УДК 35:004.05

Усик Світлана
ORCID iD 0000-0001-7219-3727
E-mail: usicom@ukr.net

ДОСЛІДЖЕННЯ ПРАВОВОГО МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

https://doi.org/10.32689/2618-0065-2020-4(6)-266-280

Анотація. Інформаційна безпека в системі публічного управління є складовою національної безпеки України, яка забезпечує захист системи публічного управління від інформаційно-комунікаційних загроз та викликів. Автор розглядає інформацію, як основу безпечного та раціонального розвитку сучасного інформаційного суспільства. Водночас, інформація може слугувати зброєю, яка впливає на світогляд людини, населення, формує негативне ставлення до певних явищ, до держави та суспільства в цілому, викривляє факти та події, що впливає на якість та ефективність сучасних реформ у суспільстві тощо. Системний характер інформаційної безпеки дозволяє визначити її забезпечення як складний, комплексний вид діяльності, що висуває особливі вимоги до його структурної характеристики. Наукові дослідження не виробили загальноприйнятого механізму структуризації забезпечення інформаційної безпеки. Одним із пріоритетних напрямів безпекової політики України повинно стати підвищення безпеки та стійкості цивільного захисту по відношенню до усього спектру загроз і ризиків, оскільки саме критична інфраструктура забезпечує життєво важливі для населення, суспільства та держави послуги та функції, без яких неможливі їх безпечне існування та благополуччя, а також належний рівень національної безпеки. Проведений аналіз стану нормативно-правового забезпечення технічного захисту інформації та інформаційної безпеки України в умовах надзвичайних ситуацій дозволяє зробити висновок про фрагментарності вибору об'єктів правового регулювання в сфері протидії загрозам національній безпеці в інформаційній сфері, недостатньою узгодженості використовуваних для цього правових механізмів, недостатню ефективність, а, найчастіше, і

суперечливості використовуваних ними правових норм. Питання забезпечення безпеки інформаційної системи попередження і ліквідації наслідків надзвичайних ситуацій, а також системи збору, обробки, обміну та видачі інформації у сфері захисту населення і територій від надзвичайних ситуацій природного і техногенного характеру, законодавчо не відображені в нормативно-правових актах, що регулюють діяльність підрозділів Державної служби з надзвичайних ситуацій України. У зв'язку з чим, в роботі сформульовані пропозиції щодо вдосконалення чинного законодавства в галузі забезпечення інформаційної безпеки при захисті населення і територій від надзвичайних ситуацій природного і техногенного характеру.

Ключові слова: інформація, безпека, надзвичайна ситуація, управління, цивільний захист.

Постановка проблеми. Одним із важливих чинників суспільного розвитку XXI століття є досить триваюча науково-технічна революція в області обчислювальної техніки й інформаційно-телекомунікаційних технологій. Її наслідком стала глобалізація процесів економічного та політичного розвитку людського суспільства, яка створила передумови для підвищення значимості всього інформаційного простору.

Однак, одночасно зростає і потенційна вразливість суспільних процесів від інформаційного впливу, тобто на зміну небезпеки виникнення ядерної катастрофи може прийти загроза розв'язання війни, яка прийме нові форми. Це буде боротьба, спрямована проти країн, що володіють передовими технологіями, з метою створення хаосу в інформаційних структурах і породження як політичної, так і економічної катастрофи.

У зв'язку з цим особливо актуальними стають проблеми забезпечення технічного захисту інформації та інформаційної безпеки в цілому, тобто забезпечення безпеки розвитку особистості, функціонування громадських структур та органів державної влади в інформаційній сфері, а особливо в умовах надзвичайних ситуацій.

Аналіз попередніх досліджень. Я. Чмир проаналізувано наукові підходи до проблеми забезпечення інформаційної безпеки системи публічного управління [1]. Визначено, що інформаційна безпека в системі публічного управління є складовою національної безпеки України, яка забезпечує захист системи публічного управління від інформаційно-комунікаційних загроз та викликів. Автор розглядає інформацію, як основу безпечного та раціонального розвитку сучасного інформаційного суспільства. Водночас, інформація може слугувати зброєю, яка впливає на світогляд людини, населення, формує негативне ставлення до певних явищ, до держави та суспільства в цілому, викривляє факти та події, що впливає на якість та ефективність сучасних реформ у суспільстві тощо.

