МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Л. В. Рибальченко, Е. В. Рижков, С. М. Тютченко,
О. С. Гавриш, А. О. Варяниченко

БЕЗПЕКА ПІДПРИЄМНИЦТВА

Монографія

Дніпро
Видавець Біла К. О.
2020

УДК 65.012
Б 39

Рекомендовано до друку науково-методичною радою
Дніпропетровського державного університету внутрішніх справ
(протокол № 10 від 23 червня 2020 р.)

Рецензенти:

Баранник Л. Б. – д-р екон. наук, проф., проф. кафедри соціального забезпечення та податкової політики Університету митної справи та фінансів;

Іванова М. І. – д-р екон. наук, проф., проф. кафедри менеджменту ДВНЗ «Дніпровська політехніка»;

Будько В. І. – доцент кафедри ВДЕ, д-р техн. наук, заступник завідуючого кафедри ВДЕ КПІ ім. Ігоря Сікорського.

Б 39 **Безпека** підприємництва : моногр. у складі міжнар. автор. кол. / [Рибальченко Л. В., Рижков Е. В., Тютченко С. М. та ін.]. – Дніпро : Видавець Біла К. О., 2020. – 180 с.

ISBN 978-617-645-392-5

Монографія «Безпека підприємництва» являє собою наукову працю, в основу якої покладено дослідження науковців в галузі економічної безпеки підприємництва, національної та міжнародної економіки.

Монографія призначена для науковців, викладачів, магістрів, аспірантів, студентів, державних службовців, фахівців, менеджерів підприємств та фінансових установ, а також широкого кола читачів, які досліджують проблеми економічної безпеки вітчизняної та міжнародної економіки.

УДК 65.012

ISBN 978-617-645-392-5

Авторський колектив монографії

Рибальченко Л.В. – к.е.н., доцент, доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ (вступ, розділи 1, 2, 3)

Рижков Е.В. – к.ю.н., доцент, завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ (підрозділи 2.2, 2.4)

Тютченко С.М. – ст. викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ (розділ 4, розділ 5, підрозділи 5.1-5.5)

Гавриш О.С. - ст. викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ (розділ 6)

Варяниченко А.О. – асистент Університету Лазарського у Варшаві, Lazarski University in Warsaw, Graduate School (розділ 5, підрозділи 5.6-5.8)

ЗМІСТ

ВСТУП

В сучасних умовах відкритого конкурентного середовища, політичної та економічної нестабільності, суб'єкти господарювання мають повну самостійність у прийнятті рішень щодо визначення стратегії розвитку, організації виробництва і збуту продукції, вибору контрагентів, джерел фінансових ресурсів та інших управлінських рішень. Практично всі ризики господарської діяльності лягають на плечі підприємців. У зв'язку з чим, набувають першочергового значення проблеми діяльності підприємств і забезпечення їх економічної безпеки.

Потреба безпеки є базовою як для окремої особистості, підприємства, суспільства, так і держави. Незважаючи на те, що проблеми економічної безпеки останнім часом набувають особливої актуальності, істотна частина досліджень відноситься до безпеки на рівні держави. Підприємство є основною ланкою економіки, тому питання забезпечення економічної безпеки на рівні господарюючого суб'єкта є актуальними.

Непередбачуваність господарської діяльності, відсутність реакції на вплив внутрішніх і зовнішніх загроз можуть призвести до небажаних наслідків і навіть до банкрутства підприємства. Дана обставина вимагає від суб'єктів управління підприємством побудови комплексної системи забезпечення економічної безпеки. Вона повинна бути побудована таким чином, щоб можна було оперативно і з мінімальними витратами нівелювати загрози, що виникають, підтримувати стійкий та ефективний розвиток.

Актуальність проблеми зростає із розвитком сучасних підприємств, які на своєму шляху стикаються із зовнішніми загрозами їх економічній безпеці, до яких належать політичні, ринкові, конкурентна боротьба на вітчизняних ринках, міжнародна конкуренція, природні катаклізми та інші, значущість яких зростає і впливає на забезпечення безпеки не лише окремого підприємства, а й економічну безпеку країни.

При виявленні факторів, які впливають на економічну безпеку підприємства, особливу увагу необхідно звернути на управління безпекою, аналіз та моніторинг стану підприємства, підвищення ефективності бізнес-процесів, а також конкурентоспроможність.

Розвиток національної економіки пов'язаний з економічною безпекою країни і на даному етапі потребує дієвих методів, механізмів, чинників регулювання та управління захистом стану безпеки підприємств та держави від різноманітних загроз. Злочини, які вчиняються в сфері економічної діяльності, становлять реальну загрозу не тільки для кожної людини, а і для суспільства та держави. Одним з найнебезпечніших видів злочинів, який призводить до економічного занепаду держави, є легалізація (відмивання) доходів, одержаних злочинним шляхом.

Високий обсяг тіньового сектору в національній економіці негативно впливає на економічний розвиток та стан економічної безпеки окремих галузей економіки та країни в цілому. Тіньова економіка є причиною поглиблення наявних в економіці дисбалансів, залишаючись одним з найбільших викликів економічній безпеці держави, тенденції зміни яких сьогодні та в подальшому визначатимуть сценарії розвитку економіки країни.

Монографія «Безпека підприємництва» представляє собою наукову працю, в основу якої покладено дослідження науковців в галузі економічної безпеки, управління безпекою, виявлення форм і проявів економічних злочинів та їх вплив на розвиток національної економіки, а також аналіз міжнародного досвіту забезпеченні економічної безпеки держави.

РОЗДІЛ 1. ХАРАКТЕРИСТИКА ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

1.1. Історичні аспекти економічної безпеки в Україні

Так склалось, що разом з появою «людини розумної» (homo sapien), історично зародилось таке поняття як «безпека», тому що усвідомлене бажання бути захищеним від зовнішніх загроз світу закладено в інстинкт самозбереження, що саме природно для людини. Вченні дуже ретельно вивчали це питання, що людина відчуває на біологічному рівні при впливі негативного фактору, який призводить до стресової ситуації, яка в свою чергу формується із відчуття страху в закладений інстинкт. Як приклад, можна навести загальновідому теорію Маслоу, який стверджував, що почуття безпеки перебуває на другому рівні трикутника (піраміди) потреб, після фізіологічних потреб.

Саме слово «безпека» існує дуже давно, але його почали використовувати, коли зрозуміли його суть і в перекладі з грецької воно означає «володіти ситуацією», а як говориться «якщо володіти ситуацією, можна володіти світом». Зараз же поняття «безпека» трактуються по-різному, дехто говорить, що це «стан, коли кому-небудь або чому-небудь ніщо не загрожує», інші, що це «відсутність небезпеки, відсутність загрози не тільки зі зовнішнього світу».

Як було зазначено, саме поняття терміну «безпека» почали використовувати не відразу, а з кінця XII ст. під трактуванням спокійного духу людини, яка відчувала себе захищеною від будь-яких посягань на неї та її душевного спокою. При цьому XVII ст. у Західній Європі дане поняття вживалось дуже рідко. Це пояснюється тим, що на той час широко використовувалось інше поняття – поліція, що трактувалось як державний устрій чи управління, метою якого було збереження суспільного блага та безпеки населення й держави.

У XVII–XVIII ст. термін «безпека» отримав нове трактування, яке характеризувалось станом спокою в результаті відсутності реальної безпеки, при цьому охоплюючи матеріальні, економічні, політичні умови, відповідні органи та організації, що сприяють утворенню такої ситуації.

Перший, хто вирішив виокремити поняття терміну «безпеки», був президент США Т. Рузвельт, який на початку XX ст. визначив її як сукупність умов, що надійно забезпечують суверенітет, захист стратегічних інтересів і повноцінний розвиток суспільства, життя та здоров'я усіх його громадян. Таке визначення увійшло в світову політику і науку.

У 70-ті роки XX ст. вперше з'явився термін "економічна безпека". Він достатньо швидко отримав розповсюдження в розвинутих капіталістичних країнах. Саме тоді, представники країн Західної Європи виступили за використання економічних методів забезпечення національної безпеки. Забезпечення економічної безпеки стало пріоритетом багатьох країн і це не обійшло стороною США, яка її направила на політику держави, про що й свідчив неодноразово секретар У. Крістофер. Також він підкреслював, що зовнішня політика держави США повинна міцно стояти на «трьох китах», тобто на добре розвинутій економічній безпеці країні, підтримці демократії та дотриманні прав людині.

Ключовими моментами в забезпеченні економічної безпеки є підвищення конкурентоспроможності товарів на внутрішньому і зовнішньому ринках, скорочення залежності країни від іноземних позик і зміцнення її можливостей виконувати міжнародні зобов'язання в торговельно-економічних та інших областях.

Після того, як історично склались певні аспекти поняття та суті безпеки у 1991-1992 роках почався процес утворення науки про економічну безпеку держави.

Якщо дивитись глибше та ширше, то саме від безпеки людини утворюється безпека держави й суспільства. Існує певній розподіл на категорії безпеки: безпека людини, національна безпека та державна безпека. Їх можна

уявити у формі ланцюга, які залежать одна від одної, вони усі відіграють велику роль в історії людства.

Тому можна сказати, що формування безпеки у різних сферах та аспектах життєдіяльності людини і держави не закінчено, можна навіть сказати, що це лише початок. Але вже зараз можна сказати, що саме державна безпека умовно охоплює три сектора: військовий (6%), економічний (69%) та політичний (25%) [1].

1.2. Сучасний стан економічної безпеки в Україні

На думку фахівців, економічна безпека є фундаментом для функціонування всіх елементів, які відносяться до цієї системи: політичної, соціальної, військової, екологічної, технологічної, інформаційної безпеки тощо, тому вона займає центральне місце в системі національної безпеки. Це зумовлено тим, що належне забезпечення різних сфер життєдіяльності сприяє розвитку держави. Тому пропонуємо розглянути саме поняття «економічної безпеки» перед тим, як аналізувати її стан в державі.

Економічна безпека — це комплекс дієвих заходів офіційних державних органів, які забезпечують стійкість до зовнішніх та внутрішніх загроз, характеризують здатність національної економіки до розширеного самовідтворення та задоволення потреб громадян, суспільства і держави на певному визначеному рівні та часовому проміжку. Основні напрямки:

- забезпечується досить високе і стійке економічне зростання;
- ефективне задоволення економічних потреб;
- контроль держави за рухом і використанням національних ресурсів;
- захист економічних інтересів країни на національному і міжнародному рівнях.

Також вона виступає складовою частиною національної безпеки, є матеріальною основою. Об'єктом економічної безпеки виступає як економічна система, так і її складові елементи: природні багатства, виробничі і

невиробничі фонди, нерухомість, фінансові ресурси, людські ресурси, господарські структури, сім'я, особа [2].

Для того, щоб розуміти в якому стані знаходиться економічний стан держави, існують показники економічної безпеки - це найбільш значущі параметри, що дають загальне уявлення про стан економічної системи в цілому, її стійкості і мобільності: зростання ВВП, рівень і якість життя більшості населення, темпи інфляції, рівень безробіття, структура економіки, майнове розшарування населення, криміналізація економіки, стан технічної бази господарства, витрати на науково-дослідні роботи, конкурентоспроможність, імпортна залежність, відкритість економіки, внутрішній і зовнішній борг держави.

В таблиці 1.1 наведено динаміку ВВП та прямі інвестиції в економіку держави у 2005 - 2014 рр.

