

УДК 623.618

DOI: 10.15587/2523-4153.2018.126525

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ ОЦІНКИ РІВНЯ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ В ПРОЦЕСАХ СЛУЖБОВО-БОЙОВОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

©О. В. Орел, А. С. Мідіна

Стаття присвячена комплексному дослідженню адміністративно-правових засад оцінки рівня ризиків безпеки інформації в процесах службово-бойової діяльності Національної гвардії України. Окреслений арсенал методів аналізу та оцінки ризиків, а також визначено шкалу оцінки рівня ризик-ситуацій. Акцентовано увагу на проблемних питаннях, які виникають на сучасному етапі розвитку держави

Ключові слова: адміністративно-правові засади, Національна гвардія України, оцінка, рівень ризику, безпека інформації

1. Вступ

Ускладнення воєнно-політичної ситуації після Революції Гідності кардинально вплинули на розвиток та функціонування всіх без винятку правоохоронних органів. Особливо суттєвих змін зазнали положення нормативно-правових актів, які визначають напрями діяльності військових формувань, органів захисту, охорони правопорядку та територіальної цілісності держави.

У ч. 3 ст. 17 Конституції України проголошено, що забезпечення державної безпеки і захист державного кордону України покладається на відповідні військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом [1]. Так, під час суттєвих перетворень 2014 року (Революції Гідності) на базі органу сил внутрішньої безпеки країни – Внутрішніх військ МВС України – було створено за європейською моделлю потужне військове формування з правоохоронними функціями – Національну гвардію України (далі – НГУ), здатну виконувати службово-бойові завдання, у тому числі правоохоронні функції, як в умовах мирного часу, так і в умовах запровадження правового режиму надзвичайного та/або воєнного стану [2]. Дані зміни вражаюче вплинули не лише на структуру, а й на свідомість громадян.

Відповідно до ст. 1 Закону України «Про Національну гвардію України» НГУ є військовим формуванням з правоохоронними функціями, що входить до системи Міністерства внутрішніх справ України, яке призначено для виконання завдань із захисту та охорони життя, прав, свобод і законних інтересів громадян, суспільства і держави від злочинних та інших протиправних посягань, охорони громадського порядку та забезпечення громадської безпеки тощо [3]. Виконуючи покладені завдання, НГУ в процесах своєї службово-бойової діяльності (далі – СБД), постійно стикається з циркуляцією значного обсягу інформації, який по мірі накопичення та систематизації складає визначену цінність, що привертає увагу різного роду зловмисників. Внаслідок чого, виникає необхідність у чіткій оцінці рівня ризиків безпеки інформації, що обумовлює актуальність визначеної тематики. Наголошення на основних принципах і підходах, які використовую-

ються у практичній діяльності, складають новизну обраної тематики.

2. Літературний огляд

Науково-теоретичним підґрунтям роботи стали наукові праці вчених у галузі адміністративного, конституційного права, національної безпеки, безпеки інформації та інших. Так, на нашу думку, слушно посылитися на висловлення О. В. Олійника щодо поняття адміністративно-правових засобів забезпечення інформаційної безпеки України, який зазначає, що практичне застосування методів захисту інформації завжди зумовлене: важливістю інформації та її носіїв (ступенями секретності, конфіденційності); реальними та потенційними загрозами для конкретного виду інформації з обмеженим доступом; умовами розташування режимних об'єктів, службових приміщень, технічних засобів обробки інформації та робочих місць працівників, діяльність яких пов'язана з державною таємницею та іншою інформацією з обмеженим доступом [4, с.108].

Л. Г. Чистоклетов, О. Л. Хитра опрацювали питання щодо адміністративно-правових засобів у забезпеченні інформаційної безпеки України, де визначили їх як сукупність прийомів і способів, урегульованих нормами права, спрямованих на убезпечення безпеки інформації, які виражаються в інструментах і діяннях, за допомогою яких задовольняються інтереси суб'єктів права з метою удосконалення інформаційного простору [5].

