

Солоджук В.В.

## ІНФОРМАЦІЯ ТА ІНФОРМАЦІЙНА БЕЗПЕКА В СВІТЛІ КРИМІНАЛЬНО- ПРАВОВОЇ ОХОРОНИ

УДК 343.2:349

**Постановка проблеми.** Інформаційні суспільні відносини стрімко розвиваються, постійно зростають їх кількісні характеристики, змінюються якісні. Динаміка трансформації інформаційних явищ сьогодні є найвищою, що зумовлює необхідність їх дослідження в нових реаліях суспільного життя. Інформатизація та комп'ютеризація привели до збільшення кількості цінної інформації, яка оброблюється в автоматизованих системах, від якості, достовірності й оперативності одержання якої залежить більшість важливих рішень, що приймаються на різних рівнях – від глави держави до громадянина [1, с. 3]. Ця інформація з'являється в різних сферах життя, що, крім розвитку суспільних відносин, призводить до появи й нових видів протиправних посягань. При цьому їх небезпечність визначається важливістю таких сфер, що дає підстави стверджувати про необхідність правової охорони останніх.

Категорії «інформація», «інформаційна безпека» у комплексі наукових проблем, пов'язаних із правовою охороною інформаційних суспільних відносин, займають ключове місце. Вони є значущими для багатьох гуманітарних і технічних наук і в межах кожної з них існує власне бачення та визначення, яке відповідає предмету тієї чи іншої науки. В межах суміжних юридичних наук, зокрема в цивільному, адміністративному та інформаційному праві здійснено досить велику кількість досліджень з питань визначення інформації як об'єкта регулювання та охорони. Визначення інформаційної безпеки та інформації як об'єктів кримінально-правової охорони було зроблено М.В. Карчевським, а також висвітлено в роботах Д.С. Азарова, О.Е. Радутного, Н.А. Савінової та ін.

**Виклад основного матеріалу.** Первинно, увага до інформації та інформаційної безпеки в сфері кримінального права при-

вертається в межі вирішення проблем захищеності від витоку відомостей, що містять державну таємницю. Так, М.І. Хавронюк зазначає, що безпосереднім об'єктом державної зради є національна безпека переважно у сфері державної безпеки, інформаційній, економічній, науково-технологічній і військовій сферах, уточнюючи при цьому, що інформаційна безпека, в контексті ст. 111 КК України, перш за все означає захищеність України від витоку інформації, що складає державну таємницю [2, с. 257-258]. Е.М. Кісілюк та В.І. Павловський при аналізі складу злочину державної зради зазначають, що під загрозами національній (у тому числі державній) безпеці України в інформаційній сфері слід розуміти витік інформації, яка становить державну таємницю [3, с. 31]. Подібні позиції займають й інші науковці [4, с. 10, 26].

В сучасних умовах такий підхід не відповідає тенденціям інформатизації суспільства та викликаним ними потребам у правовому регулюванні й охороні суспільних відносин. Як зазначає М.В. Карчевський, в умовах, коли можливі загрози у сфері інформаційної безпеки далеко не вичерпуються витоком відомостей, що складають державну таємницю, кримінальне право, як нормативна база охорони суспільних відносин від кримінально протиправних посягань, не повинне розглядати інформаційну безпеку настільки вузько [5, с. 10].

Поява категорії «інформаційна безпека» у вітчизняному правовому полі пов'язана зі ст. 17 Конституції України, у якій зазначено: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу». В Указі Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31.07.2000 р. [6] поняття інформаційної безпеки вже не обмежувалося тільки захистом інформаційного ресурсу, а вже вказувалося на недопущення поширення інформації, розповсюдження якої заборонено відповідно до законодавства. Мова йде як про «негативну» інформацію (порнографія, пропаганда культури насильства або жорстокості тощо), так й про «позитивну» інфор-

мацію, яка належить певним суб'єктам, які не бажають її розповсюдження (комерційна або банківська таємниця, державна таємниця, таємниця приватного життя тощо).

В подальшому поняття інформаційної безпеки було розвинуто в Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 р. – це «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» [7]. Мова йде вже не просто про технічний захист інформації, а про стан захищеності від загроз інформаційного та технологічного характеру.