Таблиця 1.1

Динаміка ВВП та прямі інвестиції в економіку держави у 2005 - 2014 рр.

Роки	**ВВП у поточних цінах, млрд.дол.**	**Темп зростання ВВП з урахуванням інфляції, %**	**Динаміка прямих інвестицій, млн.дол.**	**Відношення до показника минулого року млрд.грн.**	**%**
2005	441,4	86,2	2,9	7808	-
2006	544,1	107,8	7,5	5604	71,1
2007	720,7	142,7	7,5	9891	176,5
2008	948	180,1	1,9	10913	110,3
2009	913,3	117,2	-14,5	4816	44
2010	1082,5	137,9	4,1	6495	134,8
2011	1316,6	162,9	5,2	7207	111,0
2012	1408,8	180,2	0,3	8401	116,6
2013	1454,9	175,5	0,0	4499	53,5
2014	1566,7	134,9	-13,3	410	9,1

На протязі досліджуваного періоду, ВВП зріс у 3,55 рази, а динаміка прямих інвестицій в економіку держави була від’ємною у 2009 р. (-14,5 млн.дол.) та 2014 р. (-13,3 млн.дол.).

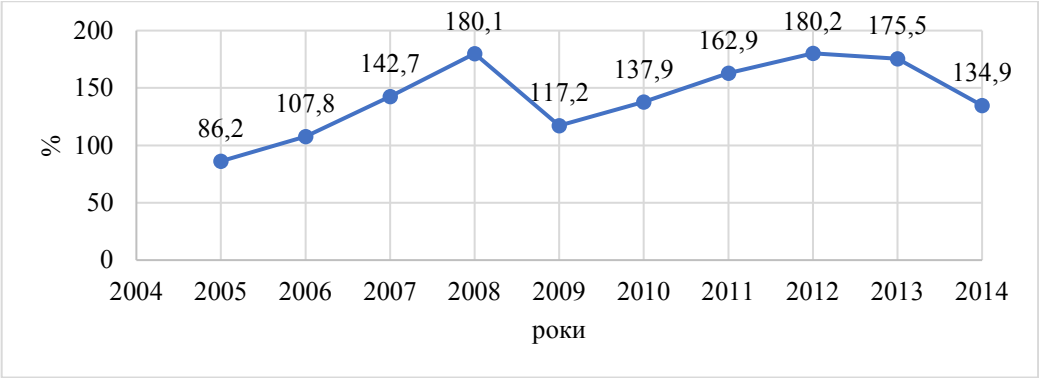

Рис. 1.1. Темп зростання ВВП з урахуванням інфляції у 2005 - 2014 рр.

Дивлячись на ці данні, можна прийти до висновку, що стан економіки в сфері інвестицій знаходився не у сприятливому становищі. Від темпів економічного зростання залежать економічна міць держави, життєвий рівень населення, виконання соціальних програм, успіх в конкурентному суперництві на світовому ринку. Тому економічне зростання, а саме зростання ВВП, є головним змістом економічного розвитку і одним з його найважливіших складових.

За даними Державної служби статистики України [4] побудовано динаміку ВВП за 2010-2019 рр. з подальшим прогнозуванням на наступні два роки у відсотках до відповідного періоду попереднього року. З 2010 по 2014 роки ВВП в країні йде до спаду, з 2015 по 2017 роки йде стабільність з маленьким відхилом у декілька відсотків, з 2018 по 2019 роки знову йде на спад. Автором побудовано прогноз ВВП на 2020-2021 роки, який свідчить про незначне зменшення ВВП у порівнянні з 2019 роком (рис. 1.1).

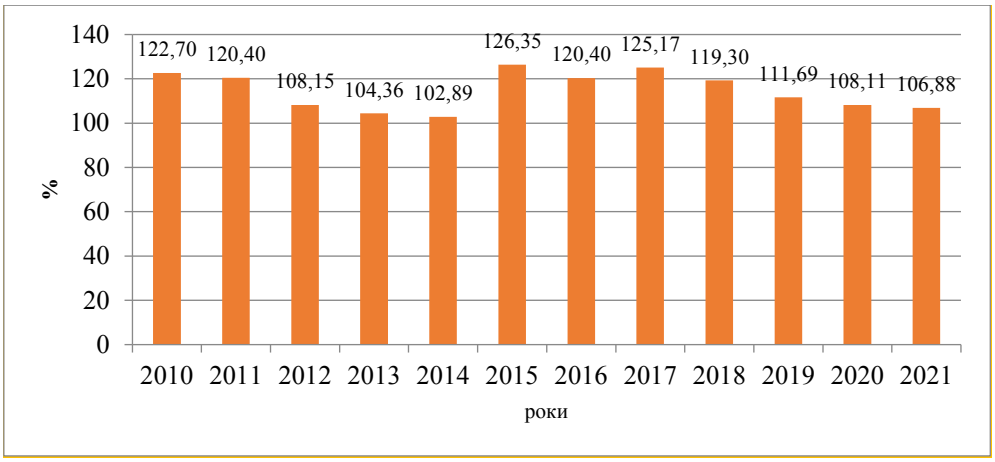

Рис. 1.1. Динаміка ВВП України у 2010 - 2021 рр. (у % до відповідного періоду попереднього року)

Основу економічної безпеки держави становить сама економіка, яка в свою чергу залежить від багатьох факторів. Тому розглянемо вплив прибутку з боку приватних підприємств, як в країні, так і в окремих регіонах та місті Дніпро.

За обсягом реалізованих послуг ми бачимо, що по всій Україні підприємства (табл. 2) здійснили послуг на 221108628,8 тис.грн. або 221,11 млрд.грн., де в свою чергу Дніпропетровська область знаходиться на третьому місці (15289393,7 тис.грн. або 15,29 млрд.грн.), Одеса на другому місці (16376126,2 тис.грн. або 16,38 млрд.грн.) та Київ займає перше місце (95346276,3 тис.грн. або 95,35 млрд.грн.) (табл. 1.2).

Таблиця 1.2

Обсяг реалізованих послуг підприємствами сфери послуг різним споживачам за видами економічної діяльності у 2019 р.

	Обсяг реалізованих послуг, тис.грн	Розподіл обсягу реалізованих послуг за категоріями споживачів (у % до загального обсягу)		
		населенню	підприємствам (установам)	іншим категоріям споживачів
1	*2*	*3*	*4*	*5*
Україна	**221108628,8**	**21,7**	**68,4**	**9,9**
м. Київ	95346276,3	21,4	75,5	3,1
Одеська	16376126,2	12,5	82,3	5,2
Дніпропетровська	**15289393,7**	**15,0**	**81,5**	**3,5**
Львівська	9472398,9	20,7	67,6	11,7
Харківська	8478737,6	27,7	70,3	2,0
Київська	8449070,3	10,2	87,8	2,0
Донецька	4957148,3	10,6	87,5	1,9
Миколаївська	4322144,1	9,9	87,6	2,5
Запорізька	3772061,8	29,3	67,7	3,0
Полтавська	2762246,2	21,6	72,4	6,0
Вінницька	2663662,7	26,6	57,2	16,2
Черкаська	2525779,8	16,6	73,4	10,0
Закарпатська	2326209,3	19,2	77,2	3,6
Кіровоградська	2119441,5	10,1	87,2	2,7
Волинська	1784965,4	22,4	73,1	4,5
Івано-Франківська	1701009,9	25,6	71,6	2,8
Чернігівська	1501452,9	29,3	61,1	9,6
Тернопільська	1478375,0	25,4	71,6	3,0
Херсонська	1475673,3	23,6	72,7	3,7
Сумська	1472207,3	26,7	62,7	10,6
Житомирська	1317970,0	34,8	63,7	1,5
Хмельницька	1263851,6	26,5	67,0	6,5

Продовження табл. 1.2

1	*2*	*3*	*4*	*5*
Рівненська	1165553,6	20,4	69,0	10,6
Чернівецька	854541,3	46,4	40,5	13,1
Луганська	459953,3	36,3	61,0	2,7

Тепер розглянемо Дніпропетровську область та окремі її галузі, щоб зрозуміти яка сфера діяльності найбільш прибуткова у даній області (табл.1.3).

Таблиця 1.3

Обсяг реалізованих послуг підприємствами різним споживачам за видами економічної діяльності по Дніпропетровській області у 2019 р.

	Обсяг реалізованих послуг, тис.грн	Розподіл обсягу реалізованих послуг за категоріями споживачів (у % до загального обсягу)			Частка у загальній сумі обсягу реалізованих послуг, %
		населенню	підприємствам (установам)	іншим категоріям споживачів	
Усього	15289393,7	15,0	81,5	3,5	100
Транспорт, складське господарство, поштова та кур'єрська діяльність	***7604178,6***	***9,5***	***88,1***	***2,4***	***49,73***
Операції з нерухомим майном	2177052,3	2,6	86,0	11,4	14,24
Діяльність у сфері адміністративного та допоміжного обслуговування	1574002,6	27,0	71,9	1,1	10,29
Професійна, наукова та технічна діяльність	1523880,3	3,2	96,1	0,7	9,97
Інформація та телекомунікації	895107,4	11,2	84,2	4,6	5,85
Тимчасове розміщування й організація харчування	592194,2	57,0	41,9	1,1	3,87
Охорона здоров'я та надання соціальної допомоги	495628,9	74,2	23,5	2,3	3,24
Освіта	282415,6	66,1	33,5	0,4	1,85
Надання інших видів послуг	85473,9	12,3	79,8	7,9	0,56
Мистецтво, спорт, розваги та відпочинок	59459,9	59,5	36,8	3,7	0,39

Згідно з даними за 2019 рік, у Дніпропетровській області найбільший обсяг реалізованих послуг припадає на транспорт, складське господарство, поштову та кур'єрську діяльність і становить 49,73% (7604178,6 тис.грн.). Далі йдуть операції з нерухомим майном 14,24% (2177052,3 тис.грн.), діяльність у сфері

адміністративного та допоміжного обслуговування 10,29% (1574002,6 тис.грн.) та інші. Необхідно звернути увагу на те, що обсяг реалізованих послуг на освіту в області становить лише 1,85% (282415,6 тис.грн.) із загальної суми усіх послуг.

Якщо порівнювати прибуток та збиток великих та середніх підприємств в усіх регіонах, то видно, що у січні-вересні 2018 року (табл.1.4) загальний фінансовий результат в Україні складав 122825,3 млн.грн., із них прибутку 70,2% підприємств (275210,5 млн.грн.) отримали прибуток і 29,8% підприємств збиток (152385,2 млн.грн.).

Таблиця 1.4

Чистий прибуток (збиток) великих та середніх підприємств за регіонами за січень-вересень 2018 року (млн.грн.)

