення національної або громадської безпеки, територіальної цілісності, запобігання злочинам, охорони здоров'я, моралі, репутації осіб, запобігання незаконному розголошенню інформації та підтримання авторитету суду [8].

Погоджуємося з думкою А.І. Семенченко, що в Україні елементи забезпечення інформаційної безпеки інтегровані у державні механізми: управління інформатизацією та цільовими програмами; розвитку інформаційного суспільства; електронного врядування; впровадження програм економічних реформ; відкритого уряду; міжнародного співробітництва [9, с. 15]. Також із початком російської агресії відбулася активізація механізму двобічного симетричного діалогу із громадянським суспільством. В Україні з'явилися некомерційні організації, місія яких полягає у виявленні та компрометації шкідливої для суспільства інформації.

У нормативно-правовому забезпеченні інформаційної безпеки України О.А. Панченко виділяє такі об'єкти захисту від шкідливої та неякісної інформації: інформаційні права і свободи осіб; інформаційні ресурси, суспільство. Стан безпеки визначається стійкістю сфер життєдіяльності до впливу деструктивної інформації, ризиком прийняття помилкових рішень. Негативно впливають на зменшення інформаційної вразливості населення України: безсистемний розвиток відповідних норм права; низький рівень правової та інформаційної культури; стан економіки

та розвитку інформаційних технологій; недосконалість системи відбору та підготовки кадрів [10, с. 58].

На підставі аналізу Конституції України, Законів України, Постанови Верховної Ради України, указів Президента України В.Ю. Степанов дійшов висновку про те, що інформаційна безпека поступово стає одним із основних компонентів національної безпеки. Інтереси суб'єктів інформаційних комунікацій пов'язані із забезпеченням доступності, цілісності та конфіденційності інформації [11]. Розглядаючи інформаційну безпеку об'єктом злочинного посягання, А.В. Ландіна пропонує додати її до основних сфер суспільних відносин, котрі охороняються Кримінальним Кодексом України [12, с. 359].

Погоджуємося з думкою О.В. Федорчака, що організаційний механізм публічного управління має відповідати інтересам суспільства та мати зворотній зв'язок із ним. Це дозволяє забезпечувати прозорість інформації, плюралізм думок і створювати необхідні соціуму інформаційні ресурси й інструменти [13]. Водночас у сфері національної безпеки та її прикордонному секторі органам державної влади під час прийняття управлінських рішень потребується пошук компромісів для узгодження законних інтересів людини, суспільства, держави та міжнародної спільноти.

Із затвердженням Інструкції про порядок виконання норм міжнародного гуманітарного права у Збройних Силах України посилено відповідальність військовослужбовців за їх порушення [14], однак зазначений документ не стосується персоналу правоохоронних органів та інших збройних формувань. Основні ключові терміни, такі як «анексія», «геноцид», «комбатанти», «не комбатанти», «окупація», «партизани», «військовослужбовець», «найманці» та ін. надаються без явного посилання на норми міжнародного гуманітарного права. Низка важливих термінів взагалі не визначена, зокрема «ополчення», «колаборанти» тощо. Це знижує ефективність: проведення інформаційних заходів; поширення норм міжнародного права; збір доказів для правового захисту військовослужбовців і цивільного населення у міжнародних судах.

Погоджуємося з думкою А. Кречетникова, що між Росією та Україною відбувається війна термінів, дійсний смисл яких населення не уявляє [15]. В українській версії Вікіпедії термін «ополчення» визначається як допоміжне військо з добровольців [16]. Це не дає уявлення про його зв'язок зі збройними силами держави. Історичний екскурс розвитку цього поняття обмежений періодом IX–XVI ст.

Це потребує поширення в суспільстві норм міжнародного права з питань ведення війни, прав і обов'язків армій, ополчення, добровольчих загонів. Для перешкодження інформаційним впливам Росії щодо статусу Криму й окремих регіонів Луганської та Донецької областей потребується роз'яснення населенню IV Конвенції про закони і звичаї війни на суходолі, де наведений термін «окупована територія» (частина території держави, де встановлена і здатна функціонувати влада супротивника) [17].