Указом Президента України №514/2009 від 08.07.2009 р. було затверджено Доктрину інформаційної безпеки України [8] (втратила чинність на підставі Указу Президента № 685/2021 від 28.12.2021 р.), яка, по-перше, визначала інформаційну безпеку одночасно як невід'ємну складову кожної зі сфер національної безпеки та як самостійну сферу національної безпеки, а по-друге, класифікувала життєво важливі інтереси в інформаційній сфері за суб'єктами (особа, суспільство та держава). До таких інтересів особи було віднесено: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та розповсюдження інформації; недопущення несанкціонованого втручання в зміст, процеси обробки, передачі та використання персональних даних; захищеність від негативного інформаційно-психологічного впливу.

Законом України «Про національну безпеку України» від 21.06.2018 р. [9] передбачено створення Стратегії національної безпеки України (ст. 26), яка «є основою для розроблення таких документів щодо планування у сферах національної безпеки і оборони, які визначатимуть шляхи та інструменти її реалізації» (п. 66) [10]. Одним з таких документів є Стратегія інформаційної безпеки [11]. Вона визначає актуальні виклики та загрози націо-

нальній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних. Метою Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина. Досягнення мети здійснюватиметься шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підлив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки.

Інформаційна безпека України в Стратегії визначається як складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Отже, аналіз національного законодавства дозволяє стверджувати, що наявною є тенденція розширення змісту законодавчого визначення поняття «інформаційна безпека» від вузького,

найпростішого її розуміння як технічного захисту інформації, до складної розгалуженої системи характеристик [5, с. 15].

Істотну частину визначень інформаційної безпеки, представлених у науковій літературі, сконструйовано за принципом розуміння цієї категорії як стану захищеності від певних небажаних наслідків. В той же час, один із провідних українських дослідників у цій сфері Б.А. Кормич визначає інформаційну безпеку як «захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані конституцією умови існування і розвитку людини, всього суспільства і держави» [12, с. 92]. Подібного розуміння дотримується й А.І. Марущак, який визначає інформаційну безпеку через комплекс прав людини: вільно, безперешкодно, на власний розсуд бути суб'єктом інформаційних процесів (шукати, одержувати та поширювати інформацію) та отримувати захист від неправомірного інформаційного втручання [13, с. 82]. Такий підхід акцентує увагу на значенні правового регулювання інформаційної сфери, а отже й її охорони. Метою правового регулювання інформаційних відносин є, з одного боку, розширення вільного доступу до інформації, а з іншого – збереження окремих регламентованих обмежень на її поширення [14, с. 304]. На необхідності захисту інформації наголошує А.В. Бегун, який відносить до нього питання, пов'язані з побудовою системи захисту від несанкціонованих дій з інформацією [15, с. 9].

Розглядаючи інформаційну безпеку як об'єкт кримінально-правової охорони М.В. Карчевський зазначив, що за суттю вона є не певним станом або захищеністю, а системою суспільних відносин. Крім цього, дуже важливою її ознакою є її динамічність, оскільки вона являє собою забезпечення стабільності та розвитку інформаційної сфери, яка постійно змінюється через різноманіття потреб учасників інформаційних відносин [5, с. 24-25]. Слід підтримати позицію вченого, що суспільні відносини, що складають інформаційну безпеку як об'єкт кримінально-правової охорони, слід визначати так, щоб висновок щодо необхідності застосування кримінально-правових засобів для охорони саме цих відносин був чітким і послідовним. Тобто особу слід вважати

такою, що перебуває в стані інформаційної безпеки тоді, коли її потреба в інформації забезпечена належним чином, коли особа має можливість одержувати достовірну та достатню для здійснення ефективної діяльності інформацію. А суспільно небезпечними слід визнати такі посягання у сфері інформаційної безпеки, які виключають або значно ускладнюють реалізацію інформаційної потреби [16].

Крім того, враховуючи різноманіття відносин, які утворюють інформаційну безпеку, можемо говорити й про те, що її кримінально-правова охорона забезпечується за допомогою норм, що передбачають посягання на різноманітні родові об'єкти, одним з яких є відносини у сфері господарської діяльності.

Інформація, створена чи виявлена, систематизована, зареєстрована й накопичена у перетвореній формі, є інформаційним ресурсом [5, с. 24-25]. Інформаційним ресурсом слід вважати всю сукупність об'єктивованої інформації, тобто інформації, яка знаходиться на певному носіїві й може слугувати задоволенню інформаційної потреби людини, держави або суспільства [5, с. 26].