Регіон	Фінансовий результат (сальдо)	Підприємства, які одержали прибуток		Підприємства, які одержали збиток	
		у % до загальної кількості підприємств	фінансовий результат	у % до загальної кількості підприємств	фінансовий результат
Україна	**122825,3**	**70,2**	**275210,5**	**29,8**	**152385,2**
м.Київ	78215,9	73,7	131905,6	26,3	53689,7
Дніпропетровська	**24616,7**	**70,1**	**49350,6**	**29,9**	**24733,9**
Запорізька	9981,9	68,8	12162,6	31,2	2180,7
Полтавська	3913,3	65,0	8970,2	35,0	5056,9
Харківська	3433,2	72,3	6340,3	27,7	2907,1
Львівська	3261,5	72,5	5884,9	27,5	2623,4
Одеська	2479,7	67,1	5931,9	32,9	3452,2
Волинська	1857,0	74,5	2785,4	25,5	928,4
Черкаська	1798,5	70,3	2917,7	29,7	1119,2
Донецька	1560,1	57,7	16264,7	42,3	14704,6
Вінницька	1147,1	69,2	2068,7	30,8	921,6
Рівненська	878,3	73,4	1400,6	26,6	522,3
Чернігівська	878,2	72,8	1274,0	27,2	395,8
Сумська	873,4	68,0	2526,1	32,0	1652,7
Івано-Франківська	831,9	68,2	1443,3	31,8	611,4
Житомирська	743,7	73,3	1763,8	26,7	1020,1
Тернопільська	402,7	67,0	892,3	33,0	489,6
Херсонська	330,1	64,5	849,4	35,5	519,3
Миколаївська	219,0	67,8	2200,8	32,2	1981,8
Кіровоградська	119,6	65,7	732,9	34,3	613,3
Закарпатська	65,8	73,2	669,1	26,8	603,3
Чернівецька	39,8	70,6	378,5	29,4	338,7
Хмельницька	-128,2	67,8	1137,9	32,2	1266,1
Луганська	-6226,2	53,9	2300,4	46,1	8526,6
Київська	-8467,7	68,6	13058,8	31,4	21526,5

З табл. 1.4 видно, що фінансовий результат підприємств Дніпропетровської області (24616,7 млн.грн) є другим після м. Києва (78215,9 млн.грн) в Україні. 70,1% підприємств отримали прибуток (49350,6 млн.грн.) і 29,9% підприємств (24733,9 млн.грн.) збиток. В таблиці 1.5 наведено фінансовий результат великих та середніх підприємств за січень-вересень 2019 року.

Таблиця 1.5

Чистий прибуток (збиток) великих та середніх підприємств за регіонами за січень-вересень 2019 року (млн.грн.)

Регіон	Фінансовий результат (сальдо)	Підприємства, які одержали прибуток		Підприємства, які одержали збиток	
		у % до загальної кількості підприємств	фінансовий результат	у % до загальної кількості підприємств	фінансовий результат
Україна	**145630,3**	**74,4**	**216149,1**	**25,6**	**70518,8**
м.Київ	89244,5	79,5	110871,4	20,5	21626,9
Дніпропетровська	**23961,4**	**73,8**	**38059,4**	**26,2**	**14098,0**
Київська	8684,2	74,6	10672,0	25,4	1987,8
Полтавська	4921,0	73,6	7418,0	26,4	2497,0
Одеська	3647,7	77,2	5323,6	22,8	1675,9
Рівненська	2204,5	75,0	2337,0	25,0	132,5
Миколаївська	2126,2	74,0	2591,3	26,0	465,1
Черкаська	2114,9	76,8	2765,6	23,2	650,7
Луганська	1994,3	51,4	2897,7	48,6	903,4
Сумська	1268,0	74,2	1645,5	25,8	377,5
Івано-Франківська	1198,0	66,2	1796,4	33,8	598,4
Вінницька	1185,2	68,4	1899,4	31,6	714,2
Херсонська	1115,5	74,5	1357,5	25,5	242,0
Запорізька	914,7	70,6	4012,2	29,4	3097,5
Харківська	910,8	77,5	3700,7	22,5	2789,9
Чернігівська	853,5	61,2	1313,8	38,8	460,3
Житомирська	540,2	70,3	1198,8	29,7	658,6
Хмельницька	366,8	58,2	1061,9	41,8	695,1
Закарпатська	256,9	74,5	572,5	25,5	315,6
Кіровоградська	247,7	65,8	597,5	34,2	349,8
Львівська	155,6	73,6	4214,1	26,4	4058,5
Тернопільська	28,9	77,1	507,9	22,9	479,0
Чернівецька	-170,9	56,2	203,2	43,8	374,1
Волинська	-540,8	73,1	961,9	26,9	1502,7
Донецька	-1598,5	55,9	8169,8	44,1	9768,3

З таблиці 1.5 наведено, що у 2019 році загальний фінансовий результат в Україні складав 145630,3 млн.грн., із них прибуток отримали 74,4% підприємств (216149,1 млн.грн), а збиток 25,6% підприємств (70518,8 млн.грн.). У Дніпропетровській області фінансовий результат склав 23961,4 млн.грн., із них прибуток отримали 73,8% підприємств (38059,4 млн.грн.), а збиток 26,2% підприємств (14098,0 млн.грн.) [4].

При такій різниці у цифрах складаються сумніви щодо правомірного ведення бізнесу у нашій країні. Більшість підприємств для свого збагачення інколи йдуть злочинним шляхом, щоб збільшити суму прибутку собі у кишеню. Ці види злочинів, що стосуються економіки підприємства й не тільки, класифікуються, як економічні злочини.

Якщо дивитися дані звіту Генеральної прокуратури України за останні 4 років «Про кримінальні правопорушення, вчинені на підприємствах, установах, організаціях за видами економічної діяльності», то можна побачити, що особливо тяжкі злочини за чотири роки зменшилися на 36,88%, тяжкі злочини зменшилися на 31,95% і середньої тяжкості на 31,8%. В цілому, кримінальні правопорушення, вчинені на підприємствах з 2016 по 2019 рр. зменшилися на 33% (табл. 1.6) [5].

Таблиця 1.6

Про кримінальні правопорушення, вчинені на підприємствах, установах, організаціях за видами економічної діяльності за 2016-2019 рр. в Україні

Рік	Особливо тяжкі	Тяжкі	Середньої тяжкості	Усього
2016	13425	113863	142583	358658
2017	12936	128689	142688	377432
2018	10355	145028	159014	419696
2019	8474	77486	97244	240296
Зменшення,%	36,88	31,95	31,8	33

Досліджено, що найменша кількість скоєних економічних злочинів припадає на початок року, а на кінець року - найбільша.

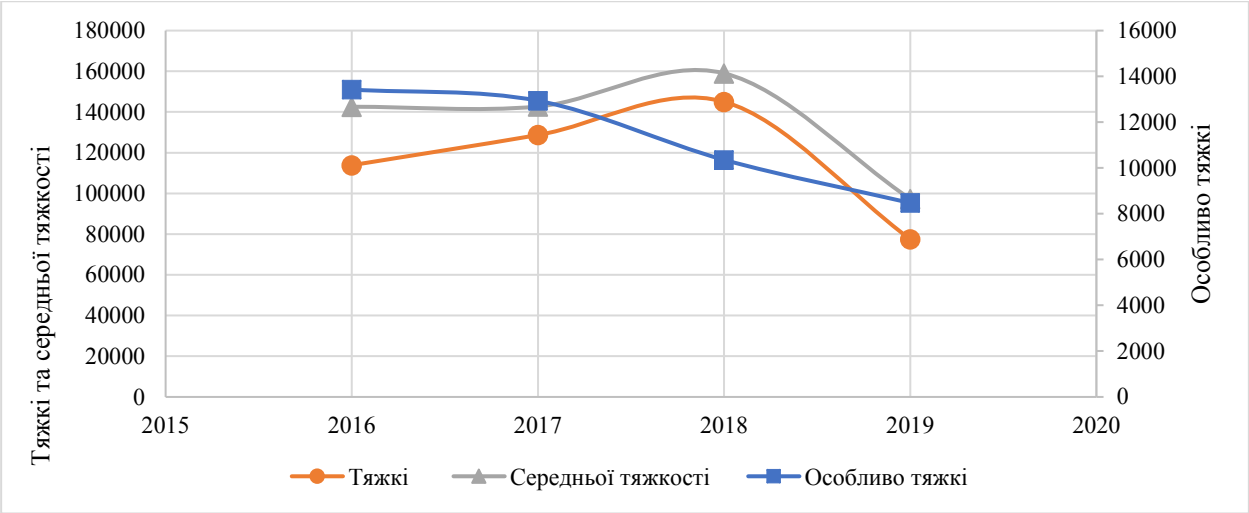

Рис. 1.2. Кримінальні правопорушення, вчинені на підприємствах, установах, організаціях за видами економічної діяльності у 2016-2019 рр. в Україні

1.3. Порівняння характеристика економічної безпеки України з іншими країнами світу

В останні роки, забезпечення формування економічної безпеки, стає найактуальнішим питанням, адже завдяки своєму географічному положенню, до України виникає великий інтерес зарубіжних країн. Але разом із тим, дане питання потребує ретельного дослідження, так як економічна безпека є найактуальнішим питанням сьогодення. При стратегічному плануванні розвитку у цій сфері потрібно опиратись на досвід інших країн в забезпеченні економічної безпеки країни.

Найважливішим завданням держави і захисту національних інтересів є забезпечення економічної безпеки та гарантування її стабільного розвитку. Ефективне і стабільне функціонування національної економіки залежить від ступеня захисту, упередження загроз, які виникнуть, або можуть виникнути та безпеки в економічній сфері держави.

Найбільш економічно ефективними є системи забезпечення економічної безпеки Великобританії, Німеччини, Франції, Італії та Іспанії. Державна політика цих країн зорієнтована на підвищення ефективності

національної економіки з одночасним підтриманням високого рівня економічної безпеки держави.

В Німеччині використовуються методи щодо забезпечення економічної безпеки, які спрямовані на підтримку цивілізованих ринкових відносин, забезпечення економічного і соціального прогресу, недопущення монополізму в окремих галузях, створення умов для справедливої конкуренції та стабільності національної валюти, захист від економічного шантажу, енергетична безпека.

У Франції методи щодо забезпечення економічної безпеки спрямовані на зниження вразливості господарської системи країни, збереження самостійності зовнішньої політики, усунення диспропорцій у рівні економічного розвитку суб'єктів господарювання; недопущення надмірної зовнішньої залежності в найважливіших секторах економіки, мінімізацію ризиків, пов'язаних із залежністю від зовнішнього світу. У Великобританії такі методи пов'язані з прогнозуванням і запобіганням найбільш небезпечних зовнішніх і внутрішніх ризиків. При виробленні та реалізації рішень, що відносяться до забезпечення економічної безпеки, акцент робиться на спеціалізовані організації, що представляють інтереси промисловців і підприємців.

В Іспанії забезпечення економічної безпеки базується на захисті інтересів пріоритетних галузей промисловості, а також спрямовані на стимулювання інвестицій, забезпечення валютного контролю, на розробку законодавства про акціонерні товариства.

В Італії методи щодо забезпечення економічної безпеки спрямовані на захист інтересів національних виробників на внутрішньому і зовнішньому ринках.

Нові країни-члени ЄС (Болгарія, Польща, Румунія, Словаччина, Чехія, Угорщина) вже завершили реформи так званого «першого покоління» і вийшли на завершальний етап реформування системи забезпечення економічної безпеки держави. При виборі методів забезпечення економічної

безпеку країни враховують геополітичну ситуацію, вектор і стратегію розвитку економіки відповідно до тенденцій регіонального та світового еволюційного процесу, напрям економічних реформ.

