

## КРИМІНАЛЬНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ІНФОРМАЦІЙНИХ ВІДНОСИН У ПРИКОРДОННІЙ СФЕРІ

*І. П. Кушнір*, кандидат юридичних наук, старший викладач кафедри теорії та історії держави і права та приватноправових дисциплін Національної академії Державної прикордонної служби України імені Богдана Хмельницького

**Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими та практичними завданнями.** Невід'ємною складовою розвитку сучасного суспільства є прогресивне зростання ролі інформаційних відносин. Кожного дня, як і в діяльності будь-якого іншого органу влади, персонал Державної прикордонної служби України (далі – ДПСУ) здійснює інформаційну діяльність щодо одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації: прав людини щодо вільного перетинання державного кордону [1]; прав громадян щодо вільного доступу до державної служби [1] та забезпечення виконання завдань, що покладаються державою на прикордонне відомство [2]. Сьогодні інформація, а точніше право на інформацію, є об'єктом державно-правової охорони, як й інші життєво важливі права людини. Право на інформацію охороняється законом. Держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до інформації [3]. Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України [3].

З появою нових видів загроз у сфері безпеки державного кордону виникла нагальна потреба в розвитку та посиленні захисту інформаційної складової, що передбачено Стратегією розвитку ДПСУ

[4]. Утілюючи це положення, прикордонним відомством серед Основних напрямів діяльності та подальшого розвитку ДПСУ у 2018 р. заплановано здійснення конкретних кроків щодо: розвитку інформаційної взаємодії, інформаційно-аналітичного забезпечення [5, п. 6]; посилення протидії інформаційним загрозам [5, п. 22.2]; забезпечення якісного моніторингу щодо дотримання законодавства з питань звернень громадян та їх запитів на отримання публічної інформації [5, п. 23.1]; забезпечення розв'язання соціальних питань, з якими звертаються громадяни, які потребують соціального захисту та підтримки [5, п. 23.2], тощо. Розвиток інформаційної складової залежить не лише від нормативного закріплення, а й від правильного та чіткого втілення норм законодавства і вимог керівництва ДПСУ в повсякденній практичній діяльності посадовими особами відомства. Гарантією правового забезпечення охорони прав, свобод людини і громадянина, громадської безпеки, безпеки людства, а також запобігання злочинам [6, ст. 1] є норми Кримінального кодексу України (далі – КК).

У чинному КК сьогодні відсутнє систематизоване закріплення статей зі складом злочинів, за які передбачена кримінальна відповідальність у разі порушення інформаційних прав, та ще й вони не завжди прямо це визначають. У КК злочини в інформаційній сфері регулюють понад 50 статей, що містяться в різних розділах [7, с. 57]. Із цього приводу 9 грудня 2011 р. до Верховної Ради України (далі – ВР) було внесено проект Закону України «Про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки» (законопроект № 9575), який до сьогодні залишається на опрацюванні в комітеті ВР [8]. У наведеному законопроекті запропоновано внести зміни до КК із метою вдосконалення системи юридичної відповідальності за правопорушення у сфері інформаційної безпеки та викласти назву розділу XVI КК у такій редакції: «Злочини у сфері інформаційної безпеки». У цьому розділі пропонується сформулювати склади злочинів у сфері інформаційної безпеки, що відповідатимуть умовам позитивного розвитку українського суспільства, його включення до світових процесів інформатизації [9].

**Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання цієї проблеми.** Державно-правове визнання інформаційних відносин, як і відповідальність за посягання на них, має недовготривалий період, але разом із цим питання відповідальності та охорони в межах інформаційної сфери вже здобули науковий інтерес. Переважно питання кримінально-правової охорони ставилися в загальному огляді відповідальності в інформаційній сфері (Л. П. Коваленко, О. М. Селезньова, Г. М. Писаренко, Т. А. Костецька, Ю. Є. Максименко та ін.). Охорона інформаційних відносин із позиції кримінального законодавства досліджувалась: М. В. Карчевським (кримінально-правова охорона інформаційної безпеки), Н. А. Савіною (кримінально-правове забезпечення розвитку інформаційного суспільства), О. К. Тугаровою (кримінально-правове забезпечення охорони інформаційних відносин) та ін.

