УДК 342.951:351.743(477)

О. В. Орел

А. С. Мідіна

І. В. Євтушенко

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СИСТЕМОУТВОРЮЮЧИЙ ЕЛЕМЕНТ МОДЕЛІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Проведено комплексне дослідження інформаційної безпеки України як системоутворюючого елементу моделі забезпечення національної безпеки України. За результатами дослідження надано авторську позицію стосовно модифікованої методики аналізу й оцінювання рівня ризик-ситуацій у процесах інформаційної безпеки сектору безпеки і оборони, а також внесено конкретні пропозиції щодо змін норм чинного законодавства. Акцентовано увагу на проблемних питаннях, які виникають на сучасному етапі розвитку держави.

Ключові слова: *інформаційна безпека, національна безпека, сектор безпеки і оборони, Національна гвардія України.*

Постановка проблеми. Тривала війна з 2014 р. і повномасштабне вторгнення 24 лютого 2022 р. до України з боку Російської Федерації внесли свої корективи до всіх сфер суспільного життя. Військова сфера не є винятком. Європейські та євроатлантичні стандарти в сучасному розвитку сектору безпеки і оборони України вказують на новий етап реформ сьогодення. Так, Національна гвардія України (НГУ), будучи учасником правовідносин у сфері протидії загрозам національній безпеці України, здійснює діяльність, врегульовану нормами військово-адміністративного права, що ґрунтується і змінюється залежно від адміністративно-правових режимів; має визначені законом повноваження щодо виявлення, відвернення, знищення та зменшення негативного впливу з боку агресора [1, с. 6]. Беручи активну участь в обороні держави, здійснюючи протидію агресору, НГУ сприяє збереженню національної безпеки нашої країни.

З огляду на те, що на території України оголошено правовий режим воєнного стану [2–8], перед нами постають особливі проблеми, притаманні саме цьому періоду: блокування інтернет-ресурсів, надлишкове втручання політики держави, надлишкове маніпулювання мисленням і поведінкою населення за допомогою засобів масової інформації (ЗМІ), пропагандою тощо. З правової позиції це: розпорошеність відповідних норм права у численних нормативно-правових актах; низький рівень правової реалізації; наявність численних бланкетних чи відсильних норм права, понять, базових дефініцій. При цьому підвищення бойового потенціалу і створення ефективного, комплексного та багатофункціонального державного інструментарію для забезпечення національної безпеки країни посідає особливе місце, що дає підґрунтя для широкої академічної дискусії й пошуків найбільш виваженого і збалансованого бачення майбутнього нашої держави.

Аналіз останніх досліджень і публікацій. Науково-теоретичне підґрунтя дослідження у цій статті становлять наукові праці вчених з різних галузей права, а саме М. Бандурки, Ю. Бабкова, Т. Кагановської, О. Сосніна, А. Кулінської, В. Горбуліна, О. Дзьобаня та деяких інших, а також нормативно-правові акти чинного законодавства. Водночас, незважаючи на велику кількість наукових праць стосовно інформаційної безпеки, з питань системоутворюючих елементів моделі забезпечення національної безпеки України та їх впливу на неї є чимало невирішених проблем. Зокрема, недостатньо вивчено закордонний досвід і специфіку превентивних заходів, пов'язаних із загрозами національній безпеці. Крім цього, безпосередньо

адміністративно-правові засади модифікованої методики аналізу й оцінювання рівня ризик-ситуацій у процесах інформаційної безпеки сектору безпеки і оборони з метою їх мінімізації в межах національної безпеки (з урахуванням вітчизняного і світового досвіду) дотепер не були предметом окремого комплексного наукового дослідження. Саме тому теоретична розробка вибраної теми, її наукова новизна, значущість та актуальність у нових реаліях сьогодення набувають особливого змісту і значення.

Мета статті – розробити на основі узагальнення теоретичних положень юридичної науки, норм чинного законодавства України і практики його застосування модифіковану методику аналізу й оцінювання рівня ризик-ситуацій у процесах інформаційної безпеки сектору безпеки і оборони, а також сформулювати пропозиції та рекомендації щодо їх мінімізації в межах національної безпеки з урахуванням вітчизняного і світового досвіду.

Для досягнення поставленої мети зроблено спробу вирішити такі основні завдання:

– сформулювати авторське визначення понять «порушення дефініцій національної безпеки» та її «суспільної небезпечності»;

– надати авторське бачення адміністративно-правових засад модифікованої методики аналізу й оцінювання рівня ризик-ситуацій у процесах інформаційної безпеки сектору безпеки і оборони, а також сформулювати пропозиції та рекомендації щодо їх мінімізації в межах національної безпеки з урахуванням вітчизняного і світового досвіду;

– виокремити основні напрями превентивних заходів, пов'язаних із загрозами національній безпеці.