Соціальна система включає соціальну, економічну, політичну, духовно-культурну складові частини, функціонування та взаємодія яких забезпечуються інформаційною підсистемою [3, с. 111]. Це вимагає розгляду інформаційної безпеки особистості як комплексного явища, ключовими елементами якого є: межі правової поведінки; склад правопорушення; соціальна справедливість; економічна доцільність. Вони не завжди достатньо враховуються законодавцем. Так, у Законі «Про громадянство України» передбачено єдине громадянство та право його зміни [18], однак не передбачена відповідальність за невиконання зобов'язання припинити іноземне громадянство. Це ускладнює розгляд суб'єктивної сторони правопорушення.

У встановленому порядку перетину державного кордону України осіб із дітьми порушений принцип соціальної справедливості. Так, без нотаріально посвідченої згоди другого з батьків право тимчасового виїзду з України на строк до одного місяця має той із них, хто має документ, що підтверджує проживання дитини разом із ним [19]. Батьки, які не розлучені та живуть у шлюбі, зобов'язані оформляти такі документи у нотаріуса.

Через супротив політичної еліти недостатньо уваги приділяється законодавчому

визначенню меж легітимності посадових осіб органів державної влади та місцевого самоврядування. Це сприяє маніпуляції інформацією, породжує соціальні конфлікти та безвідповідальність посадових осіб органів державної влади та місцевого самоврядування. Водночас у стародавніх суспільствах цьому питанню приділялося більше уваги.

Так, у 1951 р. Національним музеєм мистецтв імені Богдана та Варвари Ханенків (м. Київ) була придбана «Статуя жерця на ім'я Еснебентер» [20]. Переданий скульптором сюжет доносить до глядача панівну у стародавньому Єгипті теологічну концепцію походження влади. Це можна пояснити тим, що на ній зображено дві фігури. Одна з них меншого розміру з характерними для того часу атрибутами влади фараона (скіпетром, цепом, накладною бородою). Друга фігура, що зображена стоячою на колінах, тримає фараона за плечі. На її верхній частині обох рук у картушах написано ім'я Бога – Імен (більш відомого як Амона, для дешифровки частини написів використані рекомендації Йоганна Фрідріха [21, с. 19]). Сукупність елементів скульптури можна інтерпретувати як вибачення Бога за спричинений кризою легітимності влади соціальний конфлікт і призначення свого посередника для оперативного вирішення нагальних питань соціального життя.

Історико-культурні об'єкти є невід'ємною частиною джерел формування історичної пам'яті, національної самобутності та популяризації історії розвитку публічного управління. Експозиції музеїв, особливо ті, що знаходяться під відкритим небом, доцільно показувати з елементами їх інтеграції у територіальне і соціальне середовище, що привертає увагу відвідувачів до причин позитивних і негативних результатів публічного управління, розвитку технологій, поступового удосконалення норм права.

**Висновки і пропозиції.** Отже, у системі національної безпеки та її прикордонному секторі зростає важливість стану забезпечення інформаційної безпеки. За умов ведення проти України інформаційних війн стає необхідним створення міжнародної та міждержавних систем забезпечення інформаційної безпеки осо-

бистості, доведення та роз'яснення населенню термінології та змісту норм міжнародного гуманітарного права.

Оскільки інформація є невід'ємною частиною діяльності людини, то стан інформаційної безпеки особистості впливає на якість прийнятих нею рішень і результати праці. Через ефект синергії інформаційна безпека особистості істотно впливає на властивості системи забезпечення інформаційної безпеки держави. Стан забезпечення інформаційної безпеки особистості залежить від розуміння населенням і персоналом органів публічного управління меж правової поведінки, складу правопорушення, критеріїв соціальної справедливості й економічної доцільності.