**Окреслення не виділених раніше частин загальної проблеми, котрим присвячується означена стаття.** Аналіз цих праць свідчить про те, що в основному в них досліджені загальні питання правової та кримінальної відповідальності всіх інформаційних відносин. Питання охорони інформаційних відносин у сфері діяльності ДПСУ в кримінально-правовому контексті окремо не досліджувались. Це зумовлює актуальність та наукову новизну піднятого автором питання.

**Метою** статті є дослідження окремих аспектів кримінально-правової охорони інформаційних відносин у прикордонній сфері. Для вирішення цієї мети необхідно, по-перше, визначити, які інформаційні відносини в межах функціонування ДПСУ підпадають під кримінально-правову охорону; по-друге, установити статті КК, за якими настає кримінальна відповідальність за посягання на ці відносини.

**Виклад основного матеріалу.** Переважно інформаційні відносини, що підлягають кримінально-правовій охороні, розглядались у контексті захисту від витоку інформації. Така позиція відображає переважне право держави на захист інформаційних прав, оскільки пов'язується із захистом державної таємниці. Як справедливо зауважує М. В. Карчевський, таке становище не відповідає соціальним

тенденціям інформатизації та зумовленим ними потребам у правовому регулюванні й охороні суспільних відносин [10, с. 267]. Науковець зазначає, що суб'єкт перебуває в стані інформаційної безпеки тоді, коли ефективність його діяльності забезпечена повною, достовірною та достатньою для прийняття рішень інформацією [10, с. 271].

Діяльність ДПСУ охоплює різноманітні зовнішні та внутрішні напрями в межах охорони державного кордону та організації повсякденної діяльності, тому інформація, що знаходиться в її обігу, є досить різноманітною. Інформація, якою володіє розпорядник (кожен зі структурних підрозділів ДПСУ як суб'єкт інформаційних відносин), за змістом є такою: інформація про фізичну особу; інформація довідково-енциклопедичного характеру; науково-технічна інформація; правова інформація; статистична інформація; соціологічна інформація; інші види інформації. Крім того, за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом [3, ст. 20]. Відкритою є публічна інформація, що була отримана або створена в процесі виконання посадовими особами ДПСУ своїх обов'язків або яка знаходиться у володінні органів ДПСУ як суб'єктів владних повноважень. Така інформація є відкритою, тому не підлягає захисту, а відповідальність у цьому аспекті може настати для органів ДПСУ як розпорядників такої інформації і лише в адміністративно-правових межах за відмову, ненадання інформації або з інших підстав, передбачених законодавством [11].

Публічна інформація з обмеженим доступом є конфіденційною, таємною та службовою [11]. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, поширювання такої інформації можливе лише за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Порушення права громадянина на недоторканність приватного життя, особисту та сімейну таємницю тягне настання кримінальної відповідальності згідно зі ст. 182 КК. У разі коли недоторканність приватного життя було порушено

службовою особою ДПСУ в результаті службової недбалості, то за наявності підстав для того вчинене можна кваліфікувати за ст. 367 (425) КК. У такому випадку потерпілим від злочину може бути будь-яка особа (військовослужбовець або особа, яка не має відношення до служби в ДПСУ), без згоди якої збиралася або розповсюджувалася вказана конфіденційна інформація.

Згідно зі ст. 11 Закону України «Про соціальний і правовий захист військовослужбовців та членів їх сімей» військовослужбовці, а також члени їх сімей (у разі відсутності за місцем їх проживання державних або комунальних закладів охорони здоров'я) отримують кваліфіковану медичну допомогу у військово-медичних закладах охорони здоров'я. У зв'язку із цим медичному персоналу таких закладів доступна інформація про стан їх здоров'я [12]. За розголошення такої інформації, якщо це спричинило тяжкі наслідки, настає відповідальність згідно зі ст. 145 КК («Незаконне розголошення лікарської таємниці»).