Об'єктом дослідження є суспільні відносини у сфері національної безпеки України.

Предмет дослідження становлять адміністративно-правові засади інформаційної безпеки як системоутворюючого елементу моделі забезпечення національної безпеки.

Виклад основного матеріалу. Повномасштабне вторгнення 24 лютого 2022 р. до України з боку Російської Федерації показало слабкі та сильні сторони сектору безпеки і оборони нашої країни. Так, розгортання сучасного збройного конфлікту (гібридної війни) відбувається протягом кількох взаємопов'язаних етапів, які мають, в основному, прихований характер і пов'язані єдиною стратегічною метою. Перший етап (підготовчий) гібридної війни – інформаційно-економічний або інноваційних агресій – триває від одного до кількох років, супроводжуючись дипломатичними, інформаційними та економічними війнами. Їх характерними ознаками є прихована експансія в інформаційній та економічних сферах, що супроводжується перерозподілом, рейдерським захопленням або доведенням до банкрутства ЗМІ та державних підприємств. Метою цього етапу є встановлення контролю над ЗМІ та провідними галузями економіки.

На другому етапі за допомогою «асиметричних заходів» відбувається загострення конфліктної ситуації в окремих місцевостях, яке супроводжується дестабілізацією суспільної обстановки, актами сепаратизму та насилля з використанням внутрішньої опозиції, нерегулярних озброєних формувань, приватних армій та підрозділів спеціального призначення. Етап супроводжується переходом до відкритої фази конфлікту і може перейти в офіційний збройний конфлікт, хоча країна-агресор офіційно не проголошує початок війни і заперечує присутність своїх збройних сил.

Головною негативною метою третього етапу (заключного) є легітимізація сепаратизму та анексія територій, яка відбувається під безпосереднім контролем країни-агресора. Проведення референдумів і псевдонародних виборів з подальшим офіційним введенням збройних сил агресора під прапором миротворчих місій є характерними ознаками цього етапу. У разі позитивного розгортання подій відбувається повернення тимчасово окупованої території до складу держави та відновлюється державний кордон.

Наразі ми є свідками третього етапу розгортання збройного конфлікту (гібридної війни). Була змога бачити: під час першого етапу – застосування охоронної функції, під час другого етапу – поступовий перехід від охоронної функції до функції ліквідації наслідків надзвичайних або кризових ситуацій, а потім – і до функцій державної безпеки та спеціальної. З огляду на асиметричне розгортання загроз в умовах внутрішнього збройного конфлікту було одночасне застосування двох і більше функцій. Під час протидії загрозам збройного конфлікту основною функцією стала оборонна. Розгортання третього етапу здійснювалося за негативним напрямком, окрім основної оборонної, важливе значення покладено на охоронну функцію. Систематизацію застосування функцій і законодавства України під час розгортання етапів наведено у табл. 1.

Таблиця 1 – Взаємозв'язок функцій НГУ з етапами службово-бойового застосування та чинними законодавчими нормами в Україні

Етап	Функція	Закон
I	Охоронна	Конституція України; Про Національну гвардію України; Про Національну поліцію; Кримінальний кодекс України; Кримінально-процесуальний кодекс України; Кодекс України про адміністративні правопорушення; Про соціальний і правовий захист військовослужбовців та членів їх сімей
II	Державна безпека; охоронна; ліквідація наслідків надзвичайних або кризових ситуацій; спеціальна; оборонна	Конституція України; Про Національну гвардію України; Про Національну поліцію; Кримінальний кодекс України; Кримінально-процесуальний кодекс України; Кодекс України про адміністративні правопорушення; Про правовий режим надзвичайного стану; Про боротьбу з тероризмом; Про Службу безпеки України; Про військову службу правопорядку у Збройних Силах України; Про оборону; Про правовий режим воєнного стану; Стратегія національної безпеки України; Про державний кордон України; Про соціальний і правовий захист військовослужбовців та членів їх сімей; II протокол від 1977 р. до Женевських конвенцій 1949 р.
III	Охоронна; спеціальна; ліквідація наслідків надзвичайних або кризових ситуацій	Конституція України; Про Національну гвардію України; Про Національну поліцію; Кримінальний кодекс України; Кримінально-процесуальний кодекс України; Кодекс України про адміністративні правопорушення; Про соціальний і правовий захист військовослужбовців та членів їх сімей; Про статус ветеранів війни, гарантії їх соціального захисту

Отже, проведений аналіз засвідчив, що Національна гвардія України є суб'єктом протидії загрозам національній безпеці України; в умовах збройного конфлікту підрозділи НГУ залучаються і застосовуються згідно з нормами чинного законодавства; кожному етапу збройного конфлікту визначено відповідні функції Національної гвардії України та їх правове застосування (див. рис. 1).