Визначивши інформаційну безпеку як систему суспільних відносин щодо забезпечення реалізації інформаційних потреб громадян, суспільства, держави, яка включає: 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 функціонування, М.В. Карчевський дійшов висновку, що суб'єкт перебуває в стані інформаційної безпеки тоді, коли ефективність його діяльності забезпечена повною, достовірною та достатньою для прийняття рішень інформацією [5, с. 28]. Такий стан досягається соціальною активністю в трьох взаємопов'язаних групах суспільних відносин, що складають інформаційну безпеку: у сфері використання інформаційних технологій, у сфері забезпечення доступу до інформаційного ресурсу й у сфері формування інформаційного ресурсу. Ті суспільні відносини, які охороняються законом про кримінальну відповідальність, складають зміст інформаційної безпеки як об'єкта кримінально-правової охорони.

Відповідно до чинного законодавства суспільні відносини в сфері інформаційної безпеки відносяться до значної кількості різних родових об'єктів. Це зумовлено тим, що інформація є необхідною передумовою будь-якої діяльності людини, тому наслідки посягання в інформаційній сфері можуть наставати в достатньо великій кількості інших різноманітних сфер. Не є виключенням й сфера господарської діяльності, в якій інформаційна складова відіграє неабияку роль.

В контексті кримінальних правопорушень у сфері господарської діяльності проблеми кримінальної відповідальності за посягання на інформаційну безпеку розглядалися фрагментарно, переважно щодо інформації з обмеженим доступом (О.Е. Радутний, С.О. Харламова, П.С. Берзін), яку слід визнавати предметом кримінального правопорушення.

Традиційно в науці кримінального права при визначенні предмету кримінального правопорушення вказується на те, що ним може бути лише річ матеріального світу [17, с. 128; 18, с. 173]. І тільки останнім часом набуває розвитку підхід, започаткований О.Е. Радутним [19, с. 5-6, 10], за яким предметом злочину можуть бути і феномени, які не являють собою річ – наприклад, інформація. Предмет кримінального правопорушення – це факультативна ознака об'єкта, яка знаходить свій прояв у матеріальних цінностях (які людина може сприймати органами чуття чи фіксувати спеціальними технічними засобами), з приводу яких та/або шляхом безпосереднього впливу на які вчинюється діяння [20, с. 110-111]. Така позиція базується на наступних аргументах:

- відповідно до філософського розуміння матерії, до неї відносять усю об'єктивну реальність, що існує поза людської свідомістю і незалежно від неї, яку можна сприйняти органами відчуття або за допомогою відповідних приладів;

- кримінально протиправне діяння являє собою акт поведінки людини, спрямований на здійснення впливу на ті субстанції, які перебувають поза особою, існують об'єктивно на момент вчинення кримінального правопорушення;

- вплив на об'єкт кримінального правопорушення може бути здійснено вчиненням дії або бездіяльності щодо будь-яких матеріальних утворень;

- завдяки тому, що матеріальні об'єкти у будь-якій формі доступні для сприйняття органами чуття (чи то людиною безпосередньо, чи за допомогою відповідних приладів), дії щодо них можуть бути зафіксовані, а завдана шкода піддається якісному й кількісному виміру;

- у диспозиціях статей Особливої частини КК України фактично вказуються субстанції, на які спрямоване посягання: вони мають форму як речей, так і інших видів матерії [21, с. 174-175].

На сьогоднішній день набуває першорядного значення переосмислення самого поняття інформації, її ролі в сучасному світі. Під інформацією звичайно розуміють певні відомості про оточуючий світ і процеси, які в ньому відбуваються, повідомлення про стан справ, положення певних людей, суспільних явищ, про предмети тощо. Саме забезпечення охорони інформації від протиправного поширення, отримання доступу до неї сторонніх осіб, або ж, навпаки, від приховування певних відомостей від інших осіб вимагає її кримінально-правової охорони.

Низка термінів, що використовуються законодавцем при побудові кримінально-правових норм та які визначають відносини у сфері забезпечення інформаційної безпеки, призводить до їх різного тлумачення та відмінностей у правозастосуванні. Це такі уживані в законі слова та словосполучення, що характеризують інформацію як предмет кримінального правопорушення, як: «відомості», «дані», «таємниця», «документи», «матеріали», «носії» тощо.