Однак, вказані роботи не розкривають змісту адміністративно-правових засад оцінки рівня ризиків безпеки інформації в процесах СБД НГУ, що створює нішу для подальших наукових досліджень.

3. Мета та задачі дослідження

Метою статті є розкриття, на підставі узагальнення теоретичних положень юридичної науки, норм чинного законодавства України і практики його застосування, загальних аспектів оцінки ризик-ситуацій в процесах службово-бойової діяльності НГУ.

Для досягнення мети були поставлені наступні задачі:

– сформулювати авторське бачення адміністративно-правових засад рівня ризиків безпеки інформа-

ції в процесах службово-бойової діяльності Національної гвардії України;

– виокремити з множинних методів аналізу ризикових ситуацій, найбільш доцільні для використання в СБД НГУ;

– сформулювати пропозиції щодо оцінки ефективності проведення заходів по зниженню ризиків витоку службової інформації.

4. Розроблення модифікованої методики аналізу та оцінки ризику безпеки інформації в процесах СБД НГУ

Як відомо, сучасний світ характеризується постійно зростаючими можливостями отримання, зберігання та обробки інформації за допомогою технічних засобів. Так, за останні десятиріччя стали доступними для переважної більшості населення електронно-обчислювальні машини, зокрема портативні – ноутбуки, планшетні комп'ютери тощо; засоби, що забезпечують мобільний зв'язок, вихід до мережі Інтернет за допомогою бездротового доступу – мобільні модеми та термінали. Крім цього, суттєво зросли обсяги засобів для зберігання інформації (флеш-диски, SSD-диски, мобільні HDD-диски, постійна пам'ять портативних комп'ютерів) та швидкість запису та зчитування. Тобто створені всі передумови для суттєвого збільшення обсягів різноманітної інформації, що зберігається на різних носіях та циркулює у локальних та глобальних інформаційних мережах. Дані обставини на пряму переплітаються з потребами НГУ в цілому та її підрозділами зокрема, а саме в оперативному отриманні та обробці великих обсягів інформації.

Відповідно до Закону України “Про захист інформації в автоматизованих системах” для забезпечення розмежування доступу (ст. 6) та захисту (ст. 10) інформації в автоматизованих системах, власник автоматизованої системи (далі – АС) встановлює певні правила [6], порушення яких може призвести до знищення, модифікації та витоку інформації, незаконного обмеження прав окремих користувачів автоматизованої системи.

Ст. 11 цього ж закону наголошує, що вимоги й правила щодо захисту інформації, яка є власністю держави, або інформації, захист якої гарантується державою, встановлюються державним органом, уповноваженим Кабінетом Міністрів України. Вимоги й правила є обов'язковими для власників АС, де така інформація обробляється, і мають рекомендаційний характер для інших суб'єктів права власності на інформацію.

На підставі вищевикладеного можна зробити висновок, що сучасний суспільно-політичний стан в державі вимагає від представників НГУ постійного підвищення умов збереження інформації з обмеженим доступом, де однією з проблем виступає протиріччя між постійно зростаючими потребами та можливостями користувачів у зберіганні та обробці інформації з одного боку, та необхідністю її збереження – з іншого. У таких умовах існуючі способи забезпечення збереження інформації не є ефективними, оскільки обумовлені низкою чинників.

По-перше – не завжди правильно та обґрунтовано відноситься та чи інша інформація до певної групи обмеження – завищення грифу документа. Даний чинник пов'язаний з тим, що іноді таємними вважаються титульні листи таємних документів або документи з посиланнями на таємні документи, які при цьому не несуть таємної інформації відповідно до ЗВДТ. Також слід враховувати той факт, що деякі типові документи, які в одному відомстві не мають обмежень в доступі до них, в інших вважаються для службового користування (далі – ДСК) або таємними, що є не логічним. В результаті чого, у користувачів формується певна зневага до грифу документа.