Як видно на рис. 1, методи, що забезпечують конфіденційність, цілісність, доступність та технологічну безпеку, реалізуються у межах системи захисту інформації від несанкціонованого доступу інформації, умовно поділяються на 4 підсистеми:

– управління доступом;
– реєстрації та обліку;
– криптографічної;
– забезпечення цілісності.

Тренінг є одним із способів забезпечення превентивних заходів, пов'язаних із загрозами національній безпеці України.

Відповідно до Закону України «Про основи національної безпеки» від 19 червня 2003 р. № 964 національна безпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національним інтересам. Стаття 2 цього ж Закону наголошує, що Президентом України розробляються і затверджуються стратегії, доктрини, концепції, програми тощо.

Доктрина інформаційної безпеки України, яка затверджена Указом Президента України від 25 лютого 2017 р. № 47/2017, розкриває системоутворюючі дефініції, що відображені у табл. 2.

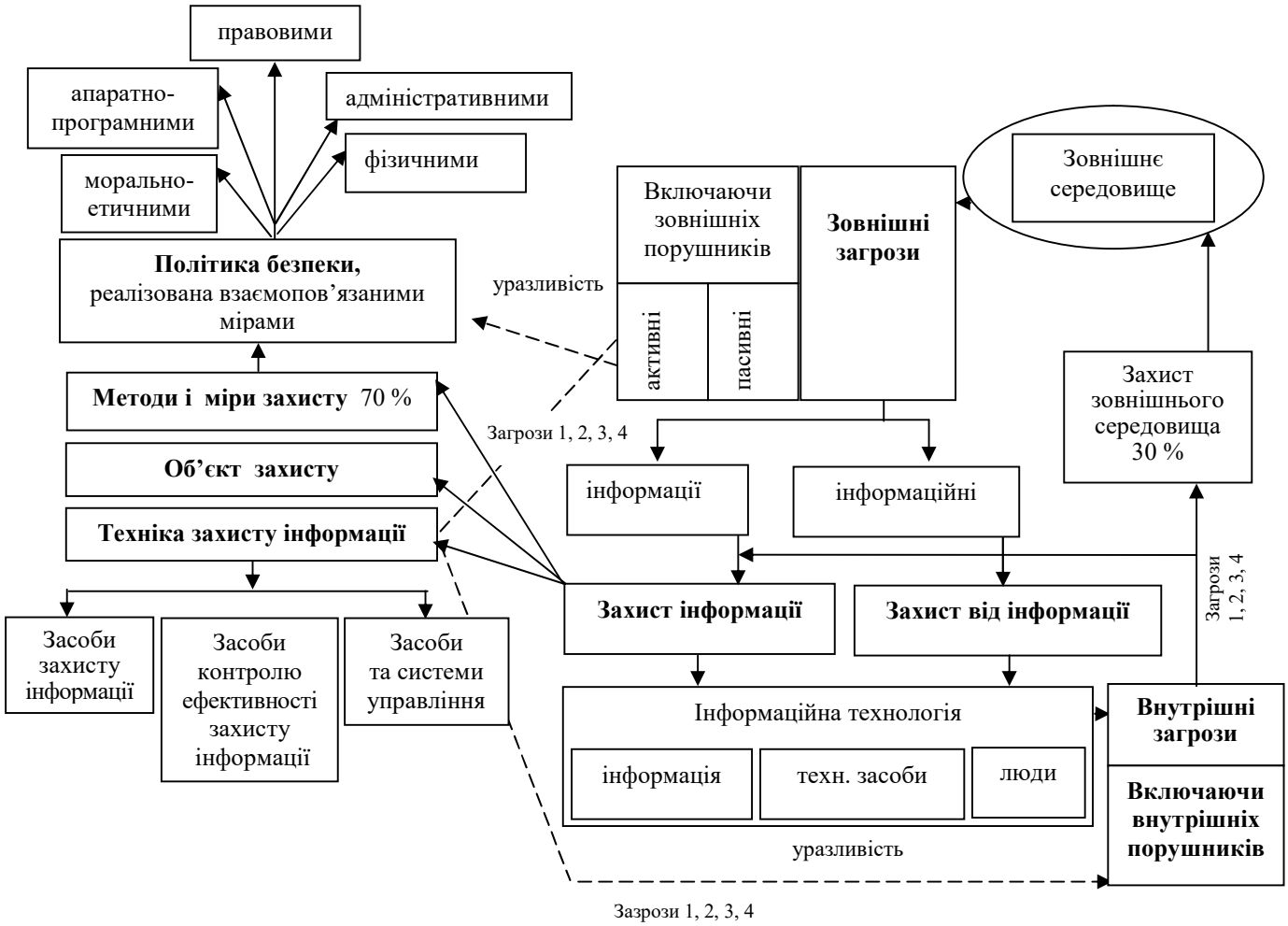

Рисунок 1 – Оцінка потенційних ризиків, пов'язаних із загрозами (система забезпечення інформаційної безпеки): 1 – загрози конфіденційності; 2 – загрози цілісності; 3 – загрози доступності; 4 – загрози технологічної безпеки

Проаналізувавши табл. 2 і рис. 1, зазначимо, що цілісна система інформаційної безпеки повинна передбачати як превентивну (профілактичну), так і внутрішню оперативну роботу. При цьому превентивна робота припускає використання технічних методів і способів контролю; внутрішньо-оперативна робота є процесом виявлення інформації небезпечного характеру.