Аналіз джерел наукової інформації свідчить про те, що поняття «інформаційна безпека» розглядається різними авторами, виходячи з фокусу їх наукових розвідок. Зокрема дослідник Б. Кормич [2] характеризує національну безпеку як стан захищеності держави від внутрішніх і зовнішніх загроз, що забезпечує умови існування людини, держави і суспільства, які гарантовані Конституцією та законами України. Існує розуміння В. Шатуна [3] щодо інформаційної безпеки як виду суспільних інформаційних правовідносин стосовно створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов’язані зі створенням, зберіганням, поширенням і використанням інформації.

Питання інформаційного забезпечення ліквідації наслідків НС природного і техногенного характеру попередньо досліджувалося П. Волянським – інформаційне забезпечення органів місцевої влади постраждалої території під час проведення аварійно-рятувальних і гуманітарних операцій [4]; С. Гур’євим – як інформаційне забезпечення мобільних рятувальних і медичних формувань, які працюють в локальних районах постраждалої території [5].

Системний характер інформаційної безпеки дозволяє визначити її забезпечення як складний, комплексний вид діяльності, що висуває особливі вимоги до його структурної характеристики. Наукові дослідження не виробили загальноприйнятого механізму структуризації забезпечення інформаційної безпеки. Для виокремлення складових його загальної структури найчастіше використовуються такі конструкції, як «напрями», «механізми» та «шляхи» забезпечення [6].

Мета статті. Визначити стан правового механізму забезпечення інформаційної безпеки в умовах надзвичайних ситуацій.

Виклад основного матеріалу. Забезпечення національної безпеки є невід'ємною функцією кожної держави, як суспільного утворення, що має гарантувати сприятливі умови для життя і продуктивної діяльності її громадян [9]. Введенням у липні 2013 року в дію Кодексу цивільного захисту України, який регулює в державі відносини, пов'язані із захистом населення, територій, навколишнього природного середовища та майна від надзвичайних ситуацій, законодавчо упорядковано і посилено функції держави щодо забезпечення техногенної та природної безпеки в Україні [10].

Одним із пріоритетних напрямів безпекової політики України повинно стати підвищення безпеки та стійкості цивільного захисту відносно до усього спектру загроз і ризиків, оскільки саме критична інфраструктура забезпечує життєво важливі для населення, суспільства та держави послуги та функції, без яких неможливі їх безпечне існування та благополуччя, а також належний рівень національної безпеки [9]. Мета інформаційної безпеки цивільного захисту полягає в забезпеченні системи стратегічних комунікацій між населенням та органами влади, розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та

захист під час виникнення надзвичайних ситуацій та ліквідації її наслідків.

Державна служба з надзвичайних ситуацій України відповідно до Положення [11] здійснює такі основні функції, пов'язані з правовим забезпеченням інформаційної безпеки України:

розробляє і подає пропозиції щодо реалізації державної політики і проекти нормативних правових актів в галузі цивільної безпеки, захисту населення і територій від надзвичайних ситуацій, забезпечення пожежної безпеки та безпеки людей на водних об'єктах, а також інші документи;

здійснює разом із центральними та місцевими органами виконавчої влади, органами місцевого самоврядування, підприємствами, установами, організаціями прогнозування імовірності виникнення надзвичайних ситуацій, визначає показники ризику та здійснює районування території України щодо ризику виникнення надзвичайних ситуацій;

здійснює контроль за створенням локальних систем оповіщення в районах розміщення потенційно небезпечних об'єктів;

здійснює збір і обробку інформації в галузі цивільного захисту, захисту населення і територій від надзвичайних ситуацій, забезпечення пожежної безпеки та безпеки людей на водних об'єктах;

забезпечує в межах своєї компетенції проведення заходів щодо захисту державної таємниці та службової інформації;

бере участь в межах своєї компетенції в інформуванні населення через засоби масової інформації та по інших каналах про прогнозовані і виникли надзвичайні ситуації та пожежі, заходи щодо забезпечення безпеки населення і територій, прийоми та способи захисту, а також здійснює інформування в галузі цивільного захисту, захисту населення і територій від надзвичайних ситуацій, забезпечення пожежної безпеки та безпеки людей на водних об'єктах.

Слід зазначити, що безпека проявляється як неможливість нанесення шкоди функціонуванню та властивостям об'єкта, або його структурним складовим. Це положення служить методологічною підставою для виділення видів безпеки. Однією з важливих структурних складових багатьох об'єктів безпеки є інформація або діяльність, предметом якої є інформація.