По-друге – працівник не завжди усвідомлює реальну різницю між ДСК та конфіденційною інформацією, а іноді і між таємною та ДСК. Наприклад, відомості про технології подвійного призначення, що мають перевагу в порівнянні з кращими зарубіжними аналогами. В цьому випадку, якщо вони дають змогу відтворення технологій, то рахуються таємними (ЗВДТ, наказ СБУ № 440 від 12.08.2005), а у випадку, не можливості відтворення цих технологій – ДСК (Перелік відомостей, що становлять службову інформацію в системі МВС України, наказ МВС № 423 від 14.05.2012). Іншими словами, за таких умов, виконавець документу не завжди може надійно оцінити можливість відтворення технологій із-за відсутності інформації щодо рівнів розвитку технологій у країнах світу.

У наказі МВС від 26.12.2016 № 1352, що змінив наказ МВС № 423 від 14.05.2012, викладені більш узагальнюючі визначення. Так наприклад, у сфері науково-дослідної діяльності службовою є інформація, що розкриває внутрішньовідомчу службову кореспонденцію, доповідні записки та іншу інформацію щодо змісту і результатів виконання окремих науково-дослідних та дослідно-конструкторських робіт, пов'язаних з розробленням, виготовленням, випробовуваннями, упровадженням, дослідною експлуатацією деяких зразків озброєння, військової та спеціальної техніки, проведенням заходів щодо боротьби зі злочинністю, удосконаленням форм і методів використання конкретних службово-бойових завдань тощо, за винятком відомостей, які віднесені до державної таємниці. Слова “окремі”, “деякі”, “тощо” суттєво розширюють коло питань щодо можливості віднесення їх до інформації ДСК та стирають межу між ДСК-інформацією та іншими видами інформації.

По-третє – складність поєднання у свідомості людини інформації з різним ступенем обмеження (ОВ, ЦТ, Т, ДСК, конфіденційна), як такої, виток якої є не припустимим. Відповідно виникає проблема рівнозначного відношення до інформації незалежно від грифу її розрізнення, тобто, на практиці розмиваються межі між групами інформації з різним ступенем обмеження, а через необхідність постійної роботи з великими обсягами інформації виникає небезпека її випадкового витоку.

По-четверте – не чітко визначено поняття “конфіденційна інформація”. Відповідно до п. 2 ст.

21 Закону України “Про інформацію” “конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом” [7]. Що стосується конфіденційної інформації юридичної особи, то це поняття у юридичній науці визначено розмито.

По-п’яте – не визначено терміни дії відомостей, які становлять службову інформацію, що не дозволяє своєчасно переглянути необхідність обмеження доступу до такої інформації.

По-шосте – не однакова структура переліків відомостей, які становлять інформацію з обмеженим доступом, що суттєво уповільнює їх одночасний аналіз на етапі визначення грифу інформації. Таким чином, створюються передумови для здійснення помилок при виконанні цього напрямку роботи.

Ризик – являє собою кількісну оцінку небезпеки тобто частоту реалізації небезпеки [8]; векторну величину з такими основними показниками, як величина шкоди від впливу того чи іншого небезпечного фактору, вірогідність виникнення небезпечного фактору, невизначеність у величинах – шкоди та вірогідності.

Сьогодні арсенал методів аналізу та оцінки ризиків достатньо великий. Серед них хотілося би виділити: статистичні методи оцінки; методи експертних оцінок; аналітичні методи (аналіз чутливості, аналіз доцільності витрат тощо); метод аналогій; методи аналізу сценаріїв розвитку; комбіновані методи. Однак, для обґрунтування рішень в умовах переваги невизначеності та ризику зазвичай використовують: ігрові моделі, методи експертних оцінок, методи, засновані на людино-машинних процесах.

Перелічені методи аналізу ризикових ситуацій не завжди можуть бути застосовані до діяльності Національної гвардії України з ряду причин:

- із-за нечіткого збору та обробки інформації, необхідної для аналізу ризикової ситуації;
- критерії оцінки носять узагальнений характер і не дозволяють судити про зовнішні та внутрішні фактори прояву ризикової події;
- недостатньої активності теорії і практики по розробці рекомендацій щодо аналізу та оцінки конкретних видів ризиків, та їх впровадженню до діяльності НГУ.