Етапами формування системи інформаційної безпеки виділено: ідентифікацію джерел загроз і ризиків; оцінювання ступеня серйозності загрози; вибір і застосування оптимального алгоритму локалізації загроз (побудову системи захисту). Проблемами інформаційної безпеки є такі: розпорошеність у численних нормативно-правових актах; низький рівень правової реалізації; наявність численних бланкетних чи відсильних норм права понять, базових дефініцій. У свою чергу, порядкове ранжирування системи інформаційної безпеки процесів службово-бойової діяльності сектору безпеки і оборони у цілому та НГУ зокрема відображено на рис. 2.

Оцінка потенційних ризиків, пов'язаних із загрозами (система забезпечення інформаційної безпеки), що описана моделлю на рис. 1, є доволі стійкою і цим забезпечує стабільність інформаційної безпеки.

Арсенал методів аналізу й оцінювання ризик-ситуацій достатньо великий. Однак, незважаючи на це, опрацьовані матеріали дали поштовх до розроблення модифікованої методики аналізу й оцінювання рівня ризик-ситуацій, сутність якої полягає у виявленні ризик-факторів у процесах інформаційної безпеки (нашої країни у цілому та НГУ зокрема) і розрахунку коефіцієнтів ризику за його видами (правомірний, допустимий, неправомірний), ступенем припустимості (виправданий, не виправданий, політичний, фізичний, економічний).

Таблиця 2 – Системоутворюючі дефініції інформаційної безпеки

<table>
<tr><th>Інформаційна безпека</th><th>Державна політика</th><th>Державна інформаційна політика</th></tr>
<tr><td>Розглядається через призму прав і свобод особи й інформаційної сфери</td><td rowspan="3">Передбачає системну превентивну діяльність органів влади з наданням гарантій, інформаційної безпеки особі, суспільним групам та суспільству в цілому</td><td rowspan="4">Відповідно до ст. 6 Закону України «Про інформацію» є сукупністю основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації і має бути така:
– у мирний час:
основа – свобода слова, обмеження – професійна етика;
– в умовах воєнного часу виникають проблеми:
1) блокування інтернет-ресурсів;
2) надлишкове втручання політики держави;
3) надлишкове маніпулювання мисленням та поведінкою населення за допомогою ЗМІ, інформаційною пропагандою тощо</td></tr>
<tr><td>Інформаційна безпека – комплекс системних превентивних заходів з надання гарантій захисту життєво важливих інтересів особистості, суспільству й державі від негативного інформаційного впливу в економіці, внутрішній і зовнішній політиці, у науково-технологічній, соціально-культурній і оборонній сферах, системах державного управління, державної безпеки, самостійного і незалежного розвитку всіх елементів національного інформаційного простору</td></tr>
<tr><td>Інфопростір. Основні 5 елементів:
– національні ресурси;
– інформаційна інфраструктура;
– інформаційно-телекомунікаційні структури;
– інформаційні технології;
– системи ЗМІ</td><td>Базові закони:
«Про інформацію»,
«Про науково-технічну інформацію»,
«Про національну програму інформатизації»,
«Про Концепцію Національної програми інформатизації»,
«Про поштовий зв’язок» тощо</td></tr>
<tr><td>Безпека інформаційної сфери – стан захищеності інформації та сфери її створення, накопичення, зберігання, оброблення, поширення, використання, тобто сфери її обігу.
Інформаційні впливи – здійснюються на життєво важливі сфери діяльності громадян, суспільства, держави з метою нав’язування визначеної системи цінностей, поглядів і рішень, спрямованих на керування їхньою поведінкою для бажаних трансформацій у політичній, соціальній, економічній та інших напрямах</td></tr>
<tr><td colspan="3">Інформаційне законодавство виступає гарантом державної політики.
Правове відображення інформаційної безпеки – сукупність правових умов, що забезпечують оптимальне функціонування і розвиток суб’єктів в інформаційному середовищі</td></tr>
</table>

У результаті її використання одержуємо значення коефіцієнтів ризику у розрізах за видами і ступенем припустимості, а також значення узагальненого показника – коефіцієнта загального (сукупного) ризику. Для інтерпретації інформації про рівень ризик-ситуації в процесах інформаційної безпеки значення коефіцієнта ризику ранжирують за рівнем впливу на кінцеві результати діяльності з використанням так званих шкал ризику, які дають змогу за значенням коефіцієнтів ризику на кількісно-якісному рівні виявляти рівень впливу ризику на військове формування з правоохоронними функціями. У науковій літературі бракує єдиного підходу до формулювання та критеріїв оцінювання 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.