На сьогодні склались дві тенденції в органах державної влади у визначенні поняття та структури інформаційної безпеки. Представники гуманітарного напряму пов'язують інформаційну безпеку лише із забезпеченням державної таємниці. Представники силових структур пропонують поширити сферу інформаційної безпеки практично на всі питання й відносини в інформаційній сфері. «Хто володіє інформацією, той володіє світом». Інформаційна безпека суспільства й держави характеризується ступенем їх захищеності, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості тощо) щодо небезпечних, дестабілізуючих, деструктивних дій, які шкодять інтересам країни. Отже, під захистом інформації розуміється комплекс заходів, які здійснюються власником інформації щодо виокремлення своїх прав на володіння й розпорядження інформацією, створення умов, які обмежують її поширення, виключають чи суттєво ускладнюють несанкціонований, незаконний доступ до таємної інформації та її носіїв.

Інформація, що захищається, може містити різні категорії відомостей, з установленим ступенем їх секретності та мати свої особливості регулювання збереження її цілісності.

Технічний захист інформації, як окрема складова діяльності з забезпечення безпеки інформації є діяльністю, спрямованою на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а

також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

У Доктрині інформаційної безпеки України [7] зазначено, що від обсягу, швидкості та якості обробки інформації значною мірою залежить ефективність управлінських рішень, зростає значення методів управління з використанням інформаційних технологій соціальними та економічними процесами, та найголовніше – це спроможність ідентифікувати науково-технічні та екологічні проблеми, здійснювати моніторинг їх розвитку із подальшим прогнозуванням наслідків, що безпосередньо залежить від ефективності використовуваної інформаційної інфраструктури та її захисту.

На сучасному етапі основними реальними та потенційними загрозами інформаційній безпеці України є приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації чи надзвичайні ситуації техногенного та природного характеру; недостатня надійність або взагалі незахищеність інформаційно-телекомунікаційних систем, які відповідають за збирання, обробку та передачу інформації в умовах надзвичайних ситуацій; низький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпечних об'єктів і територій, завчасного прогнозування та реагування на надзвичайні ситуації.

Тобто, особливе значення для повноцінного функціонування державних об'єктів має забезпечення безпеки інформаційної інфраструктури країни при аваріях, катастрофах і стихійних лихах.

На нашу думку, забезпечення інформаційної безпеки в умовах надзвичайних ситуацій – це забезпечення безпеки інформаційних систем, що сприяють прийняттю рішень по оперативним діям, пов'язаним з розвитком таких ситуацій і ходом ліквідації їх наслідків, а також забезпечення безпеки

систем збору і обробки інформації про можливе виникнення надзвичайних ситуацій.

Приховування, затримка надходження, спотворення і руйнування оперативної інформації, несанкціонований доступ до неї окремих осіб або груп осіб можуть привести як до людських жертв, так і до виникнення різного роду складнощів при ліквідації наслідків надзвичайної ситуації, пов'язаних з особливостями інформаційного впливу в екстремальних умовах: до приведення в рух великих мас людей, що зазнають психічний стрес; до швидкого виникнення і розповсюдження серед них паніки і заворушень на основі чуток, неправдивої або недостовірної інформації.

Необхідно відзначити, що негативні впливи на об'єкти інформаційної безпеки можуть призвести до серйозних збитків життєво важливим інтересам та завдати значних соціально-економічних втрат державі, суспільству, репутації ДСНС України і його структурам, та окремим громадянам [8]. Діяльність із забезпечення інформаційної безпеки, в тому числі і в умовах надзвичайних ситуацій, проявляється у формі соціального регулювання, в тому числі правового, а також політичної діяльності і організаційних заходів з протидії загрозам національним інтересам в інформаційній сфері.

Окремі положення нормативно-правових актів законодавства України, що регулюють відносини в галузі прав і свобод людини і громадянина, внутрішньо суперечливі і, в деяких випадках, не узгоджуються з нормами міжнародного права. Зайва декларативність правових норм призводить до того, що їх порушення далеко не завжди тягне за собою настання відповідної відповідальності, що істотно знижує ефективність правового регулювання даних відносин законодавством і створює передумови для звернення потерпілих в міжнародні судові інстанції.