Саме тому математичний апарат багатьох методів оцінки ризику практично не використовується у прийнятті рішень щодо практичної діяльності НГУ. Для керівника особливе значення набуває попередній аналіз можливої ризикової ситуації. Для цього, на

нашу думку, необхідним є проведення кількісного та якісного аналізу ризикових ситуацій (їх факторів і причин).

Опрацьовані матеріали дали поштовх до розробки модифікованої методики аналізу та оцінки ризику, сутність якої полягає у виявленні ризик-факторів діяльності НГУ та розрахунку коефіцієнтів ризику за його видами (правомірний, допустимий, неправомірний), ступенем припустимості (виправданий, не виправданий, політичний, фізичний, економічний). У результаті її використання ми отримуємо значення коефіцієнтів ризику у розрізах за видами та ступенем припустимості, а також значення узагальненого показника – коефіцієнта загального (сукупного) ризику.

Для інтерпретації інформації про ризик-ситуації, в діяльності НГУ, значення коефіцієнта ризику ранжирують за рівнем впливу на кінцеві результати діяльності з використанням так званих шкал ризику, які дозволяють по значенню коефіцієнтів ризику на кількісно-якісному рівні виявляти рівень впливу ризику на військове формування з правоохоронними функціями.

У науковій літературі не має єдиного підходу до формулювання та критеріїв оцінки шкали ризику. Різноманіття показників, за допомогою яких здійснюється ризик-оцінка, породжує й багатоманітність шкал ризику, які, у свою чергу, є рекомендаціями припустимості того чи іншого рівня ризику.

Виходячи з вищезазначеного та особливостей діяльності Національної гвардії України, нами запропонована шкала ризику [9], що буде доцільна для застосування в діяльності НГУ [10] в якості оцінки критичності ризикових подій, які аналізуються [11, 12]. Дана шкала побудована на основі пофакторної оцінки внутрішніх ризиків із використанням комплексу прийомів аналітичного та евристичного методів. У результаті використання запропонованої нами модифікованої методики аналізу та оцінки ризику до конкретного процесу СБД НГУ ми отримуємо значення поодиноких коефіцієнтів ризику за його видами (правомірний, допустимий, неправомірний) та ступенем припустимості (виправданий, не виправданий, політичний, фізичний, економічний), які розташовуються в межах інтервалу від 0 до 1, а також величину загального (сукупного) коефіцієнту ризику, що розташовується в інтервалі від 0 до 3, оскільки процеси СБД НГУ, знаходяться одночасно під впливом правомірного, допустимого, неправомірного, виправданого, не виправданого, політичного, фізичного та економічного ризик-факторів. Використовуючи прийом інтервальної оцінки результативного параметру запропонована до практичного застосування шкала оцінки рівня ризику має наступний вигляд (табл. 1).

Таблиця 1

Шкала оцінки рівня ризику процесів службово-бойової діяльності Національної гвардії України

Значення коефіцієнту ризику	Значення сукупного (загального) коефіцієнту ризику	Рівень ризику
0,0–0,29	0,0–0,3	Незначний (мінімальний) ризик
0,3–0,39	0,31–0,9	Прийнятний (допустимий) ризик
0,4–0,59	0,91–1,5	Високий ризик
0,6–0,79	1,51–2,0	Максимальний (критичний) ризик
0,8–1,0	2,1–3,0	Катастрофічний (недопустимий) ризик

У результаті отримуємо комплексний підсумковий показник ризику, який побудований на кількісно-якісному аналізі та оцінці ризик-ситуації.

Як вже зазначалося вище, запропонована шкала може бути використана та адаптована до будь-яких умов діяльності. Особливістю у разі адаптування повинні стати напрямки та умови діяльності конкретного відомства (установи, організації), а також безпосередня участь експертів даної організації (установи, відомства). При побудові – доцільно використовувати таку інформацію, як узагальнені значення коефіцієнтів; коефіцієнти, засновані на статистичних даних результатів діяльності та значення коефіцієнтів, які розроблені експертами.