З огляду на зазначене вище й особливості сектору безпеки і оборони в цілому та НГУ зокрема автори статті запропонували шкалу ризику, що буде доцільною для застосування як оцінка критичності ризикових подій, які аналізуються [9]. Ця шкала побудована на основі пофакторної оцінки внутрішніх ризиків із використанням комплексу прийомів аналітичного та евристичного методів.

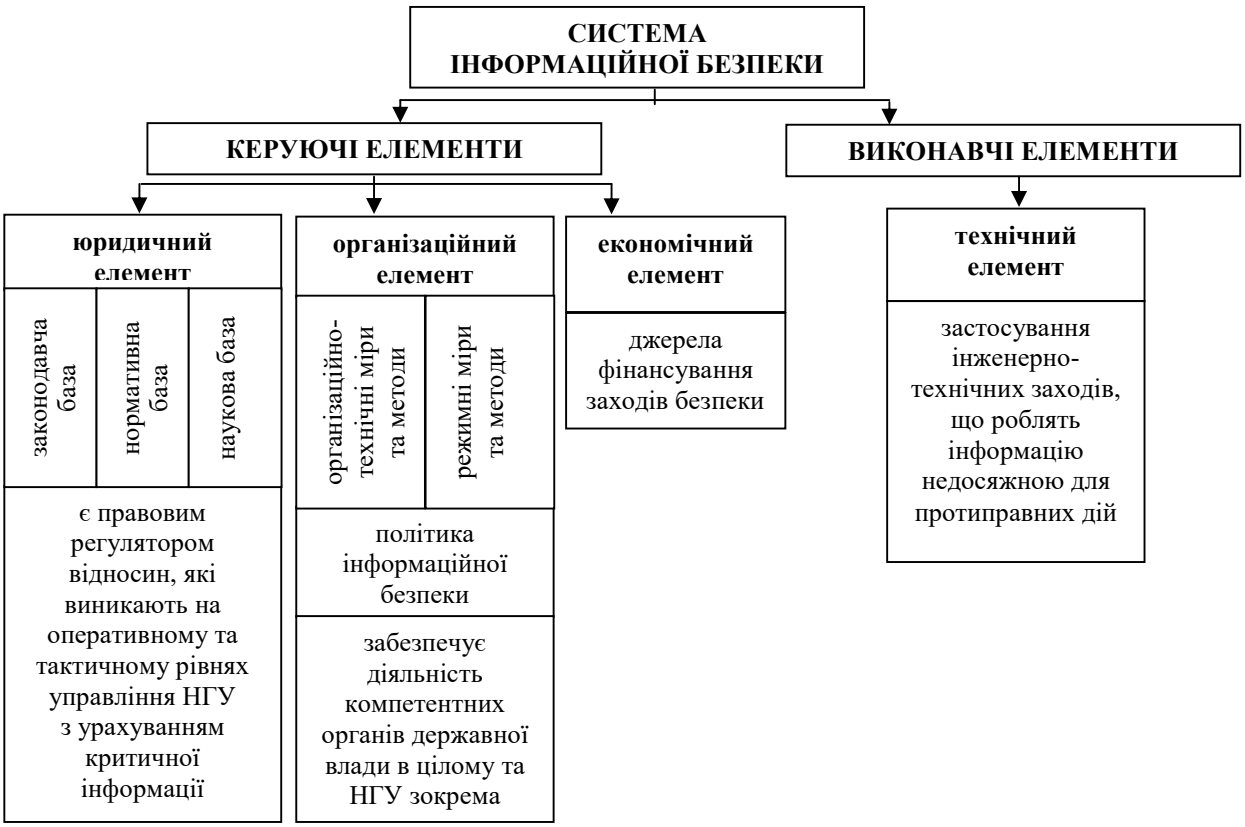

Рисунок 2 – Порядкове ранжирування системи інформаційної безпеки процесів службово-бойової діяльності сектору безпеки і оборони у цілому та НГУ зокрема

У результаті застосування запропонованої модифікованої методики аналізу й оцінювання ризик-ситуацій до конкретного процесу інформаційної безпеки 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) коефіцієнта ризику, що розташовується в інтервалі від 0 до 3, оскільки процеси інформаційної безпеки перебувають одночасно під впливом правомірного, допустимого, неправомірного, виправданого, не виправданого, політичного, фізичного та економічного ризик-факторів.