Таємна інформація – це інформація, доступ до якої обмежується відповідно до законодавства та розголошення якої може завдати шкоди особі, суспільству і державі. Перелік відомостей, що становлять державну таємницю, у сфері охорони державного кордону передбачений наказом СБУ «Про затвердження Зводу відомостей, що становлять державну таємницю» від 12 серпня 2005 р. № 440. За розголошення відомостей такого характеру в КК передбачена відповідальність згідно зі ст. 328 («Розголошення державної таємниці»). У разі втрати документів або інших матеріальних носіїв секретної інформації, що містять державну таємницю, настає відповідальність, передбачена ст. 329 КК. Військовослужбовці ДПСУ в разі розголошення відомостей військового характеру, що становлять державну таємницю, за відсутності ознак державної зради несуть відповідальність відповідно до ст. 422 КК. Кримінальна відповідальність за шпигунство, тобто передачу або збирання з метою передачі іноземній державі, іноземній організації або їхнім представникам відомостей, що становлять державну таємницю, передбачена статтями 111 КК (у разі вчинення цих дій громадянином України) та 114 КК (якщо ці дії вчинені іноземцем або особою без

громадянства). Згідно із Законом України «Про військовий обов'язок і військову службу» військову службу в ДПСУ можуть проходити виключно громадяни України, водночас законодавчо не визначено заборони іноземцям та особам без громадянства перебувати на посадах працівників ДПСУ. У зв'язку з цим можемо зробити висновок, що шпигунські дії, вчинені військовослужбовцями ДПСУ, можуть бути кваліфіковані лише за ст. 111 КК, працівниками ДПСУ – як за ст. 111, так і ст. 114 КК (залежно від їх громадянства).

Службовою інформацією є інформація, що міститься: у документах органів ДПСУ, які становлять внутрішньовідомчу службову кореспонденцію; доповідних записках; рекомендаціях, пов'язаних з охороною державного кордону або здійсненням контрольних функцій, процесом прийняття рішень, а також рекомендаціях, що передують публічному обговоренню та/або прийняттю рішень; інформація, що зібрана в процесі оперативно-розшукової діяльності, у сфері оборони країни і яку не віднесено до державної таємниці. За передачу або збирання з метою передачі іноземним підприємствам, установам, організаціям або їх представникам таких відомостей, зібраних у процесі оперативно-розшукової діяльності, у сфері оборони країни, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства, передбачена кримінальна відповідальність згідно зі ст. 330 КК.

Широке використання комп'ютерних технологій у діяльності ДПСУ зумовлює необхідність технічного захисту інформаційної безпеки, що відображено в окремому розділі XVI КК «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Різноманітність сучасних інформаційних відносин, що підлягають кримінально-правовій охороні, потребує певної диференціації. Серед інформаційних відносин, що охороняються законом про кримінальну відповідальність, М. В. Карчевський виокремлює: 1) відносини щодо забезпечення доступу до інформаційних ресурсів; 2) відносини щодо формування інформаційного ресурсу; 3) відносини щодо забезпечення функціонування інформаційних

технологій як засобів доступу до інформаційного ресурсу та його формування [10, с. 270–271]. О. К. Тугарова злочини у сфері обігу інформації розмежовує за такими групами: злочини, що посягають на врегульовані законом суспільні відносини у сфері обігу інформації з обмеженим доступом та іншої інформації, що охороняється законом; злочини, що посягають на врегульовані законом суспільні відносини у сфері технічного захисту інформації; злочини, що посягають на врегульовані законом суспільні відносини у сфері інформаційно-психологічної безпеки особи та суспільства [13, с. 65]. У межах нашого дослідження варто ще розмежувати означені суспільні відносини за суб'єктивним складом. У прикордонній сфері кримінально-правовій охороні підлягають інформаційні права таких суб'єктів: осіб, які не пов'язані стійкими відносинами з ДПСУ (які перетинають державний кордон України, подають запит на інформацію про діяльність ДПСУ, про правила та особливості перетинання державного кордону України тощо); осіб, які входять до складу ДПСУ (військовослужбовці та працівники); суб'єкта, органу публічної влади – ДПСУ (інформація про діяльність відомства, його посадових осіб тощо).