Стратегія національної безпеки США спрямована на підтримку високого рівня боєздатності озброєних сил, для чого необхідно підвищувати ефективність і конкурентоспроможність економіки, відкривати нові іноземні ринки і створювати нові робочі місця. Для Японії характерним є збереження та розвиток економічної потужності країни, формування сприятливого глобального середовища, що забезпечить максимальну реалізацію національних інтересів. Китайська модель економічного розвитку спрямована на збереження темпів економічного зростання, створення більш інклюзивного суспільства й підвищення якості життя, а також розвиток інноваційної нації. Економічна безпека Китаю дотримується жорстких обмежень на прямі іноземні інвестиції в стратегічно важливі сфери економіки (оборонна промисловість, цивільна авіація, залізничний транспорт і зв'язок). Обмежуються також інвестиції у провідні банківські установи, страхові компанії, зовнішньоторговельні фірми, а також гірничорудні підприємства.

Політика забезпечення економічної безпеки Чехії, Польщі, Словаччини та країн Балтії визначена відповідними документами з національної безпеки (стратегіями, концепціями) й ґрунтується на зближенні національних інтересів із загальноєвропейськими інтересами в контексті євроінтеграції, а також характеризується політичною, економічною й інституціональною трансформацією відповідно із західноєвропейськими стандартами. Головними загрозами економічній безпеці цієї групи країн є економічне відставання регіонів Центральної Європи від західноєвропейських країн, труднощі переходу до ринкової економіки, проблеми формування демократичних і ринкових інститутів.

Використання міжнародного досвіду економічної безпеки до вимог України є дуже довготривалим у часі. Для цього потрібно враховувати рівень

економічного розвитку, розвитку інститутів управління, забезпечення та контроль над безпекою у цілому [6].

За даними досліджень організації Institute for Economics and Peace у 2019 році, рейтинг економічного стану безпеки України у 2017-2018 рр. був таким, що за рік Україна досягла значних результатів (рис. 1.3) і покращила свої позиції у 2018 році у порівнянні з 2017 роком. Наприклад, за рейтингом бюджетної прозорості Україна за станом на 2018 рік посіла 39 місце, де піднялась на 18 сходинок у порівнянні з 2017 роком (57 місце). Покращився і стан свободи людини, де із 134 місця (у 2017 р.) піднялася на 118 місце (у 2018р).

Таблиця 1.7

Міжнародний рейтинг України у 2017-2018 рр.	2017 рік	2018 рік	Покращення
Бюджетної прозорості	57	39	18
Свободи людини	134	118	16
Економічної свободи	149	134	15
Глобальних інновацій	50	43	7
Конкурентоспроможності	89	83	6
Легкості ведення бізнесу	76	71	5
Найкращих країн світу	63	69	-6
Інвестиційної привабливості	134	131	3
Найкращих країн для ведення бізнесу	80	77	3
Екологічних країн світу	20	18	2
Сприйняття корупції	131	130	1
Свободи ЗМІ	102	101	1
Найсильніших армій світу	30	29	1
Індекс процвітання	112	111	1

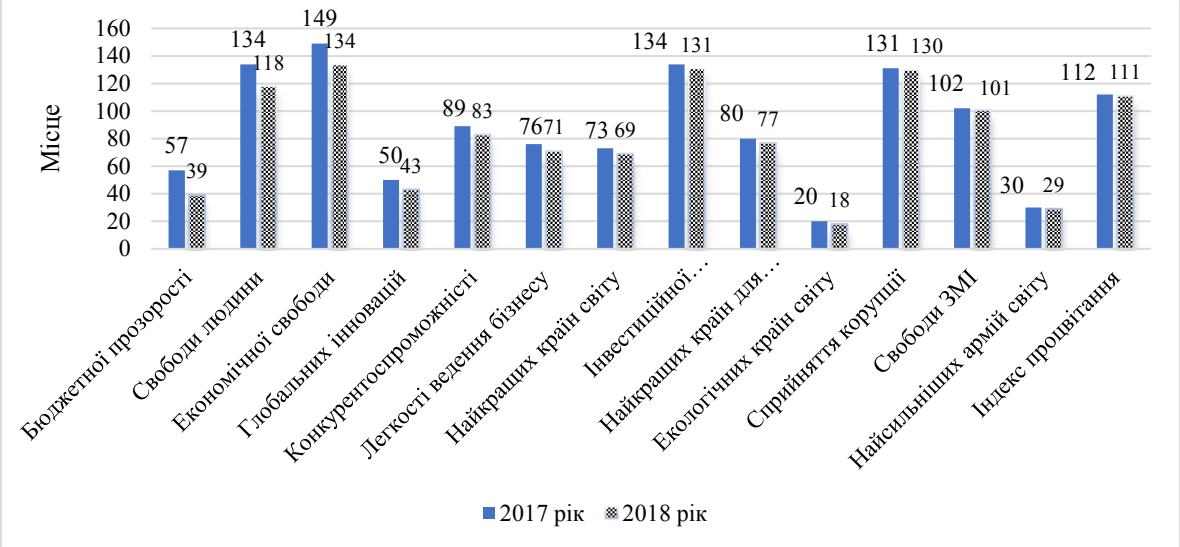

Рис. 1.3. Рейтинг економічного стану безпеки України у 2017-2018 рр.

Стан економічної свободи також покращився на 15 пунктів (із 149 піднялась на 134 місце). Відбулося покращення і в глобальному рейтингу інновацій (143 місце), глобальній конкурентоспроможності (83 місце), рейтингу легкості ведення бізнесу (71 місце), рейтингу інвестиційної привабливості (131 місце). Погіршення стану за показником найкращі країни світу на шість пунктів (із 63 на 69 місце). В інших рейтингах відбулися незначні зміни [7].

Рейтинговий список економічного стану України та інших країн світу за даними організації Institute for Economics and Peace за 2017 рік такий, що за індексом ведення бізнесу Україна займала 76 місце, за рейтингом економічної свободи 149 місце, за індексом потужності армії займає 30, за рейтингом якості автомобільних доріг 134, за індексом розвитку людського капіталу 24 місце, за індексом глобальної конкурентоспроможності 81 місце, за рейтингом аутсорсингової привабливості 24 місце та за рейтингом національних брендів займає 61 місце.

Також серед країн є окремі порівняльні категорії, які не менш стосуються економічної безпеки держави. Розглянемо рейтинг країн за рівнем життя країн світу у 2014-2017 рр. (табл.1.8) Так, у 2017 році першу трійку очолюють: Норвегія, Нова Зеландія та Фінляндія. Україна спустилась на 37 пунктів порівняно з 2016 роком і займає 107 місце серед 149 країн, в той час як у 2014 році посідала 64 місце.

Таблиця 1.8

Рівень життя країн світу у 2014-2017 рр.

Держава	**2017**	**2016**	**2015**	**2014**
	Ранг			
Норвегія	1	1	1	1
Нова Зеландія	2	4	3	5
Фінляндія	3	9	8	8
Швейцарія	4	2	2	2
Данія	9	3	4	6
Польща	34	29	31	34
Україна	**107**	**70**	**63**	**64**

Найнижчими показниками в Україні були: охорона здоров’я, безпека та державне управління, це якраз те, на що потрібно більш звернути уваги при стратегічному плануванні концептуального плану забезпечення економічної безпеки. Даний рейтинг характеризується такими показниками, як: економіка, підприємництво, управління, освіта, охорона здоров’я, рівень свободи, безпеки особистості, соціальний захист населення та навколишнє середовище. Це дослідження вказує на суттєві погіршання рівня життя в країні за показниками 2014-2017 років.

Розглянемо більш детально рівень життя в країнах світу у 2019 році. Рівень життя - це ступінь задоволення ключових потреб населення і людей, які проживають в тій чи іншій країні світу. При розгляді рівня життя в першу чергу розглядаються матеріальні потреби людей, задоволення яких значною мірою залежить від рівня добробуту і споживання людини. Поняття якість життя представляє собою: стан здоров'я, тривалість життя, стан навколишнього середовища, соціальну обстановку, психологічний комфорт, задоволення культурних і релігійних потреб, тощо.

Рівень і якість життя в країні - це одна з найважливіших якісних характеристик соціального життя населення. Якість життя характеризує структуру потреб населення країни і можливості їх задоволення та реалізації в конкретній країні світу.

Якість життя це не тільки відображення матеріального добробуту населення в країні, а й інші показники, які відображають духовні та соціальні потреби людини. Якість життя є найбільш об'єктивним і інтегрованим показником, що відображає соціальний стан суспільства в країні. Люди з низьким рівнем і якістю життя, мають великі життєві труднощі та обмеження в країнах. Низький рівень життя в цілому негативно відбивається на їх фінансовому стані. І навпаки, люди в країнах з високою якістю і рівнем життя, відчувають задоволення і мають великі перспективи реалізації своїх ключових потреб.

На показник рівня і якості життя часто орієнтуються іммігранти, коли вибирають ту чи іншу країну для свого потенційного місця проживання. Однак, тут важливо розуміти, що умови проживання в країнах, в тому числі і якість життя, можуть відрізнятися для корінних і постійних мешканців країни та для приїжджих з інших країн. Тому окремо від рейтингу країн світу за якістю життя також існує рейтинг кращих країн для еміграції.

Показник рівень життя вимірюється за такими параметрами економічної та соціальної сфер країни, складовими яких є:

- ✓ демографія - народжуваність, смертність, тривалість життя;
- ✓ сімейне життя - кількість шлюбів, розлучень;
- ✓ громадське і релігійне життя;
- ✓ добробут - ВВП на душу населення, купівельна спроможність;
- ✓ рівень зайнятості, безробіття та умови праці в країні;
- ✓ політична стабільність в країні;
- ✓ рівень політичної волі;
- ✓ рівень безпеки та злочинності;
- ✓ клімат і географічне розташування;
- ✓ стан навколишнього середовища;
- ✓ рівноправність чоловіків і жінок в різних сферах.

В таблиці 1.9 наведено рівень життя деяких країн світу у 2019 році, до складу яких увійшло 77 країн.

Таблиця 1.9

Рівень життя країн світу у 2019 році

(бали)

Держава	Місце	Індекс якості життя	Купівельна спромож-ність	Безпека	Здоров'я	Вартість життя	Вартість житла до доходу	Транспорт	Навколишнє середовище
Данія	1	196,47	110,69	75,28	79,22	83,88	7,52	29,60	20,79
Швейцарія	2	196,08	127,76	78,82	73,23	122,67	9,11	29,12	21,31
Фінляндія	3	195,06	108,78	77,25	75,27	72,18	7,88	30,62	11,57
Австралія	4	189,73	118,09	57,30	76,82	73,39	7,68	35,66	23,15
Польща	36	145,90	66,06	70,33	62,52	39,38	10,95	31,68	52,88
Україна	**65**	**103,32**	**33,14**	**50,96**	**51,13**	**30,94**	**13,42**	**38,44**	**65,55**

Розглядаючи показник купівельна спроможність, тобто кількість товарів і послуг, що можуть бути придбані за одиницю грошей, величина, обернена до рівня цін, тобто платоспроможність населення, можна сказати, що купівельна спроможність України (33,14) із Данією (110,69) у 3,34 рази є меншою, а з Польщею (66,06) у два рази. Купівельна спроможність населення корелює з доходами і може стимулювати рівень споживання. Рівень безпеки в України більше, ніж на 30% є нижчим, ніж в Данії, Швейцарії та Фінляндії, а за станом здоров'я нижчий за 35%.