З використанням прийому інтервальної оцінки результативного параметра запропонована до практичного застосування шкала оцінювання рівня ризику має вигляд, як подано у табл. 3.

У результаті одержуємо комплексний підсумковий показник ризику, який побудований на кількісно-якісному аналізі й оцінці ризик-ситуації. Як уже зазначалося, запропонована шкала може бути використана й адаптована до будь-яких умов діяльності. Особливістю у разі адаптування мають стати напрями й умови діяльності конкретного відомства (установи, організації), а також безпосередня участь експертів цього відомства (установи, організації). У процесі побудови доцільно використовувати таку інформацію, як: узагальнені значення коефіцієнтів; коефіцієнти, що ґрунтуються на статистичних даних результатів діяльності, та значення коефіцієнтів, які розроблені експертами.

Таким чином, проведений аналіз нормативно-правових документів, які визначають рівень ризик-ситуацій у процесах інформаційної безпеки в секторі безпеки і оборони у цілому та НГУ зокрема, а також його оцінку, засвідчив, що: НГУ є суб'єктом протидії загрозам національній безпеці України; модифікована методика аналізу й оцінювання рівня ризик-ситуацій інформаційної безпеки нашої країни полягає у виявленні ризик-факторів у діяльності сектору безпеки і оборони та розрахунку коефіцієнтів ризику за його видами (правомірний, допустимий, неправомірний), ступенем припустимості (виправданий, не виправданий, політичний, фізичний, економічний).

Таблиця 3 – Шкала оцінювання рівня ризику в процесах інформаційної безпеки України

Значення коефіцієнта ризику	Значення сукупного (загального) коефіцієнта ризику	Рівень ризику
0,0 – 0,29	0,00 – 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 – 1,00	2,10 – 3,0	Катастрофічний (недопустимий) ризик

Шляхами поліпшення інформаційної безпеки є такі: забезпечення захисту інформації; захист і контроль національного інформаційного простору; забезпечення належного рівня інформаційної достатності; підвищення інтелектуального (психологічного), політико-ідеологічного, технічного, економічного, соціального фактора відповідно до динамічності інформаційної сфери.

Підтвердженням зазначеного є досвід таких країн, як Франція та Німеччина. Так, нормативно-правове регулювання забезпечення інформаційної безпеки Франції передбачено Білою книгою оборони та національної безпеки – базовим нормативним актом, в якому визначаються стратегічні напрями державної політики Франції у сфері забезпечення безпеки. У ній серед найбільш імовірних загроз територіям Франції та європейській спільноті названі масштабні атаки на інформаційні системи; шпіонаж і стратегічний вплив. Основними шляхами протидії зазначеним загрозам у документі визначено: взаємодію з питань протидії атакам на інформаційні системи, насамперед у межах країн-членів ЄС; проведення як відкритих, так і прихованих активних заходів протидії проявам агресії в інформаційних мережах; підготовку кібервійськ на професійній основі.

Нормативно-правове регулювання забезпечення інформаційної безпеки ФРН передбачено Федеральним законом «Про вдосконалення обробки даних і захисту інформації», який закладає основу для подальшої кодифікації законодавства Німеччини.

Отже, можна з упевненістю стверджувати, що міжнародне співробітництво складає важливу сторону діяльності Національної гвардії України і виступає потужним важелем у підвищенні її іміджу, а також дає можливість модернізувати сучасні національні адміністративно-правові засади та запроваджувати нові міжнародні моделі належного управління.

Висновки

На основі проведеного дослідження, з огляду на особливості адміністративно-правових засад інформаційної безпеки як системоутворюючого елементу моделі забезпечення національної безпеки країни наведено теоретичне узагальнення і нове вирішення наукового завдання, унаслідок чого одержано такі найважливіші результати.

1. Сформульовано авторські визначення двох понять:

– «порушення дефініцій національної безпеки» як діяння, умисно вчинене з метою грубого порушення сукупності дефініцій інформаційної безпеки, державної інформаційної безпеки та державної політики держави;

– «суспільна небезпечність порушення дефініцій національної безпеки України» як комплекс діянь, умисно вчинених з метою грубого порушення системної діяльності фізичних та(або) юридичних осіб та їх суспільних відносин, що захищають життєво важливі інтереси людини і громадянина, суспільства, своєчасне виявлення, запобігання і нейтралізацію реальних і потенційних загроз національним інтересам.

2. Удосконалено порядкове ранжирування системи інформаційної безпеки процесів службово-бойової діяльності сектору безпеки і оборони у цілому та НГУ зокрема, яка містить керуючі та виконавчі елементи.

3. Для Національної гвардії України найефективнішим є досвід Франції та Німеччини.