**Висновки і перспективи подальших розвідок.** Розвиток інформаційного суспільства зумовлює створення відповідних умов в діяльності ДПСУ за двома основними напрямками: по-перше, доступ громадян чи зацікавлених органів влади до відкритої публічної інформації; по-друге, забезпечення захисту інформації з обмеженим доступом, яка стала відома й обробляється у зв'язку виконанням завдань держави (незалежно від носія збереження). Одним із засобів охорони інформаційних відносин з урахуванням доступу до інформації та її захисту в прикордонній сфері є встановлення кримінальної відповідальності за найбільш тяжкі порушення законодавства України про інформацію як один із видів відповідальності, що застосовується поряд із дисциплінарною, цивільно-правовою та адміністративною.

Питання вдосконалення норм кримінального законодавства щодо захисту інформаційних відносин у сфері діяльності ДПСУ у зв'язку із розширенням їх меж та різновидів можуть стати предметом подальших наукових розробок.

## Перелік літератури

1. Конституція України: Закон України від 28 черв. 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
2. Про Державну прикордонну службу України: Закон України від 3 квіт. 2003 р. № 661-IV. *Відомості Верховної Ради України*. 2003. № 27. Ст. 208.
3. Про інформацію: Закон України від 2 жовт. 1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.
4. Про схвалення Стратегії розвитку Державної прикордонної служби: розпорядж. Каб. Міністрів України від 23 листоп. 2015 р. № 1189-р. *Офіційний вісник України*. 2015. № 94. Ст. 3227.
5. Основні напрями діяльності та подальшого розвитку Державної прикордонної служби України у 2018 році. *Прикордонник України*. 2018. № 3–4 (5593–5594). С. 13–15.
6. Кримінальний кодекс України: Закон України від 5 квіт. 2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.
7. Писаренко Г. М. Юридична відповідальність в інформаційній сфері: окремі аспекти становлення. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2016. Вип. 36 (2). С. 55–58.
8. Проект Закону України «Про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки». *Законопроекти Верховної Ради України*. URL: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=42065](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=42065) (дата звернення: 09.06.2018).
9. Пояснювальна записка до проекту Закону України «Про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки». *Законопроекти Верховної Ради України*. URL: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=42065](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=42065).
10. Карчевський М. В. До питання визначення інформаційної безпеки як об'єкта кримінально-правової охорони. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. Вип. 1. С. 267–272.
11. Про доступ до публічної інформації: Закон України від 13 січ. 2011 р. № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.
12. Про соціальний і правовий захист військовослужбовців та членів їх сімей: Закон України від 20 груд. 1991 р. № 2011-XII. *Відомості Верховної Ради України*. 1992. № 15. Ст. 190.



13. Тугарова О. К. Кримінально-правове забезпечення охорони інформаційних відносин. *Науковий вісник Херсонського державного університету. Серія: Юридичні науки*. 2015. Вип. 4, т. 3. С. 61–66.

### Транслітерація переліку літератури

1. The Constitution of Ukraine Закон України від 28.06.1996 р. № 254к/96-VR (1996). *Vidomosti Verkhovnoi Rady Ukrainy*, 30, art. 141.

2. Pro Derzhavnu prykordonnu sluzhbu Ukrainy : Закон України від 03.04.2003 р. № 661-IV. (2003). *Vidomosti Verkhovnoi Rady Ukrainy*, 27, art. 208.

3. Pro informatsiiu: Закон України від 02.10.1992 р. № 2657-XII. (1992). *Vidomosti Verkhovnoi Rady Ukrainy*, 48, art. 605.