Низка найбільш серйозних недоліків правового забезпечення захисту прав і свобод людини і громадянина в

інформаційній сфері, що посилюються при виникненні надзвичайних ситуацій та в ході їх ліквідації, включає :

недосконалу визначеність механізмів забезпечення доступу до відкритої інформації органів державної влади та органів місцевого самоврядування, що створює умови для порушення прав і свобод людини і громадянина, включаючи право на інформацію, про стан навколишнього середовища, факти та обставини, що створюють загрозу для життя і здоров'я людей;

відсутність встановлених норм відповідальності за обмеження або порушення права на доступ до відкритої інформації;

відсутність державного регулювання поширення інформації, призначеної для необмеженого кола споживачів, у відкритих інформаційно-телекомунікаційних мережах.

До основних недоліків правового забезпечення безпеки функціонування інформаційних і телекомунікаційних систем та мереж зв'язку, українських інформаційних ресурсів відносяться:

диспропорції в розвитку загальної складової державного законодавства, наявність протиріч між ними, а також відсутність законодавчої бази для узгодження законотворчої діяльності України та її суб'єктів;

недостатнє нормативно-правове державне регулювання відносин в області розвитку технічного захисту інформації під час забезпечення інформаційної безпеки;

недостатня ефективність правових механізмів встановлення відповідальності за правопорушення у сфері забезпечення інформаційної безпеки.

Проведений аналіз стану нормативно-правового забезпечення технічного захисту інформації та інформаційної безпеки України в умовах надзвичайних ситуацій дозволяє зробити висновок щодо фрагментарності вибору об'єктів правового регулювання в сфері протидії загрозам національній безпеці в інформаційній сфері, недостатньою узгодженості використовуваних для цього правових механізмів, недостатню

ефективність, а, найчастіше, і суперечливості використовуваних ними правових норм.

Сьогодні державне регулювання технічного захисту інформації та забезпечення інформаційної безпеки в умовах надзвичайних ситуацій як єдина система узгоджених норм правового регулювання відносин у сфері протидії загрозам національним інтересам України в інформаційній сфері розвинене недостатньо.

Є певні недоліки і в розвитку правотворчого процесу в області забезпечення інформаційної безпеки в умовах надзвичайних ситуацій. На жаль, правотворчість в цій області характеризується хаотичністю, розрізненістю ініціатив окремих суб'єктів законодавчої ланки, а також дій органів виконавчої влади.

Найбільш уразливими об'єктами забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій є система прийняття рішень з оперативних дій (реакцій), пов'язаним із розвитком таких ситуацій і ходом ліквідації їхніх наслідків, а також; система збору й обробки інформації про можливе виникнення надзвичайних ситуацій.

Особливе значення для нормального функціонування зазначених об'єктів має забезпечення безпеки інформаційної інфраструктури країни при аваріях, катастрофах і стихійних лихах. Приховування, затримка надходження, перекручування та руйнування оперативної інформації, несанкціонований доступ до неї окремих осіб чи груп осіб можуть призвести як до людських жертв, так і до виникнення різних утруднень при ліквідації наслідків надзвичайної ситуації, по-в'язаних з особливостями інформаційного впливу в екстремальних умовах: переміщення великих мас людей через психічний стрес; швидкого виникнення та поширення серед людей паніки й безпорядків на підставі чуток, помилкової чи недостовірної інформації.

До специфічних для даних умов напрямів забезпечення інформаційної безпеки належать:

розробка ефективної системи моніторингу об'єктів підвищеної небезпеки, порушення функціонування яких може призвести до виникнення надзвичайних ситуацій, і прогнозування надзвичайних ситуацій;

удосконалення системи інформування населення про загрози виникнення надзвичайних ситуацій, про умови їхнього виникнення.

Висновки та напрями подальших досліджень. Проблема державного регулювання в галузі забезпечення інформаційної безпеки при надзвичайних ситуаціях має комплексний характер і включає в себе регулювання питань законодавства.

Питання забезпечення безпеки інформаційної системи попередження і ліквідації наслідків надзвичайних ситуацій, а також системи збору, обробки, обміну та видачі інформації у сфері захисту населення і територій від надзвичайних ситуацій природного і техногенного характеру, законодавчо не визначені, не відображені в нормативно-правових актах, що регулюють діяльність підрозділів Державної служби з надзвичайних ситуацій України.