Для розвитку системи правового регулювання потребується зменшення інформаційної невизначеності в окремих нормах права, встановлення разом із обов'язками та заборонами юридичної відповідальності за їх порушення. Заборони й обмеження щодо розповсюдження інформації мають бути чітко визначені законами, відповідати конституції та нормам міжнародного права, а також виключати можливість подвійного їх тлумачення. Нагальним питанням залишається нормативне визначення критеріїв легітимності посадових осіб органів державної влади та місцевого самоврядування.

В українському суспільстві недостатньо уваги приділяється використанню об'єктів історичної та культурної спадщини для зменшення загроз інформаційної безпеки особистості, популяризації теорії та історії публічного управління. Це потребує удосконалення концепцій розвитку музейної справи, організації відповідних тематичних виставок, екскурсій. Забезпечення інформаційної безпеки особистості у сфері національної безпеки та її прикордонному секторі потребує використання органами публічного управління комплексного підходу та проведення міждисциплінарних наукових досліджень. Вона досягається застосуванням державою механізмів публічного управління та використанням методів правового регулювання.

Напрямом подальших досліджень може бути визначення структури та змісту концепції забезпечення інформаційної безпеки особистості.

**Список використаної літератури:**

1. Петрик В.М., Присяжнюк М.М., Мельник Д.С. та ін. Забезпечення інформаційної безпеки держави : підручник / за заг. ред. О.А. Семенченка, В.М. Петрика. Київ : ДНУ «Книжкова палата України», 2015. 672 с.
2. Панченко О.Б., Банчук Н.В. Информационная безопасность личности. Киев : КИТ, 2011. 672 с.
3. Загальна теорія держави і права (основні поняття, категорії, прав. Конструкції та наук. концепції) : навчальний посібник / за ред. О.В. Захарчука, Н.М. Оніщенко. Київ : Юрінком Інтер, 2016. 400 с.
4. Communicated act 2003. United Kingdom Low from 17.07.2003. URL: <https://www.legislation.gov.uk/ukpga/2003/21/introduction/enacted>.
5. The Audiovisual Media Services Regulations 2020. The United Kingdom Statutory instruments from 30.09.2020 № 1062. URL: <https://www.legislation.gov.uk/uksi/2020/1062/made>.
6. Рожкова Г. Як Латвія вирішила законодавчо боротися із пропагандою на телебаченні. URL: <https://www.stopfake.org/uk/yak-latviya-vyrishyla-zakonodavchoborotyua-iz-propagandyu-na-telebachenni/>.
7. Рожкова Г. Інструменти ЄС у боротьбі з дезінформацією. Ч. 2. URL: <https://www.stopfake.org/uk/instrumentyues-u-borotbi-z-dezinformatsiyeyu/>.
8. Конвенція про захист прав людини і основоположних свобод. Ратифікована Законом України від 17 липня 1997 р. № 475/97-ВР. URL: [https://zakon.rada.gov.ua/laws/show/995\\_004#Text](https://zakon.rada.gov.ua/laws/show/995_004#Text).
9. Семенченко А.І. Організаційно-правові механізми державного управління розвитком електронного врядування в Україні в контексті інформаційної безпеки та інтеграції в ЄС. *Наука і оборона*. 2013. № 3. С. 14–20. URL: [http://nbuv.gov.ua/UJRN/nauio\\_2013\\_3\\_4](http://nbuv.gov.ua/UJRN/nauio_2013_3_4).
10. Панченко О.А. Інформаційна безпека в контексті викликів і загроз національній безпеці. *Державне управління та місцеве самоврядування*. 2020. Вип. 2. С. 57–63. URL: [http://nbuv.gov.ua/UJRN/dums\\_2020\\_2\\_8](http://nbuv.gov.ua/UJRN/dums_2020_2_8).
11. Степанов В.Ю. Інформаційна безпека як складова державної інформаційної політики. *Державне будівництво*. 2016. № 2. URL: [http://nbuv.gov.ua/UJRN/DeVu\\_2016\\_2\\_4](http://nbuv.gov.ua/UJRN/DeVu_2016_2_4).
12. Ландіна А.В. Інформаційна безпека як об'єкт злочину. *Правова держава*. 2016. Вип. 27. С. 354–361. URL: [http://nbuv.gov.ua/UJRN/PrDe\\_2016\\_27\\_46](http://nbuv.gov.ua/UJRN/PrDe_2016_27_46).
13. Федорчак О.В. Класифікація механізмів державного управління. *Науковий вісник*. 2008. Вип. 1. URL: [http://lvivacademy.com/vidavnitstvo\\_1/visnik/fail/O\\_Fedorchak.pdf](http://lvivacademy.com/vidavnitstvo_1/visnik/fail/O_Fedorchak.pdf).
14. Про затвердження Інструкції про порядок виконання норм міжнародного гуманітарного права у Збройних Силах України. Наказ Міністерства оборони України від 23 березня 2017 р. № 164. URL: <https://zakon.rada.gov.ua/laws/show/z0704-17#Text>.
15. Кречетніков А. «Ополченці» та «терористи»: війна слів триває. *BBCNews Україна*. 2014. URL: [https://www.bbc.com/ukrainian/politics/2014/07/140714\\_propaganda\\_war\\_zsh](https://www.bbc.com/ukrainian/politics/2014/07/140714_propaganda_war_zsh).
16. Ополчення. *Вікіпедія*. URL: <https://uk.wikipedia.org/wiki/Ополчення>.
17. IV Конвенція про закони і звичаї війни на суходолі та додаток до неї: Положення про закони і звичаї війни на суходолі. Міжнародна Конвенція, Дата підписання: 18 жовтня 1907 р. Набрала чинності для України 24 серпня 1991 р. URL: [https://zakon.rada.gov.ua/laws/show/995\\_222#n2](https://zakon.rada.gov.ua/laws/show/995_222#n2).
18. Про громадянство України : Закон України від 18 січня 2001 р. № 2235-III. URL: <https://zakon.rada.gov.ua/laws/show/2235-14#Text>.
19. Про затвердження правил перетинання державного кордону громадянами України : Постанова Кабінету Міністрів України від 27 січня 1995 р. № 57. URL: <https://zakon.rada.gov.ua/laws/show/57-95-%D0%BF#Text>.
20. Статуя жерця на ім'я Еснебентер. *Національний музей мистецтв імені Богдана та Варвари Ханенків (м. Київ)*. Інв. 354 АТК.
21. Фридрих И. Дешифровка забытых письменностей и языков / пер. с нем. И.М. Дунаевская ; за ред. И.М. Дьяконова. Москва : Едиториал УРСС, 2003. 207 с.