4. Pro skhvalennia Stratehii rozvytku Derzhavnu prykordonnu sluzhbu: pozporiadzhennia Kabinetu Ministriv Ukrainy від 23.11.2015 р. № 1189-р. (2015). *Ofitsijnyj visnyk Ukrainy – Official Gazette of Ukraine*, 94, art. 3227.

5. Osnovni napriamky diialnosti ta podalshoho rozvytku Derzhavnoi prykordonnoi sluzhbu Ukrainy u 2018 r.: *Prykordonnyk Ukrainy – Official Gazette of Ukraine*, 3-4 (5593-5594), art. 13-157.

6. Kryminalnyi kodeks Ukrainy: Закон України від 05.04.2001 р. № 2341-III. (2001). *Vidomosti Verkhovnoi Rady Ukrainy*, 25–26, art. 131.

7. Pysarenko, H. M. (2016). Yurydychna vidpovidalnist v informatsiinii sferi: okremi aspekty stanovlennia. *Naukovii visnyk Uzhhorodskoho natsionalnogo universytetu – Scientific herald of Uzhhorod National University*. Ser.: *Pravo*. issue 36(2), 55-58. [in Ukrainian].

8. Kartka zakonoproekt Zakonu pro vnesennia zmin do deiakykh aktiv Ukrainy shchodo vidpovidalnosti za posiahannia u sferi informatsiinoi bezpeky. *Zakonoproekty Verkhovnoi Rady Ukrainy*. URL: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=42065/](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=42065/)

9. Poiasniuvalna zapyska do proektu Zakonu Ukrainy «Pro vnesennia zmin do deiakykh aktiv Ukrainy shchodo vidpovidalnosti za posiahannia u sferi informatsiinoi bezpeky». *Zakonoproekty Verkhovnoi Rady Ukrainy*.

10. Karchevskii, M. V. (2012). Do pyttannia vyznachennia informatsiinoi bezpeky yak obiekta kryminalno-pravovoi okhorony. *Borotba z orhanizovanoi zlochinnistiu i koruptsiieiu (teoriia i praktyka) – Fighting Organized Crime and Corruption (theory and practice)*, issue 1, 267-272. [in Ukrainian].

11. Pro dustup do publichnoi informatsii : Закон України від 13.01.2011 р. № 2939-VI. (2011). *Vidomosti Verkhovnoi Rady Ukrainy*, 32, art. 314.

12. Pro sotsialnii i pravovyi zakhyst viiskovosluzhbovtziv ta chleniv yikh simei : Zakon Ukrainy vid 20.12.1991 r. № 2011-XII. (1992). *Vidomosti Verkhovnoi Rady Ukrainy*, 15, art. 190.

13. Tuharova, O. K. (2015). Kryminalno-pravove zabezpechennia okhorony informatsiinykh vidnosyn. [Public information relationsip Criminal framework protection]. *Naukovii visnyk Khersonskoho derzhavnoho universytetu – Kherson State University Herald Scientific. Ser.: Yurydychni nauki. issue 1*, 267-272. [in Ukrainian].

### ***Кушнір І. П. Кримінально-правове забезпечення охорони інформаційних відносин у прикордонній сфері***

У статті розглядаються питання кримінально-правової охорони інформаційних відносин. З появою нових видів загроз національній безпеці України у сфері охорони та захисту державного кордону питання розвитку та посилення захисту інформації набувають особливо важливого значення. Про це акцентовано у Стратегії розвитку Державної прикордонної служби України та в Основних напрямках діяльності та подальшого розвитку Державної прикордонної служби України у 2018 р. Належне дотримання інформаційного законодавства залежить і від установленної відповідальності за його порушення, що покладається на окремі норми КК України. Констатовано, що ці норми розміщені в різних розділах та не мають належної систематизації. Питання системного реформування кримінально-правового забезпечення охорони інформаційної безпеки України піднято на рівні Верховної Ради України та сьогодні залишається у статусі законопроекту.