Вартість життя — це виражена в грошовій формі кількість матеріальних благ і послуг, які фактично споживаються населенням. Вартість життя можна визначити як сукупність витрат, які робить людина, сім'я чи група населення для придбання товарів і послуг, які необхідні для забезпечення життєдіяльності та відновлення працездатності. В Україні у 2019 році вартість життя майже у три рази (2,71 рази) нижче, ніж в Данії.

А от вартість житла до доходу в Україні в 1,78 рази вище, ніж в Данії, тобто в країні з найвищим рівнем життя. Щодо навколишнього середовища, то цей показник також у три рази є більший, ніж у перших двох країнах світу Данії і Швейцарії, що вказує на негативний стан екології в Україні.

В системі економічної безпеки головним показником вважається обсяг та рівень видатків на фінансування національної оборони держави, що в нашій ситуації за станом 2014-2019 років є значно важливим. Світова практика виокремлює три основні підходи на формування воєнної доктрини:

1) повна відмова від військових видатків;

2) створення могутньої воєнної супердержави;

3) фінансування оборони за принципом мінімальної достатності.

Головним завданням Збройних сил України вважається захист суверенітету, незалежності та територіальної цілісності. Тому розглянемо видатки на оборону та правоохоронні органи у 2013-2021 роках.

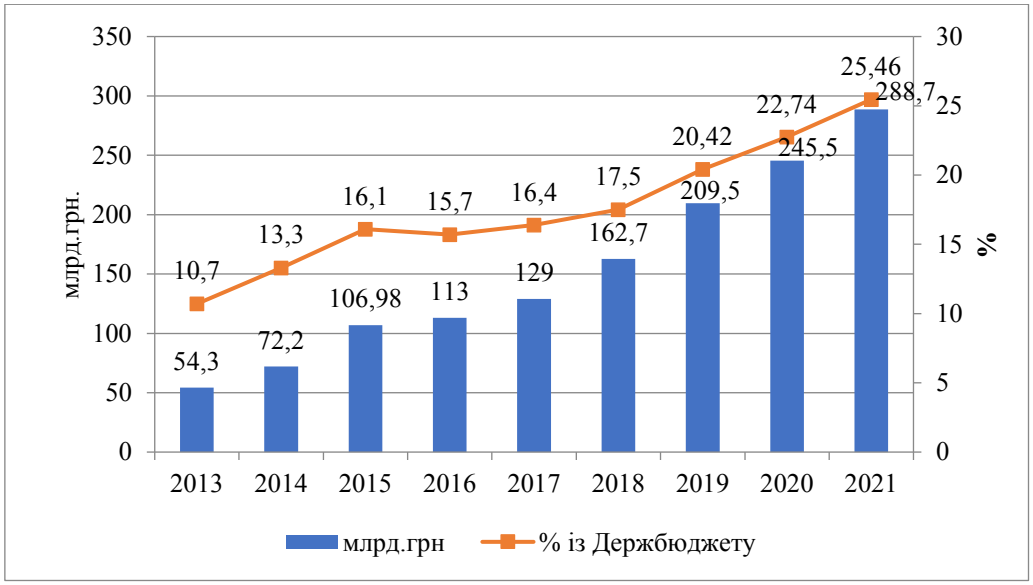

Рис. 1.5. Видатки на оборону та правоохоронні органи в Україні у 2013-2021 рр.

З 2013 по 2018 рр. видатки на оборону та правоохоронні органи з Держбюджету країни зросли у 3,8 рази (з 54,3 млрд.грн. до 162,7 млрд.грн.), що становить 10,7% та 17,5% загального розміру видатків Держбюджету України відповідно. У 2019-2020 рр. видатки на утримання та розвиток Збройних Сил України зросли і становили 209,5 та 245,8 млрд.грн. відповідно, що складає 5 та 5,45% відсотків валового внутрішнього продукту країни.

За розрахованим прогнозом на 2021 рік видатки на утримання та розвиток Збройних Сил України становитимуть 288,7 млрд.грн., що складає не менше 5% відсотків валового внутрішнього продукту країни і відповідає Стратегії національної безпеки України та Концепції розвитку сектору безпеки і оборони [8].

Індекс Global Firepower щорічно надає аналітичний виклад даних про сучасні військові сили країн світу. Даний рейтинг об'єднує в собі більше 50 різних показників, крім таких як чисельність армії, кількості танків, кораблів, літаків та іншої військової техніки, він враховує географічний чинники, природні ресурси, наявність робочої сили, рівень фінансування військової сфери транспортну інфраструктуру країни, доступ до нафтопродуктів та інші фактори, які можуть вплинути на боєздатність армії (табл. 1.9) [9].

Таблиця 1.9

Рейтинг країн згідно з індексом військової могутності

№ з/п	Країна	Індекс 2019	№ з/п	Країна	Індекс 2018	№ з/п	Країна	Індекс 2016
1	США	0,0615	1	США	0,0818	1	США	0,0897
2	Росія	0,0639	2	Росія	0,0841	2	Росія	0,0964
3	Китай	0,0673	3	Китай	0,0852	3	Китай	0,0988
4	Індія	0,1065	4	Індія	0,1417	4	Індія	0,1661
5	Франція	0,1584	5	Франція	0,1869	5	Франція	0,1993
6	Японія	0,1707	6	Великобританія	0,1917	6	Великобританія	0,2466
7	Південна Корея	0,1761	7	Південна Корея	0,2001	7	Японія	0,2466
8	Великобританія	0,1797	8	Японія	0,2107	8	Туреччина	0,2623
9	Туреччина	0,2089	9	Туреччина	0,2216	9	Німеччина	0,2646
10	Німеччина	0,2097	10	Німеччина	0,2461	10	Італія	0,2724
29	**Україна**	**0,5082**	**29**	**Україна**	**0,5383**	**30**	**Україна**	**0,5867**
137	Бутан	6,3988	136	Бутан	7,5497	126	Центральна Африканська Республіка	3,7343

У 2016-2019 рр. США, Росія і Китай традиційно розділили між собою першу трійку, Україна ж посіла у списку 30 та 29 місця. У першу десятку також увійшли Індія, Франція, Великобританія, Японія, Туреччина та Німеччина [10].

Аналіз проведеного дослідження показує, що за ці роки Україні не вдалось створити якісну національну економічну безпеку, яка б забезпечувала динамічний розвиток держави та відповідала високим світовим стандартам. Конструктивно доведено, що на сьогодні існують проблеми в енергетичній, фінансовій, виробничій, макроекономічній, інвестиційно-інноваційній, соціальній, продовольчій, демографічній та зовнішньоекономічній сферах, які унеможливлюють стабільний соціально-економічний розвиток України та призводять до зниження загального рівня національної економічної безпеки.

Усе це потребує в необхідності розроблення та затвердження на економічному рівні Концепції економічної безпеки України, реалізація якої створить можливості ефективного захисту і реалізації національних економічних інтересів на основі цілеспрямованого впливу на існуючі загрози зовнішнього та внутрішнього походження.

Список використаних джерел до розділу 1

1. Сутність та історія формування національної економічної безпеки. - [Електронний ресурс] - Режим доступу: http://megalib.com.ua

2. Акімова Л.М. Етапи становлення економічної безпеки держави: зарубіжний та вітчизняний досвід: Державне управління: удосконалення та розвиток. № 8. - 2016.

3. Rybalchenko L. Ensuring enterprise economic security / L.Rybalchenko, E. Ryzhkov // Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. - 2019. - Special Issue № 1 (102). – P. 268-271

4. Державна служба статистики України. - [Електронний ресурс] – Режим доступу: http://www.ukrstat.gov.ua

5. Генеральна прокуратура України. – [Електронний ресурс] – Режим доступу: https://www.gp.gov.ua

6. Насипайко Д.С., Кузьмін Є.С., Могилей А.О. Економічна безпека України: стан та перспективи. - 2011. - Наукові записки КНТУ, вип.11. - С. 183-187

7. Institute for Economics and Peace. – [Електронний ресурс] – Режим доступу: http://economicsandpeace.org

8. Human Development Indices and Indicators. – [Електронний ресурс] – Режим доступу: https://www.ua.undp.org

9. Military Strength Ranking 2019 (Рейтинг военной силы 2019 года) - [Електронний ресурс]. – Режим доступу: https://www.globalfirepower.com/countries-listing.asp

10. Tymoshenko, O. and Oleshko, A. (2018), “State policy of economic security of Ukraine in conditions of global instability”, Ekonomika ta derzhava, vol. 9, pp. 30–33. DOI: 10.32702/2306-6806.2018.9.30 (Accessed 4 June 2019).

РОЗДІЛ 2. БОРОТЬБА З ЕКОНОМІЧНИМИ ЗЛОЧИНАМИ В УКРАЇНІ

2.1. Форми економічної злочинності та їх вплив на стан безпеки держави

Високий рівень економічного стану країни є головним критерієм оцінки розвинутого суспільства, так як економіка забезпечує гідний рівень життя, існування країни та її прогрес і процвітання. Тому злочини, які вчиняються в сфері економічної діяльності становлять реальну загрозу не тільки для кожної людини, а і для суспільства та держави.

Економічні злочини підлягають даній класифікації як злочини, які спричинили значні збитки державі, чи підприємству. Як показала практика, притягнути до відповідальності фізичних осіб складно. Прикладом таких злочинів є ухилення від сплати податків, незаконні валютні операції, розкрадання державної чи підприємницької власності. Економічна злочинність відноситься до організованої злочинності, так як сама організована злочинність включає в себе ряд інших злочинів, такі як розповсюдження наркотиків, контрабанда та ін.

За останні десятиліття організована економічна злочинність в Україні пройшла такий шлях розвитку, що діяльність транснаціональних організованих злочинних угруповань перетворилась на масштабну загрозу соціальній, економічній і політичній стабільності в державі. Тому проблема запобігання та протидії економічній злочинності набуває глобального характеру. Розглянемо схему економічної злочинності, яка представлена на рис. 2.1.