**Kukin I. The individual information security actual problems research in the national security system and its border sector**

*The article considers some issues and ways to improve the legal regulation to ensure the individual information security in the national security system and its border sector.*

*Emphasis is placed on the information warfare technologies development growth of information security impact on the national security level and due to the synergy effect of its connection with the real individual information security level.*

*It is noted that information security characterizes the protection level of the individual, society and state, which eliminates the possible harm to them from dangerous information influences and ensures their sustainable development. Public administration to ensure it is impossible without strengthening the individual information security through the use public administration state mechanisms, which include legal regulation methods.*

*The main priorities of the state information policy are given. Legal uncertainty problems of public administration bodies officials legitimacy criteria, insufficient understanding the international humanitarian law basic terms and norms of the state population that creates a basis for the information manipulation in the conditions of conducting information wars against Ukraine are shown.*

*It is noted that the individual information security level is achieved by eliminating the problems of information uncertainty in the legal framework, compliance with the public administration staff and other persons the limits of legal behavior, the development of legal awareness in society. Examples of insufficient consideration of the social justice factors and economic expediency in the normative legal acts of Ukraine are given.*

*In order to improve the public management of the individual information security in the field of border security and its border sector, it is proposed to create international and interstate systems of personal information security, develop a concept, improve measures to prove and explain to the public the terminology and international humanitarian law content. It also shows the possibility of using historical and cultural heritage objects to strengthen the individual information security, to promote the theory and history of public administration.*

**Key words:** *information security, legal regulation, individual information security, national security, border security.*