5. Результати досліджень

На сьогоднішній день нагальна потреба для юридичної науки – дати відповідь на питання, які встануть в процесі оцінки ризик-ситуацій в процесах службово-бойової діяльності НГУ, оскільки наука і понині не дала однозначної бази щодо методів аналізу та оцінки ефективності проведення заходів по зниженню ризиків витоку службової інформації.

В перспективах дослідження даної проблеми пропонуємо розглянути рівень юридичної відповідальності за порушення в сфері витоку службової інформації.

6. Висновки

1. Сформовано авторське бачення адміністративно-правових засад рівня ризиків безпеки інформації в процесах службово-бойової діяльності Національної гвардії України як сукупність прийомів і способів, урегульованих нормами права, спрямованих на

захист безпеки інформації, визначення рівня кількісно-якісної оцінки небезпеки в процесах службово-бойової діяльності Національної гвардії України, що виражаються в інструментах і діяннях, за допомогою яких задовольняються інтереси суб'єктів права з метою удосконалення інформаційного простору.

2. Серед множинних методів аналізу ризик-ситуацій, з врахуванням конкретних обставин подій, найбільш доцільними для використання в СБД НГУ є: статистичні методи оцінки; методи експертних оцінок; аналітичні методи; метод аналогій; методи аналізу сценаріїв розвитку; комбіновані методи. Для обґрунтування рішень в умовах переваги невизначеності та ризику – ігрові моделі, методи експертних оцінок, а також методи, засновані на людиномашинних процесах.

3. Запропонована модифікована методика аналізу та оцінки ризику, сутність якої полягає у виявленні ризик-факторів діяльності НГУ та розрахунку коефіцієнтів ризику за його видами (правомірний, допустимий, неправомірний), ступенем припустимості (виправданий, не виправданий, політичний, фізичний, економічний), отриманні значення коефіцієнтів ризику у розрізах за видами та ступенем припустимості, а також значення узагальненого показника – коефіцієнта загального (сукупного) ризику, може бути використана та адаптована до будь-яких умов діяльності відомства (установи, організації).

4. Заходами щодо оцінки ефективності зниження ризиків витоку службової інформації можуть стати міроприємства, направлені на юридичне узагальнення між відомствами (установами, організаціями) типових документів з відповідним грифом розрізнення.

Література

1. Конституція України: Закон України від 28.06.1996 // Відомості Верховної Ради України. 1996. № 30. Ст. 141. URL: <http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>
2. Пояснювальна записка до проекту Закону України «Про Національну гвардію України» від 11.03.2014. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=50122 (Дата звернення: 10.01.2018)
3. Про Національну гвардію України: Закон України від 13.03.2014 № 876- VII // Відомості Верховної Ради України. 2014. № 17. Ст. 594. URL: <http://zakon5.rada.gov.ua/laws/show/ru/876-18>
4. Олійник О. В. Методологічні засади забезпечення системи інформаційної безпеки та її складової – захисту інформаційних ресурсів // Право і безпека. 2014. № 1 (52). С. 103–109.
5. Чистоклетов Л. Г., Хитра О. Л. Адміністративно-правові засоби у забезпеченні інформаційної безпеки України: конф. // ІТ право: проблеми і перспективи розвитку в Україні. Львів, 2017. URL: <http://aphd.ua/publication-217/>
6. Про захист інформації в автоматизованих системах: Закон України від 05.07.1994 // Відомості Верховної Ради.

1994. № 31. Ст. 286. URL: <http://zakon5.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>

7. Про інформацію: Закон України від 02.10.1992. № 2657-XII // Відомості Верховної Ради. 1992. № 48. Ст. 650. URL: <http://zakon0.rada.gov.ua/laws/show/2657-12>

8. Визначення ризику та методи його оцінки // Студопедия. URL: http://studopedia.su/10_10258_visnachennya-riziku-ta-metodi-yogo-otslnki.html (Дата звернення: 10.01.2018)

9. Измайлович С. В. Использование шкалы риска в процессе оценки риск-ситуаций. Новополоцк: УО Полоцкий государственный университет, 2010.