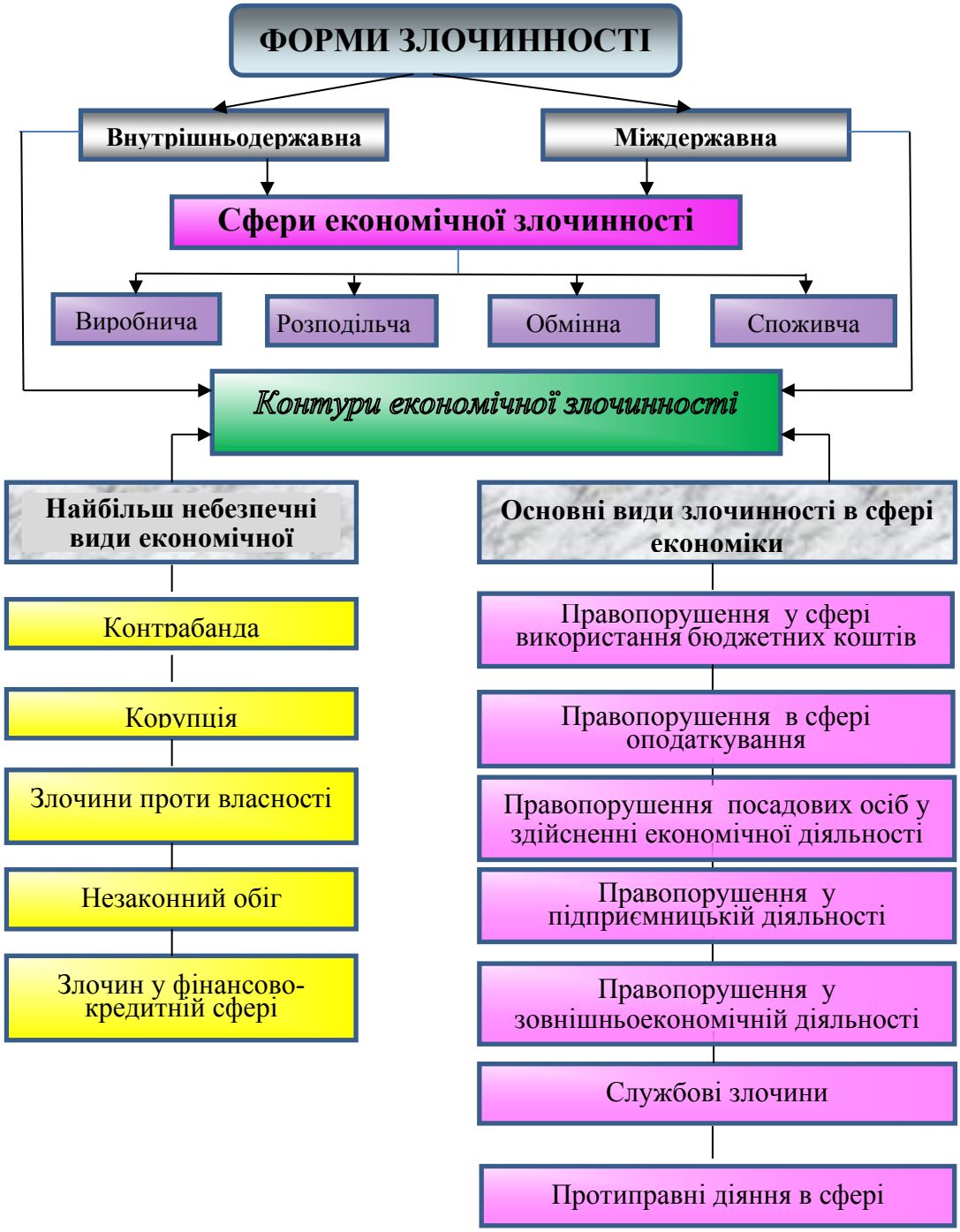

Рис. 2.1. Форми економічної злочинності

Одним з найнебезпечніших видів злочинів, який призводить до економічного занепаду держави, є легалізація (відмивання) доходів, одержаних злочинним шляхом. На рис. 2.2 наведено схему легалізації доходів тіньової економіки. Зараз широко використовується в економічних злочинах інформаційно-технічні прилади. Злочини, які вчиненні за їх допомогою відносять до кіберзлочинів. Більшість інформації знаходяться на електронних носіях, а в століття розвитку технологій, вкрасти інформацію з підприємства

не так й складно, якщо вона погана захищена [20].

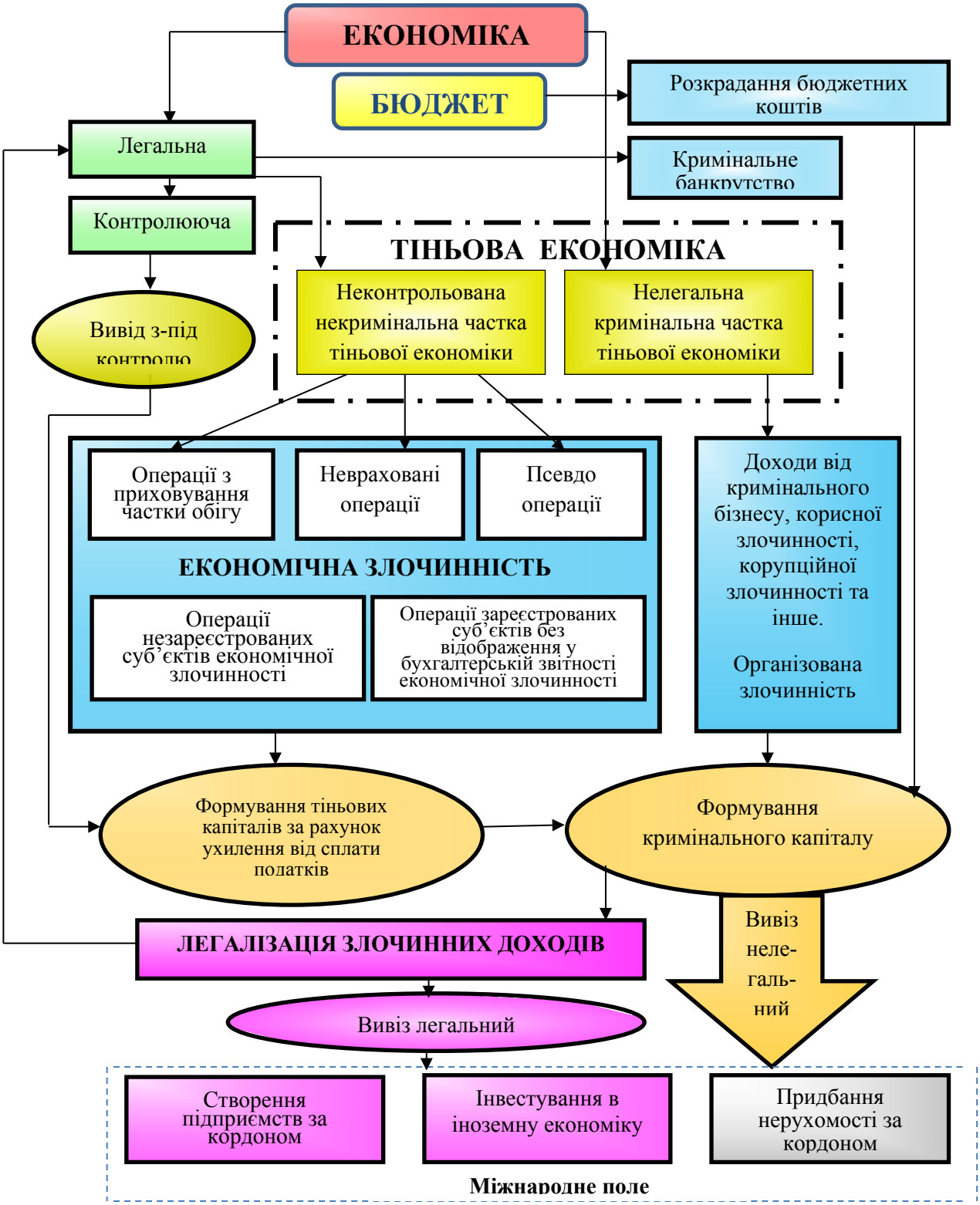

Рис.2.2. Легалізація доходів тіньової економіки

Часто в економічних злочинах використовується кіберзлочини, тому й легалізація доходів, одержаних злочинним шляхом, вчиняється з можливістю використання комп'ютерних технологій у фінансовій та банківській системі,

його ще можуть називати в деяких джерелах «кібервідмивання грошей». Тінізація економіки досягла такого масштабу, яку експерти оцінюють від 40% до 60% ВВП. Злочинні формування намагаються взяти під свій контроль банківські системи та фінансово-кредитні установи, так як саме через них проводиться процес конвертації грошових коштів, де потім їх виводять за кордон. Також є ще один із засобів легалізації та відмивання коштів злочинним шляхом через використання фіктивних фірм та конвертаційних центрів [20].

Проаналізуємо кримінальні правопорушення у 2016-2019 рр., в яких провадження закрите (табл.2.1).

Таблиця 2.1

Зареєстровані та закриті кримінальні провадження в Україні з 2016 по 2019 рр.

Рік	Зареєстровані кримінальні провадження	Закриті кримінальні провадження
2016	358 658	126 984
2017	377 432	107 794
2018	419 696	84 745
2019	480 592	70 934

Рис. 2.3. Зареєстровані та закриті кримінальні провадження в Україні з 2016 по 2019 рр.

Кількість зареєстрованих кримінальних правопорушень, вчинених на підприємствах, установах, організаціях за видами економічної діяльності йде на зростання протягом 2016-2019 рр., а кількість закритих кримінальних

проваджень зменшується. Чим менше закритих злочинів, тим менше отримано матеріальної компенсації до державного бюджету. Також через не закриті провадження досі існують ці схеми з відмивання коштів, існує тіньова економіка та люди, які «прикарманюють» гроші, що належать державі та населенню цієї держави.

2.2. Вплив тіньової економіки та економічну безпеку України

Тіньова економіка – є однією з основних складових, яка перешкоджає конкурентоспроможності, підвищенню рівня життя населення та економічному розвитку України. Рівень тіньової економіки відображає корупційну складову державних органів, рівень злочинів в економічній та політичній сферах.

Проблема, яка досліджується, є актуальною для всіх країн світу, так як тіньовою економікою є господарська діяльність, яка розвивається поза державним обліком та контролем, не відображається в офіційній статистиці, не оподатковуються власні прибутки, які мають тенденцію до зростання та виводяться за межі країни. Доходи, отримані в тіньовому бізнесу, слугують джерелом злочинної діяльності, корупції, тероризму.

Негативними факторами для ведення бізнесу у нашій країні визначено (в порядку зменшення): інфляцію, корупцію, політичну нестабільність, високі податкові ставки, складність податкового законодавства, нестабільність урядів, ускладнений доступ до фінансів, неефективну державну бюрократію, регулювання валютного ринку, недостатню освіченість працівників, погану етику робочої сили, недостатню здатність до інновацій, обмежувальне регулювання ринку праці, невідповідну якість інфраструктури, злочинність та крадіжки, низьку якість охорони здоров'я [14].

Існує кілька методів, які використовуються для оцінки динаміки рівня тіньової економіки: витрати населення – роздрібний товарооборот, електричний метод, методом збитковості підприємств, монетарний метод.

Аналізуючи динаміку рівня тіньової економіки за окремими методами, які використано у розрахунках Міністерством економічного розвитку і торгівлі, два з чотирьох методів «витрати населення – роздрібний товарооборот» та «електричний метод», з використанням яких здійснюється оцінка рівня тіньової економіки, показали її зменшення за 9 місяців 2018 року (49% від обсягу офіційного ВВП) порівняно з 9 місяцями 2017 року (51% від обсягу офіційного ВВП) на 2% «витрати населення – роздрібний товарооборот» та з 29% до 27% «електричний метод» відповідно (рис. 2.4).

Оцінки рівнів тіньової економіки, здійснені з використанням монетарного методу та методу збитковості підприємств, зафіксували відсутність змін у рівнях (порівняно з 9 місяцями 2017 року), що свідчить про "затухання" дії стимулюючих чинників у цих сферах, що формували тенденцію до зменшення рівня тіньової економіки у 2017 році та першій половині 2018 року.

За методом збитковості підприємств рівень тіньової економіки склав 22% від обсягу офіційного ВВП, а за монетарним методом зафіксував розмір тіньової економіки на рівні 22-23% від обсягу офіційного ВВП.