Державне регулювання технічного захисту інформації та інформаційної безпеки в умовах надзвичайних ситуацій є самостійною складовою інформаційної безпеки в цілому, що здійснюється в рамках реалізації державної політики в галузі забезпечення інформаційної безпеки. Норми, які регламентують правове забезпечення інформаційної безпеки в умовах надзвичайних ситуацій утворюють правовий інститут комплексного характеру, і регулюють суспільні відносини щодо захисту національних інтересів в інформаційній сфері (життєво важливих інтересів особистості, суспільства і держави на збалансованій основі) від загроз в умовах надзвичайних ситуацій.

Напрямом подальшого дослідження є обґрунтування пропозицій щодо вдосконалення чинного законодавства в галузі забезпечення інформаційної безпеки при захисті

населення і територій від надзвичайних ситуацій природного і техногенного характеру.

Список використаних джерел

1. Чмир Я. І. Проблеми забезпечення інформаційної безпеки в системі публічного управління. *Аспекти публічного правління*. 2018. Т. 6. № 9. С. 16–22.
2. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України. Одеса: Юридична література, 2003. 314 с.
3. Шатун В. Т. Інформаційна безпека – невід'ємна складова національної безпеки України. *Наукові праці. Державне управління*. 2016. Т. 267. Вип. 255. С.174–180.
4. Волянський П. Б. Управління інформаційною безпекою медичних установ у межах медичного захисту за умов надзвичайних ситуацій мирного характеру. *Теоретичні і прикладні питання державного будівництва*. Одеса. 2012. URL : http://www.nbuv.gov.ua/e-journals/tppd/2012_10/zmist/R_ 2/021%20Volianskiy.pdf (дата звернення: 18.08.2020).
5. Гур'єв С. О., Терент'єва А. В., Волянський П. Б. Кризовий менеджмент та принципи управління ризиками в процесі ліквідації надзвичайних ситуацій : монографія. ІДУЦЗ. К., 2008. 148 с.
6. Тихомиров О. О. Класифікації забезпечення інформаційної безпеки. *Вісник Запорізького національного університету. Юридичні науки.* 2011. № 1. С. 164–169.
7. 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 № 47/2017 // База даних "Законодавство України" / ВР України. URL : https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 18.07.2020).
8. Барило О. Г. Оцінювання обсягу корисної інформації органами державного управління у надзвичайних ситуаціях. *Економіка та держава*. 2011. № 3. С. 147–148.

9. Єременко С. А. Правові засади інформаційного забезпечення єдиної державної системи цивільного захисту України. *Інформація і право*. 2017. № 3(22). С. 117–123.
10. Кодекс цивільного захисту України : закон України від 02.10.2012 р. № 5403-VI. // База даних "Законодавство України" / ВР України. URL : http://zakon1.rada.gov.ua/laws/show/5403-17 (дата звернення: 24.07.2020).
11. Про затвердження Положення про Державну службу України з надзвичайних ситуацій : Постанова Кабінету Міністрів України від 16 .12.2015 №1052 // База даних «Законодавство України» / ВР України. URL : https://zakon.rada.gov.ua/laws/show/1052-2015-%D0%BF#Text (дата звернення : 20.10.2020).

References

1. Chmyr Ya. I. (2018). Problemy zabezpechennya informacijnoyi bezpeky v systemi publichnogo upravlinnya [Problems of information security in the system of public administration]. *Aspekty publichnoho pravlinnia – Aspects of public administration*, vol. 6, 9, 16–22 [in Ukrainian].
2. Kormych, B. A. (2003). *Orhanizatsiino-pravovi zasady polityky informatsiinoi bezpeky Ukrainy [Organizational and legal bases of information security policy of Ukraine]*. Odesa: Yurydychna literature [in Ukrainian].
3. Shatun V. . (2016). Informatsiina bezpeka – nevidiemna skladova natsionaln oi bezpeky Ukrainy [Information security is an integral part of Ukraine's national security]. *Naukovi pratsi. Derzhavne upravlinnia – Scientific works. Public administration*, vol. 267, issue 255, 174–180 [in Ukrainian].
4. Volianskyi P. B. (2012). Upravlinnia informatsiinoiu bezpekoiu medychnykh ustanov u mezhakh medychnoho zakhystu za umov nadzvychainykh sytuatsii myrnoho kharakteru [Management of information security of medical institutions within the framework of medical protection in conditions of peaceful emergencies]. *Teoretychni i prykladni pytannia derzhavnoho budivnytstva – Theoretical and applied issues of state building*, 10. Retrived from http://www.nbuv.gov.ua/e-journals/tppd/2012_10/zmist/R_ 2/021%20Volianskiy.pdf [in Ukrainian].