Відповідно до тлумачного словника з української мови, інформація (лат. informatio) – це відомості про навколишній світ, процеси, які в ньому відбуваються, про події, ситуації, чиясь діяльність, що їх сприймають людина і живі організми, машини та інші системи [22, с. 368]. Схоже за змістом, але доповнене можливістю збереження на матеріальних носіях або відображення в електронному вигляді, визначення інформації міститься в українському законодавстві. Так, Закон України «Про інформацію» визначає інформацію як «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» (ст. 1) [23]. Таке визначення відображає



лише формальний бік цього явища і не враховує його соціального значення як цінності, товару, влади, зброї для нападу й захисту, потенціалу для розвитку і причини деградації, світогляду, засобу взаємодії тощо. Глибина осягнення феномену «інформація» впливає на усвідомлення низки явищ, які визначають майбутнє людства.

Так, визнання інформації предметом кримінального правопорушення вважається правильним на тій підставі, що вона завжди передається за допомогою відповідних носіїв, її можна побачити, почути, відчувати на дотик (це, наприклад, голос людини або інший звук, певне зображення); інформацію можна змінити, знищити, заблокувати, спотворити, скопіювати, заволодіти, поширити тощо [24, с. 155]. На ознаки протиправного діяння, що посягає на інформаційну безпеку, вказують такі терміни: «розголошення», «розповсюдження», «завідомо неправдиве повідомлення», «втрата», «привласнення», «заклик», «фальсифікація» тощо [25, с. 278-282].

**Висновок.** В сучасному суспільстві відбувається принципова зміна ролі інформації: вона стає основним ресурсом в економіці, без неї є неможливим політичне, культурне, приватне життя людини, через що таке суспільство навіть отримало назву «інформаційне суспільство». Це призводить до того, що виникає потреба в нормативно-правовому відображенні таких змін, адже без належного регулювання інформаційних прав і свобод людини, за відсутності високого рівня їх охорони, стає неможливим ефективний механізм реалізації інформаційних відносин. Безсумнівно, однією з найважливіших складових такого механізму є кримінально-правова охорона інформації, адже від цього буде залежати напрямок, інтенсивність розвитку та ефективність суспільних відносин.

1. Юдін О.К. *Інформаційна безпека держави: навчальний посібник* / О.К. Юдін, В.М. Бозуш. Харків, 2005. 576 с.
2. *Науково-практичний коментар до Кримінального кодексу України / за ред. М.І. Мельника, М.І. Хавронюка. 8-е вид., перероб. і доп. Харків, 2011. 1280 с.*
3. *Кримінальне право України (Особлива частина): підручник / за заг. ред. О.М. Литвинова. Харків, 2011. 572 с.*

4. *Кримінальне право України: Особлива частина: підручник / за заг. ред. Є.Л. Стрельцова. Харків, 2009. 496 с.*
5. *Карчевський М.В. Кримінально-правова охорона інформаційної безпеки України: монографія. Луганськ, 2012. 528 с.*
6. *Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні: указ Президента України від 31.07.2000 р. № 928/2000. URL: <https://zakon.rada.gov.ua/laws/show/928/2000#Text> (дата звернення: 16.05.2022).*
7. *Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: закон України від 09.01.2007 р. № 537-V. URL: <https://zakon.rada.gov.ua/laws/show/537-16#Text> (дата звернення: 16.05.2022).*
8. *Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: указ Президента України від 25.02.2017 р. № 47/2017. URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> (дата звернення: 16.05.2022.).*
9. *Про національну безпеку України: закон України від 21.06.2018 р. № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#n355> (дата звернення: 16.05.2022).*
10. *Стратегія національної безпеки України: безпека людини – безпека країни, затверджена указом Президента України від 14.09.2020 р. № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#n12> (дата звернення: 16.05.2022).*
11. *Стратегія інформаційної безпеки, затверджена указом Президента України від 28.12.2021 р. № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення: 16.05.2022).*
12. *Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навч. посібник. Київ, 2004. 384 с.*
13. *Марущак А.І. Інформаційне право: доступ до інформації: навч. посіб. для студ. ВНЗ. Київ, 2007. 531 с.*
14. *Колодій І.М. Інформаційна безпека: деякі проблеми визначення поняття. Держава і право. 2008. Вип. 40. С. 300 – 305.*
15. *Бегун А.В. Інформаційна безпека: навчальний посібник. Київ, 2008. 280 с.*
16. *Соснін О.В. Державна політика в галузі управління інформаційним ресурсом України: автореф. дис. ... д-ра політ. наук: 23.00.02. Одеса: Одеська національна юридична академія, 2005. 36 с.*