4. Тренінг є одним із способів забезпечення превентивних заходів, пов’язаних із загрозами національній безпеці.

5. Модифікована методика аналізу й оцінювання рівня ризик-ситуацій інформаційної безпеки нашої країни полягає у виявленні ризик-факторів у діяльності сектору безпеки і оборони та розрахунку коефіцієнтів ризику за його видами (правомірний, допустимий, неправомірний), ступенем припустимості (виправданий, не виправданий, політичний, фізичний, економічний).

6. З метою вдосконалення норм чинного кримінального законодавства обґрунтовано запропоновані такі зміни і доповнення:

доповнити Розділ 20 Кримінального кодексу України (КК України) статтею 436^1. Порушення дефініцій національної безпеки України, яка передбачає 4 частини з визначеним рівнем кримінальної відповідальності:

– частина 1. Порушення дефініцій національної безпеки України, тобто діяння, умисно вчинене з метою грубого порушення сукупності дефініцій інформаційної безпеки, державної інформаційної безпеки та державної політики держави, – карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або арештом на строк до шести місяців, або обмеженням волі на строк до п'яти років;

– частина 2. Ті самі дії, вчинені групою осіб, – караються обмеженням волі на строк до п'яти років або позбавленням волі на строк до чотирьох років;

– частина 3. Дії, передбачені частинами першою або другою цієї статті, якщо вони були вчинені особою, раніше судимою за статті, передбачені Розділами 1, 14, 15, 16, 20 цього Кодексу, – караються позбавленням волі на строк від двох до семи років;

– частина 4. Дії, передбачені частинами першою, другою або третьою цієї статті, якщо вони вчинені в особливий період або в умовах воєнного стану, – караються позбавленням волі на строк від п'яти до десяти років.

З об'єктивної сторони порушення дефініцій національної безпеки України є суспільно небезпечною умисною дією, що грубо порушує сукупність дефініцій інформаційної безпеки, державної інформаційної безпеки та державної політики держави.

Об'єкт – дефініції національної безпеки України у цілому та сукупність дефініцій інформаційної безпеки, державної інформаційної безпеки, державної політики держави зокрема.

Суб'єктивна сторона порушення дефініцій національної безпеки України характеризується прямим та непрямим умислом, а також мотивами порушити життєво важливі інтереси людини і громадянина, суспільства, своєчасне виявлення, запобігання і нейтралізацію реальних і потенційних загроз національним інтересам. Суб'єктивні ознаки як мотив вчинення і спрямованість умислу є основними критеріями, які відрізняють порушення дефініцій національної безпеки України від суміжних злочинів.

Суб'єктом порушення дефініцій національної безпеки України можуть бути особи, які досягли 14-річного віку.

У частині 2 ст. 436^1 КК України передбачено відповідальність за порушення дефініцій національної безпеки України, вчинене групою осіб (про поняття групи осіб див. коментар до ст. 28 КК України). При цьому кваліфікація порушення дефініцій національної безпеки України не змінюється від того, чи за попередньою домовленістю, чи без попередньої змови його було вчинено. Різновидом порушення дефініцій національної безпеки України, що вчинене за попередньою змовою групою осіб, слід визнавати і вчинення його організованою групою. Відповідальності за таке порушення дефініцій національної безпеки України, крім безпосередніх виконавців, підлягає й організатор, якщо вчинення такого злочину охоплювалося його умислом.

У частині 3 ст. 436^1 КК України передбачено відповідальність за порушення дефініцій національної безпеки України, визначене у перших двох частинах цієї статті, якщо воно було вчинене особою, раніше судимою за статті, передбачені Розділами 1, 14, 15, 16, 20 цього Кодексу. Порушення дефініцій національної безпеки України визнається злісним за ознакою його рецидиву, тобто вчиняється особою, яка раніше була судима за статтями, передбаченими Розділами 1, 14, 15, 16, 20 цього Кодексу, за умови, що судимість з неї не знята і не погашена. Протиправні дії, вчинені повторно без наявності судимості за одну з них, не є підставою для кваліфікації вчиненого за ч. 3 ст. 436^1, але це повинно бути враховано при призначенні покарання як обтяжуюча обставина (п. 1 ч. 1 ст. 67 КК України).

У випадку вчинення винним різних за ступенем тяжкості протиправних діянь кожне з них (за наявності реальної сукупності) має бути

кваліфіковане за відповідною частиною ст. 436[1] КК України, і остаточне покарання необхідно призначати за правилами ст. 70 Кримінального кодексу України.

Подальші наукові дослідження будуть спрямовані на вдосконалення чинного законодавства у сфері національної безпеки.