Проаналізовані у статті відносини дозволили виокремити суб'єктів інформаційних відносин у прикордонній сфері, що підлягають кримінально-правовій охороні: особи, які не пов'язані стійкими відносинами з ДПСУ (які перетинають державний кордон України тощо); особи, які входять до складу ДПСУ (військово-службовці та працівники); ДПСУ як орган публічної влади (службова та таємна інформація, інформація про діяльність відомства, його посадових осіб тощо).

Одним із засобів охорони інформаційних відносин з урахуванням доступу до інформації та її захисту в прикордонній сфері є застосування кримінальної відповідальності.

**Ключові слова:** кримінально-правова охорона, інформація, інформаційні відносини, прикордонна сфера.

### ***Кушнір І. П. Уголовно-правовое обеспечение охраны информационных отношений в пограничной сфере***

В статье рассматриваются вопросы уголовно-правовой охраны информационных отношений. С появлением новых видов угроз национальной безопасности Украины в сфере охраны и защиты государственной границы вопросы развития

и усиления защиты информации приобретают особенно важное значение. Об этом акцентировано в Стратегии развития Государственной пограничной службы Украины и в Основных направлениях деятельности и дальнейшего развития Государственной пограничной службы Украины в 2018 р. Надлежащее соблюдение информационного законодательства зависит и от установленной ответственности за его нарушение, что возлагается на отдельные нормы УК Украины. Констатировано, что эти нормы расположены в разных разделах и не имеют надлежащей систематизации. Вопрос системного реформирования уголовно-правового обеспечения охраны информационной безопасности Украины, поднятый на уровне Верховного Совета Украины, и сегодня остается в статусе законопроекта.

Проанализированные в статье отношения позволили выделить субъектов информационных отношений в пограничной сфере, подлежащих уголовно-правовой охране: лица, не связанные устойчивыми отношениями с ГПСУ (пересекающие государственную границу Украины и т. д.); лица, входящие в состав ГПСУ (военнослужащие и работники); ГПСУ как орган публичной власти (служебная и секретная информация, информация о деятельности ведомства, его должностных лиц и т. д.).

Одним из средств охраны информационных отношений с учетом доступа к информации и ее защиты в пограничной сфере является применение уголовной ответственности.

**Ключевые слова:** уголовно-правовая охрана, информация, информационные отношения, пограничная сфера.

### ***Kushnir I. P. Criminal and law provision for protection of information relations in border guard sphere***

*The article deals with the issues of criminal and legal protection of information relations. With the advent of new types of threats to the national security of Ukraine in the field of security and protection of the state border, the issues of development and strengthening of information security are of particular importance. This is accentuated in the Strategy for the Development of the State Border Guard Service of Ukraine and in the Basic Directions for Activities and Further Development of the State Border Guard Service of Ukraine (SBGSU) in 2018. The due observance of the information legislation also depends on the established responsibility for its violation, which is based on separate norms in the Criminal Code of Ukraine. It is stated that these norms are located in different sections and are not systematized properly. The issues of systematic reforms of the criminal and legal provision for the protection of information security of Ukraine are passed at the level of the Verkhovna Rada of Ukraine and remain in the status of the bill nowadays.*

*The relations have been analyzed in the article and it allowed to identify the subjects of information relations in the border guard sphere which subject to criminal and legal protection: those persons who are not bound by stable relations with the SBGSU (those who cross the state border of Ukraine, etc.); persons belonging to the SBGSU (military personnel and employees); the SBGSU as a public author-*

*ity (official and secret information, information on the activities of the agency, its officials, etc.).*

*One of the means for protecting information relations with regard to access to information and its protection in the border guard sphere is the application of criminal responsibility.*

**Key words:** *criminal and legal protection, information, information relations, border guard sphere.*

*Рекомендовано до опублікування на засіданні кафедри теорії та історії держави і права та приватноправових дисциплін Національної академії Державної прикордонної служби України імені Богдана Хмельницького (протокол № 17 від 28.06.2018 р.)*