5. Huriev, S. O., Terentieva, A. V., Volianskyi, P. B. (2008). *Kryzovyi menedzhment ta pryntsypy upravlinnia ryzykamy v protsesi likvidatsii nadzvychainykh sytuatsii [Crisis management and principles of risk management in the process of emergency response]*. Kyiv: N.p. [in Ukrainian].
6. Tykhomyrov O. O. (2011). Klasyfikatsii zabezpechennia informatsiinoi bezpeky [Classifications of information security]. *Visnyk Zaporizkoho natsionalnoho universytetu. Yurydychni nauky – Bulletin of Zaporizhzhia National University. Legal sciences*, 1, 164–169 [in Ukrainian].
7. Ukaz Prezydenta Ukrainy : Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy» vid 29 grud. 2016 roku № 47/2017 [Decree of the President of Ukraine: On the decision of the National Security and Defense Council of Ukraine of December 29, 2016 "On the Doctrine of Information Security of Ukraine" from December 29 2016, № 47/2017]. Retrived from https://zakon.rada.gov.ua/laws/show/47/2017#Text (2020, July 18) [in Ukrainian].
8. Barylo O. H. (2011). Otsiniuvannia obsiahu korysnoi informatsii orhanamy derzhavnoho upravlinnia u nadzvychainykh sytuatsiiakh [Estimation of the amount of useful information by public administration bodies in emergencies]. *Ekonomika ta derzhava – Economy and state*, 3, 147–148 [in Ukrainian].
9. Yeremenko S. A. (2017). Pravovi zasady informatsiinoho zabezpechennia yedynoi derzhavnoi systemy tsyvilnoho zakhystu Ukrainy [Legal bases of information support of the unified state system of civil protection of Ukraine]. *Informatsiia i pravo – Information and law*, 3(22), 117–123 [in Ukrainian].
10. Zakon Ukrainy : Kodeks tsyvilnoho zakhystu Ukrainy vid 2 zhov. 2012 roku № 5403-VI [Code of Civil Protection of Ukraine from October 2 2012, № 5403-VI]. Retrived from http://zakon1.rada.gov.ua/laws/show/5403-17 (2020, July 24) [in Ukrainian].

THE CONCEPT OF ENSURING INFORMATION SECURITY IN THE CONDITIONS OF EMERGENCIES

Usyk Svitlana, Postgraduate, Institute of Public Administration and Research in Civil Protection, 04074, Kyiv, Rybalska str., 18, tel. 098 03 96 700, e-mail usicom@ukr.net,

Abstract. Information security in the system of public administration is a component of the national security of Ukraine, which provides protection of the public administration system from information and communication threats and challenges. The author considers information as a basis for safe and rational development of the modern information society. At the same time, information can serve as a weapon that affects the human worldview, population, forms a negative attitude to certain phenomena, to the state and society as a whole, distorts facts and events that affect the quality and effectiveness of modern reforms in society and more. The systemic nature of information security allows us to define its provision as a complex activity that makes special demands on its structural characteristics. Research have not developed a generally accepted mechanism for structuring information security. One of the priorities of Ukraine's security policy should be to increase the security and resilience of civil protection in relation to the full range of threats and risks, as critical infrastructure provides vital services and functions for the population, society and state, without which their safe existence and well-being are impossible, as well as the appropriate level of national security. The analysis of the state of legal support of technical protection of information and information security of Ukraine in emergencies allows us to conclude that the choice of objects of legal regulation in the sphere of combating threats to national security in the information sphere, lack of coherence of legal mechanisms used, lack of efficiency, and, most often, the contradictions of the legal norms used by them. Issues of security of the information system of prevention of emergencies and their consequences, as well as the system of collection, processing, exchange and issuance of information in the sphere of protection of population and territories from emergencies of natural and man-made nature, are not legally reflected in regulations governing the State Emergency Service of Ukraine. In this regard, the paper formulates proposals for improving the current legislation in the sphere of information security in the protection of the population and territories from emergencies of natural and man-made nature.

Key words: information, security, emergency, management, civil protection.