Перелік джерел посилання

1. Орел О. В., Мідіна А. С. Генезис Національної гвардії України як суб'єкта протидії загрозам національній безпеці України. *ScienceRise: Juridical Science.* 2018. № 2 (4). С. 4–7.

2. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. № 28. *Відомості Верховної Ради України*. 2015. № 389-VIII. Ст. 250.

3. Про затвердження Указу Президента України «Про введення воєнного стану в Україні» : Закон України від 24.02.2022 р. № 2102-IX. *Офіційний сайт Верховної Ради України*. URL: https://rada.gov.ua (дата звернення: 05.10.2022).

4. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 р. № 64. *Офіційний сайт Верховної Ради України*. URL: https://rada.gov.ua (дата звернення: 05.10.2022).

5. Про продовження строку дії воєнного стану в Україні : Указ Президента України від 14.03.2022 р. № 133. *Офіційний сайт Верховної Ради України*. URL: https://rada.gov.ua (дата звернення: 05.10.2022).

6. Про продовження строку дії воєнного стану в Україні : Указ Президента України від 18.04.2022 р. № 259. *Офіційний сайт Верховної Ради України*. URL: https://rada.gov.ua (дата звернення: 05.10.2022).

7. Про продовження строку дії воєнного стану в Україні : Указ Президента України від 22.05.2022 р. № 341. *Офіційний сайт Верховної Ради України*. URL: https://rada.gov.ua (дата звернення: 05.10.2022).

8. Про продовження строку дії воєнного стану в Україні : Указ Президента України від 12.08.2022 р. № 573. *Офіційний сайт Верховної Ради України*. URL: https://rada.gov.ua (дата звернення: 05.10.2022).

9. Орел О. В., Мідіна А. С. Адміністративно-правові засади оцінки рівня ризиків безпеки інформації в процесах службово-бойової діяльності Національної гвардії України. *ScienceRise: Juridical Science.* 2018. № 1 (3). С. 45–49.

Стаття надійшла до редакції 25.10.2022 р.

UDC 342.951:351.743(477)

O. Orel, A. Midina, I. Yevtushenko

INFORMATION SECURITY AS A SYSTEM-FORMING ELEMENT OF THE NATIONAL SECURITY ENSUREMENT MODEL OF UKRAINE

The article is devoted to a comprehensive study of the information security of Ukraine. The author's vision of ways to improve the administrative and legal foundations of information security as a system-forming element of the national security model of Ukraine is formulated. Based on the results of the research, the paper provides a theoretical generalization and a new solution to the scientific problem, as a result of which the following most important results were obtained. The author's definition of the concept of "violation of the definitions of national security" is formulated as an act intentionally committed with the aim of grossly violating the set of definitions of information security, state information security and state policy of the state; "public danger of violating the definitions of the national security of Ukraine", as a set of actions intentionally committed with the aim of grossly disrupting the systemic activity of individuals and/or legal entities and their social relations that protect the vital interests of a person and citizen, society, timely detection, prevention and neutralization real and potential threats to national interests.

The ordinal ranking of the information security system of the service-combat activity processes of the security and defense sector in general and the NSU in particular, which includes management and executive elements, has been improved. Control elements include: the legal element, which includes legislative, regulatory and scientific bases – is a legal regulator of relations that arise at the operational and tactical

levels of management, taking into account critical information; organizational element, which includes organizational and technical measures and methods, as well as regime measures and methods; affects the information security policy and ensures the activity of competent state authorities in general and NSU in particular; the economic element includes the sources of financing security measures. The executive elements include the technical element, which includes the application of engineering and technical measures that make information inaccessible for illegal actions.

In order to improve the norms of the current criminal legislation, the following changes and additions are reasonably proposed: to supplement Chapter 20 of the Criminal Code of Ukraine with Article 436-1. Violation of the definitions of the national security of Ukraine, which provides for 4 parts with a defined level of criminal liability.

The author's position on the modified method of analysis and assessment of the level of risk situations in the processes of information security of the security and defense sector is given, and attention is also focused on problematic issues that arise at the current stage of the state's development.

Keywords: *information security, national security, security and defense sector, National Guard of Ukraine.*

Орел Оксана Вікторівна – кандидат юридичних наук, доцент, начальник кафедри правового забезпечення Національної академії Національної гвардії України
https://orcid.org/0000-0002-6870-6769

Мідіна Анастасія Сергіївна – аспірантка Національно-наукового інституту «Інститут державного управління» Харківського національного університету імені В. Н. Каразіна
https://orcid.org/0000-0003-0749-0455

Євтушенко Ігор Володимирович – кандидат юридичних наук, доцент кафедри тактико-спеціальної, вогневої та спеціальної фізичної підготовки Інституту підготовки юридичних кадрів для Служби безпеки України Національного юридичного університету імені Ярослава Мудрого
https://orcid.org/0000-0003-4299-6398