10. Про військовий обов'язок і військову службу: Закон України від 25.03.1992. № 2232-XII // Відомості Верховної Ради України. 1992. № 27. Ст. 385. URL: <http://zakon5.rada.gov.ua/laws/show/2232-12>

11. Про правовий режим воєнного стану: Закон України від 12.05.2015. № 389-VIII // Відомості Верховної Ради України. 2015. № 28. Ст. 250. URL: <http://zakon5.rada.gov.ua/laws/show/389-19>

12. Про правовий режим надзвичайного стану: Закон України від 16.03.2000. № 1550-III // Відомості Верховної Ради України. 2000. № 23. Ст. 176. URL: <http://zakon0.rada.gov.ua/laws/show/1550-14>

*Рекомендовано до публікації д-р юрид. наук, професор Матюхіна Н. П.
Дата надходження рукопису 20.02.2018*

Орел Оксана Вікторівна, кандидат юридичних наук, доцент, кафедра соціально-гуманітарних дисциплін, Національна академія Національної гвардії України, майдан Захисників України, 3, м. Харків, Україна, 61001

E-mail: kafedra.tulz11@gmail.com

Мідіна Анастасія Сергіївна, Національна академія Національної гвардії України, майдан Захисників України, 3, м. Харків, Україна, 61001

E-mail: amidina@ukr.net

УДК 343.131(477)

DOI: 10.15587/2523-4153.2018.127167

ПРОЦЕСУАЛЬНИЙ СТАТУС ЗАХИСНИКА ЗА КПК УКРАЇНИ: ПРОБЛЕМИ РЕГЛАМЕНТАЦІЇ ТА ШЛЯХИ ЇХ УДОСКОНАЛЕННЯ

© С. Є. Абламський

Статтю присвячено проблемним питанням правового регулювання статусу захисника у кримінальному провадженні, визначенню основних особливостей процесуального статусу захисника, та його структурних компонентів у руслі сучасного законодавчого регулювання, а також з'ясуванню його функціонального призначення. Наголошено на необхідності закріплення в окремій статті КПК України процесуальних прав захисника як самостійного учасника кримінального провадження

Ключові слова: кримінальне провадження, процесуальний статус, захисник, адвокат, сторона захисту, обов'язки, права

1. Вступ

Сучасні соціально-економічні процеси, що відбуваються в Україні у результаті євроінтеграції, створили передумови для запровадження загальновищаних міжнародних правових стандартів захисту прав і свобод людини. З огляду на це урядом нашої країни проводиться концептуальне оновлення національного законодавства, в тому числі кримінального процесуального. Натомість аналіз чинного Кримінального процесуального кодексу України 2012 року (далі – КПК України) свідчить про те, що законодавча регламентація процесуального статусу захисника як учасника кримінального провадження залишається недостатньо врегульованою, оскільки в його положеннях відсутня окрема стаття, в якій би чітко були визначені права та обов'язки захисника. Зазвичай під процесуальним статусом розуміється становище того чи іншого суб'єкта в правовій реальності, що відображається у взаєминах з іншими учасниками та державою загалом, тобто його правосуб'єктність.

2. Літературний огляд

Деякі науковці [1–3] розглядали окремі проблемні питання правового статусу захисника та його участі в кримінальному провадженні. Інші вчені [4–6] присвятили свої дослідження розмежуванню невід'ємних прав підозрюваного та його захисника, і тому лише побічно торкалися процесуального статусу захисника. Окремо слід виокремити праці правників [7, 8], які здійснили комплексне дослідження кримінальних процесуальних гарантій діяльності захисника-адвоката та надання їм правової допомоги у кримінальному провадженні.

Отже, всі наукові ідеї та позиції вчених мають важливе значення, адже спрямовані на удосконалення різних аспектів процесуального статусу захисника як учасника кримінального провадження. Проте наукові позиції з окремих питань даної проблематики мають дискусійний характер і потребують свого уточнення. Очевидною є потреба у науковому осмисленні визначення та законодавчого унормування прав