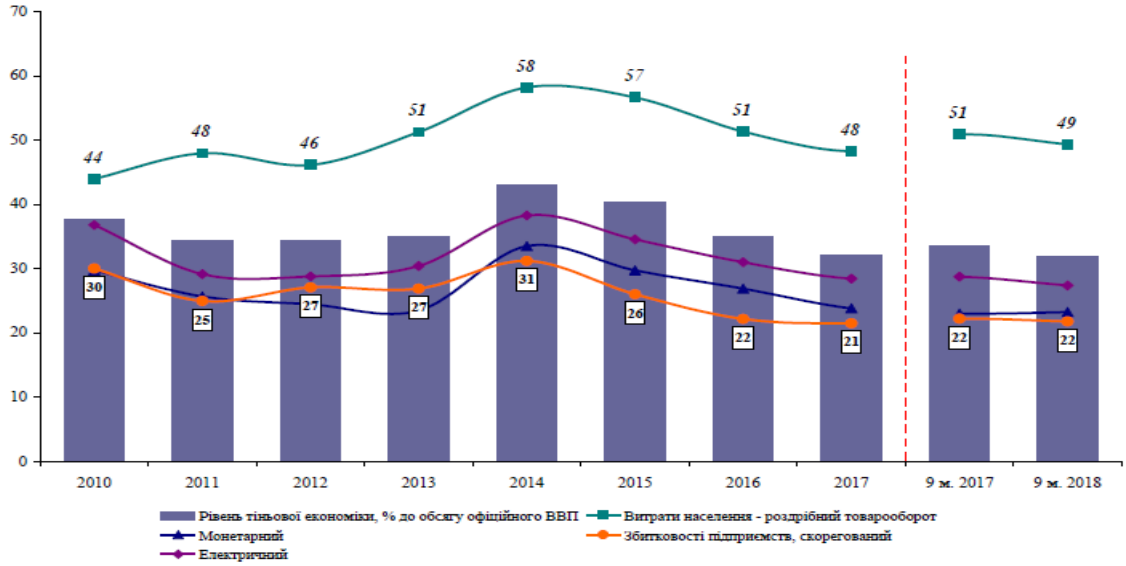

Рис. 2.4. Динаміка рівня тіньової економіки за окремими методами, % від обсягу офіційного ВВП

Кожен метод розрахунку рівня тіньової економіки охоплює сферу національної економіки (з відповідно різною часткою в ній нелегального

сектору). Тому лише інтегральний показник рівня тіньової економіки є комплексним індикатором, що характеризує тіньову економіку країни.

Цікавим є рівень тіньової економіки у видах економічної діяльності за методом збитковості підприємств (рис. 2.5).

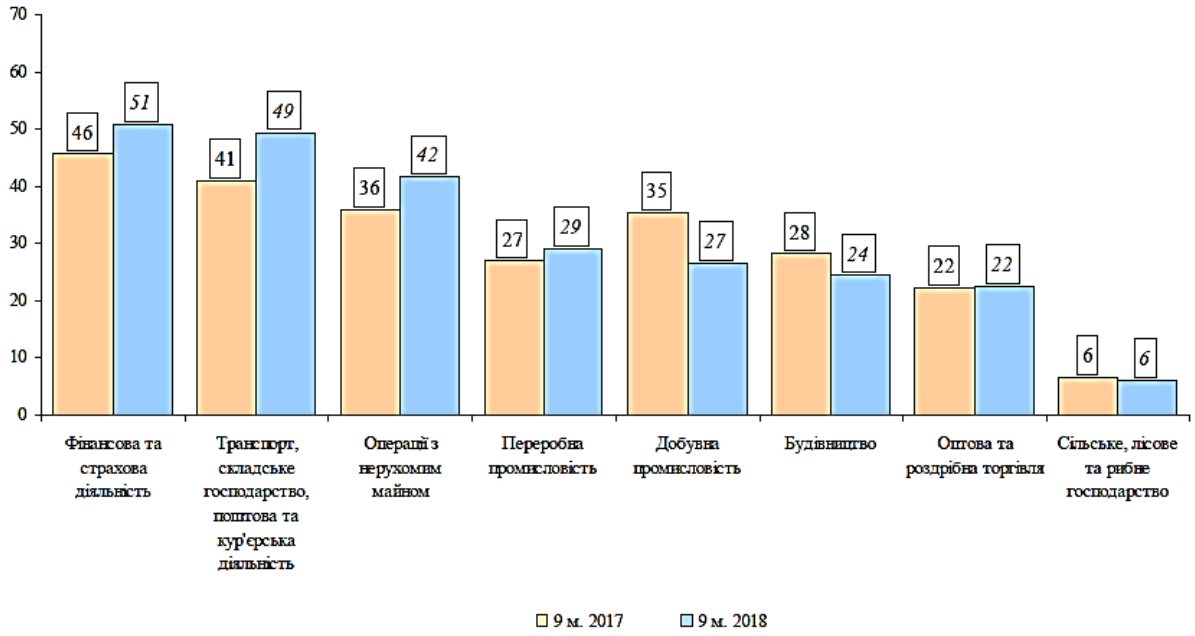

Рис. 2.5. Рівень тіньової економіки за видами економічної діяльності, % від обсягу офіційного ВДВ відповідного ВЕД

Тенденція до зменшення рівня тіньового сектору за підсумком січня-вересня 2018 року збереглася у двох основних видах економічної діяльності (ВЕД) – добувній промисловості (з 35% до 27%) (до відповідного періоду 2017 року) та будівництві (з 28% до 24%) (рис. 2.5).

Чотири ВЕД, а саме: “Фінансова та страхова діяльність”, “Транспорт, складське господарство, поштова та кур’єрська діяльність”, “Операції з нерухомим майном” та «Переробна промисловість» показали збільшення рівня тіньової економіки, отримане в умовах зростання обсягів збитків підприємств цих ВЕД.

Як наслідок, рівень тіньової економіки у ВЕД “Транспорт, складське господарство, поштова та кур’єрська діяльність” збільшився на 8% (із 41% до 49%) порівняно з відповідним періодом 2017 року; у «Переробній промисловості» – на 2% (з 27% до 29%) відповідно. Збільшення рівня тіньової

економіки у ВЕД “Операції з нерухомим майном” – на 6% (з 36% до 42%) порівняно з рівнем 9 місяців 2017 року), у ВЕД “Фінансова та страхова діяльність” – 5% (з 46% до 51%) відповідно.

Рівень тіньової економіки в оптовій та роздрібній торгівлі, а також “Сільське, лісове та рибне господарство” порівняно з 9 місяцями 2017 року не змінився. При цьому перелік найбільш тінізованих ВЕД очолив ВЕД “Фінансова та страхова діяльність” (51% від обсягу ВДВ у ВЕД).

Традиційно низьким рівень тіньової економіки залишився у ВЕД “Сільське, лісове та рибне господарство” – 6% від обсягу валової доданої вартості у відповідному виді економічної діяльності.

Світовий рейтинг економічної безпеки у 2010-2019 роках [16] побудовано за такими основними показниками, як: право власності, судова ефективність, цілісність влади, податковий тиск, державні витрати, фізичне здоров’я, свобода ведення бізнесу, право на вільну працю, вільність грошових відносин, вільність торгівельних відносин, інвестиційна та фінансова незалежність (рис. 2.6) [17, 19].

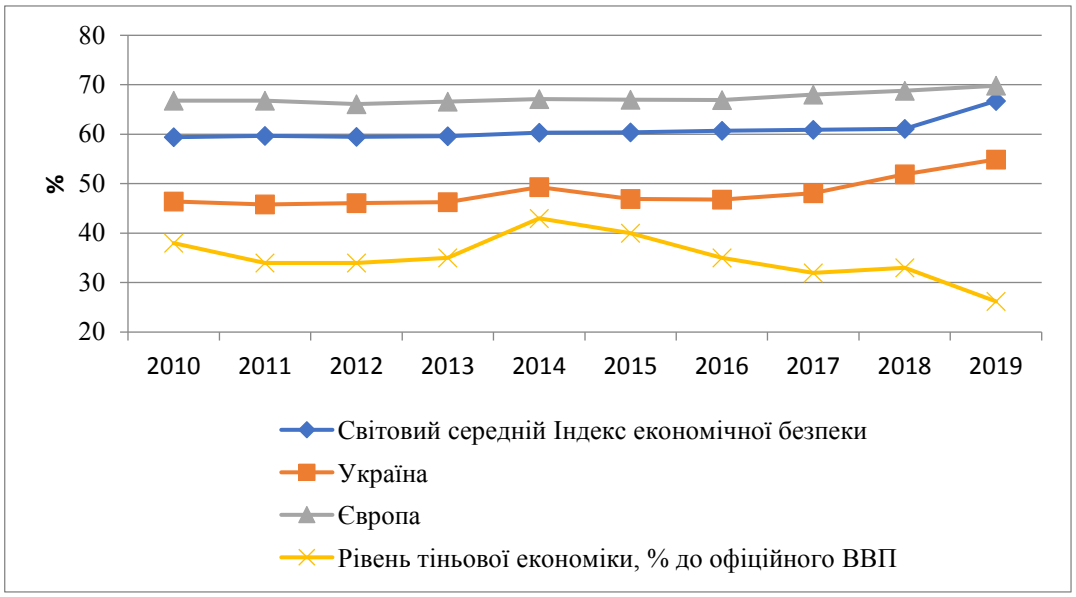

Рис. 2.6. Світовий індекс економічної безпеки у 2010-2019 рр.

Індекс економічної безпеки показує взаємозв’язок між економічною незалежністю та цілим рядом соціально-економічних показників. Економічна незалежність пов’язана із станом охорони здоров’я, екологією, доходами на

душу населення, розвитком людського потенціалу, демократією та боротьбою із злиднями. Досліджуючи динаміку рівня економічної безпеки України за 2010–2019 рр. (рис. 2.6), можемо зробити висновок, що Україна знаходиться нижче середнього світового індексу рівня економічної безпеки та спостерігається обернена залежність між рівнем економічної безпеки та рівнем тіньової економіки. Так, зі зростанням рівня тіньової економіки у 2014 році зменшується рівень економічної безпеки України, а у 2019 році із зменшенням рівня тіньової економіки відбулося зростання рівня економічної безпеки України. Отже, тінізація господарської діяльності є реальною загрозою економічній безпеці України та негативно позначається на всіх сферах суспільного життя, істотно впливає на обсяги та структуру ВВП, спотворює офіційні дані про реальний стан економіки, спричиняє втрату податкових надходжень, провокує несправедливий та непрозорий розподіл національного доходу в суспільстві.

Високий обсяг тіньового сектору в національній економіці негативно впливає на економічний розвиток та стан економічної безпеки окремих галузей економіки та країни в цілому. Тіньова економіка є причиною поглиблення наявних в економіці дисбалансів, залишаючись одним з найбільших викликів економічній безпеці держави, тенденції зміни яких сьогодні та в подальшому визначатимуть сценарії розвитку економіки країни.

Досліджуючи системні фактори тінізації національної економіки, необхідно зазначити, що до однієї з основних загроз, яку представляє тіньова економіка для економічної системи, є спотворення механізмів дії законів та інструментів ринку, що призводить до неефективності механізмів стимулювання економіки, стримуючи економічний розвиток країни.