17. *Кримінальне право України: Загальна частина: підручник / за ред. В.Я. Тація, В.І. Тютюгіна, В.І. Борисова. 6-те вид., переробл. і допов. Харків, 2020. 584 с.*
18. *Гришук В.К. Кримінальне право України: Загальна частина: Навч. посіб. для студентів юрид. фак. вищ. навч. закл. Київ, 2006. 568 с.*
19. *Радутний О.Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю (аналіз складів злочинів): автореф. дис. ... канд. юрид. наук: 12.00.08. Харків, 2002. 21 с.*
20. *Музика А.А., Лацук Є.В. Предмет злочину: теоретичні основи пізнання: Монографія. Київ, 2011. 192 с.*
21. *Українське кримінальне право. Загальна частина: підручник / за ред. В.О. Навроцького. Київ, 2013. 712 с.*
22. *Дубчинський В.В. Сучасний тлумачний словник української мови: 65000 слів. Харків, 2006. 1008 с.*
23. *Про інформацію: закон України від 02.10.1992 р. № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 16.05.2022).*
24. *Дудоров О.О., Хавронюк М.І. Кримінальне право: навч. посібник / За заг. ред. М.І. Хавронюка. Київ, 2014. 944 с.*
25. *Дзюба Ю.П. Інформаційна безпека в системі міжгалузевих зв'язків кримінального права. Наука кримінального права в системі міждисциплінарних зв'язків: матер. Міжнар. наук.-практ. конф., 9-10 жовтня 2014 р. Харків, 2014. С. 278-282.*

**Солоджук В.В. Інформація та інформаційна безпека в світлі кримінально-правової охорони**

У статті проводиться аналіз розуміння інформаційної безпеки та інформації в контексті їх кримінально-правової охорони. Проаналізований розвиток розуміння інформаційної безпеки в доктрині кримінального права та суміжних галузей права, а також в інших суспільних науках. Крім того, визначений шлях зміни розуміння інформаційної безпеки у вітчизняному законодавстві за наявною тенденцією розширення її змісту від вузького, найпростішого розуміння як технічного захисту інформації, до складної розгалуженої системи характеристик. Встановлено, що принципова зміна ролі інформації, яка відбувається в сучасному суспільстві, коли вона стає основним ресурсом в економіці, без неї є неможливим політичне, культурне, приватне життя людини, призводить до того, що виникає потреба в нормативно-правовому відображенні таких змін, адже без належного регулювання інформаційних прав і свобод людини, за відсутності високого рівня їх охорони, стає неможливим ефективний механізм реалізації інформаційних відносин. Безсумнівно, однією з найважливіших складових такого механізму є кримінально-правова охорона інформації, адже від цього буде

залежати напрямом, інтенсивність розвитку та ефективність всіх суспільних відносин. Визнання інформації предметом кримінального правопорушення вважається правильним на тій підставі, що вона завжди передається за допомогою відповідних носіїв, її можна побачити, почути, відчувати на дотик; інформацію можна змінити, знищити, заблокувати, спотворити, скопіювати, заволодіти, поширити тощо.

**Ключові слова:** інформація, інформаційна безпека, таємниця, відомості, кримінально-правова охорона, предмет кримінального правопорушення.

**Solodzhuk V.V. Information and information security in the light of criminal law protection**

The article analyzes the understanding of information security and information in the context of their criminal law protection. The development of the understanding of information security in the doctrine of criminal law and related branches of law, as well as in other social sciences, is analyzed. In addition, the way of changing the understanding of information security in domestic legislation is defined according to the existing tendency to expand its content from a narrow, simple understanding as technical protection of information to a complex branched system of characteristics. It has been established that the fundamental change in the role of information that takes place in modern society, when it becomes the main resource in the economy, without it the political, cultural, and private life of a person is impossible, leads to the fact that there is a need for a regulatory and legal reflection of such changes, because without proper regulation of information rights and freedoms of a person, in the absence of a high level of their protection, an effective mechanism for the implementation of information relations becomes impossible. Undoubtedly, one of the most important components of such a mechanism is the criminal law protection of information, because the direction, intensity of development and effectiveness of all social relations will depend on it. Recognizing information as the subject of a criminal offense is considered correct on the basis that it is always transmitted using appropriate media, it can be seen, heard, and felt; information can be changed, destroyed, blocked, distorted, copied, appropriated, distributed, etc.

**Keywords:** information, information security, secret, details, criminal law protection, subject of criminal offence.