Актуальними на сьогоднішній день є такі чинники тінізації економіки, як:

- ✓ високий рівень корупції;

За даними рейтингу “Індекс сприйняття корупції 2019” за рівнем корупції Україна посідає 126 місце із 180 країн (у 2017 р. – 30 балів, 130-е

місце). Серед сусідів Україні вдалося обійти лише Росію, яка з 28 балами займає 137-е місце, Польща – 41 місце, Словаччина – 59 місце, Білорусь – 66 місце [15]. Основні показники, за якими Україна традиційно займає низькі місця у рейтингу:

- ✓ організована злочинність (Україна посідає 110 місце із 140 країн світу);
- ✓ низька ефективність функціонування органів судової системи (незалежність судів – 117 місце, ефективність правової бази – 107 місце);
- ✓ випадки тероризму (131 місце);
- ✓ захист прав власності (129 місце);
- ✓ захист прав інтелектуальної власності (114 місце);
- ✓ рівень інфляції (130);
- ✓ платоспроможність банків (135 місце);
- ✓ низький рівень життя населення країни (192 місце серед 226 країн);
- ✓ непередбачуваність змін у податковому законодавстві, що спричиняє збільшення кількості помилок економічних суб'єктів при нарахуванні та сплаті податків і зборів, а також несприятливі умови ведення бізнесу [17].

2.3. Типові схеми легалізації доходів

У відмиванні грошей використовується велика кількість схем, які доволі важко виявити, адже слід враховувати особливості кожного з національних законодавств. Національний Банк України (НБУ) розкрив сім основних схем по відмиванню грошей.

Схема № 1 – «Виведення капіталу», вона дозволяє вивести гроші з України, що в свою чергу має малий вплив на попит/пропозицію валюти і курс (рис.2.7).

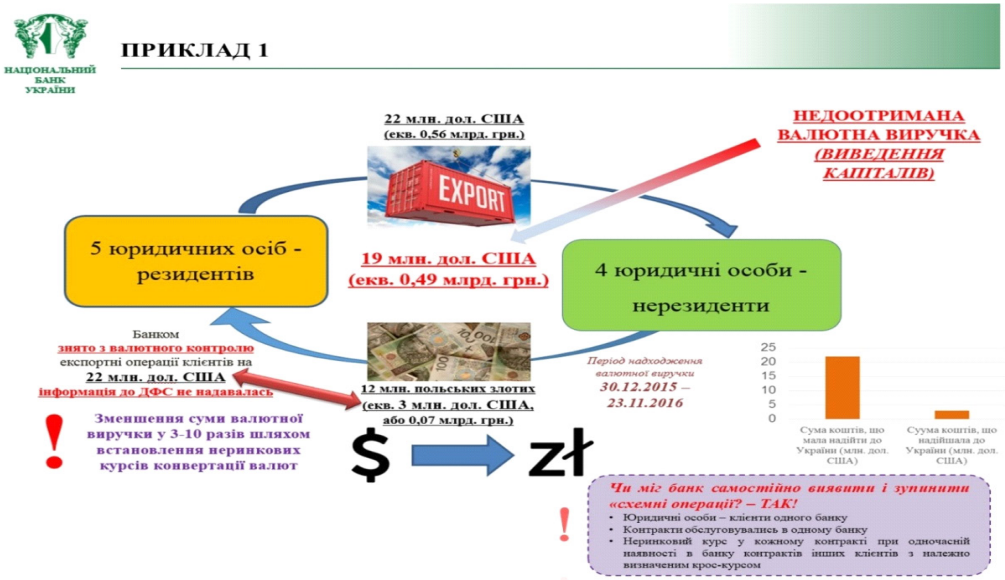

Рис.2.7. Схема «Виведення капіталу»

Схема № 2 – «Переведення в готівку», тобто зняття фізичними особами готівки, що в свою чергу служить, як оплата за будь який необхідний ресурс (рис. 2.8).

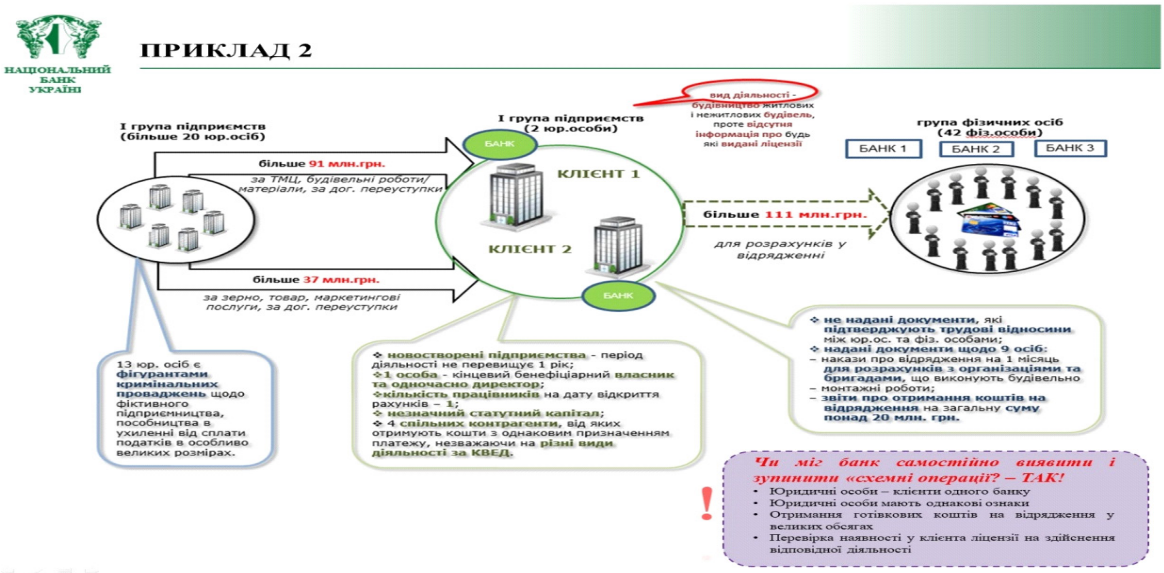

Рис.2.8. Схема «Переведення в готівку»

Схема № 3 – «Корупційна», незаконна діяльність, що приносить доходи, зокрема скоєння злочинів, випадає зі сфери, що регулюється економічними законами і принципами (рис.2.9).

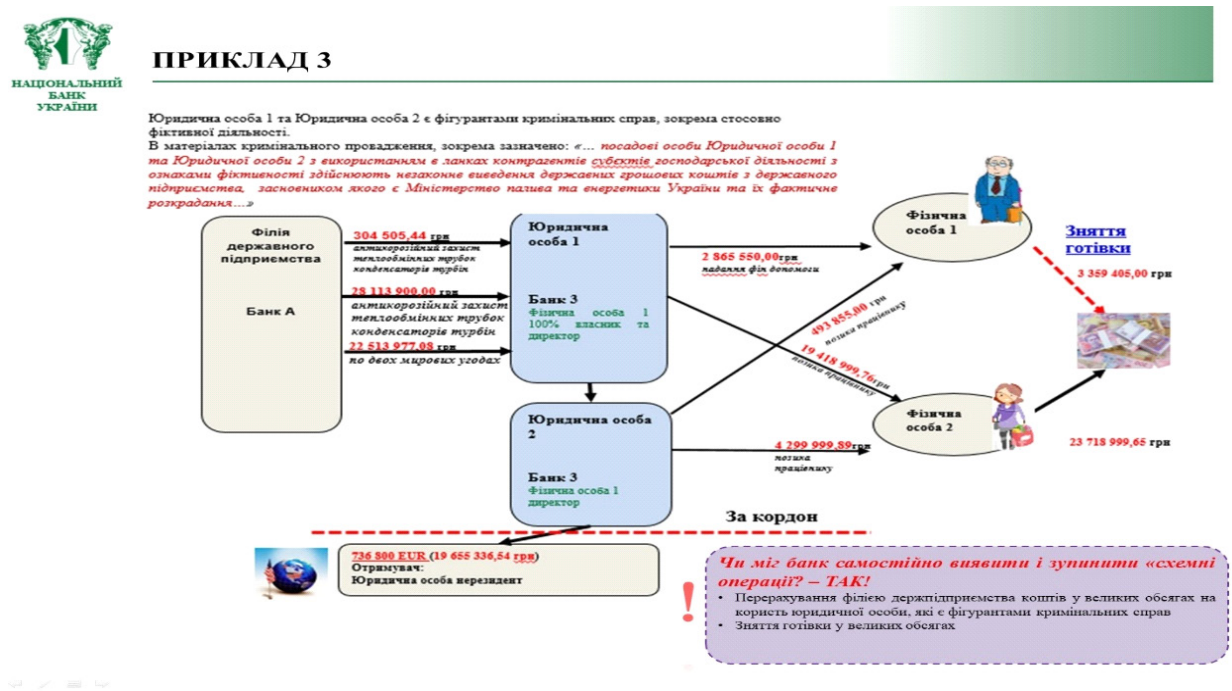

Рис.2.9. Схема «Корупційна»

Схема № 4 – «Котел», так як незаконні операції переведення у готівку проводилися через банківську систему, компанії які брали й продавали свою готівкову виручку замість процедури інкасації, отримували свій відсоток грошей в безготівковій формі (рис. 2.10).

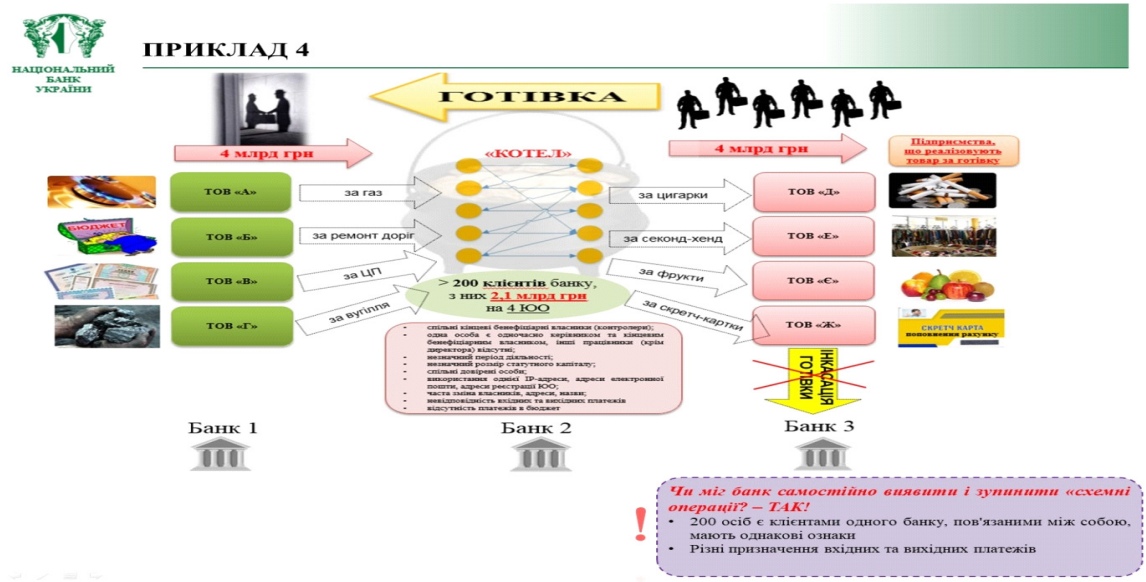

Рис. 2.10. Схема «Котел»

Схема № 5 – «Отримання готівки», група компаній через банк сплачувала збір вторинної сировини для подальшої обробки та саме за цією схемою банк видавав «на руки» велику суму грошей (рис.2.11).

Рис.2.11. Схема «Отримання готівки»

Схема № 6– «Готівка без готівки», це ще один приклад конвертації безготівкових коштів у готівку без інкасації (рис.2.12).

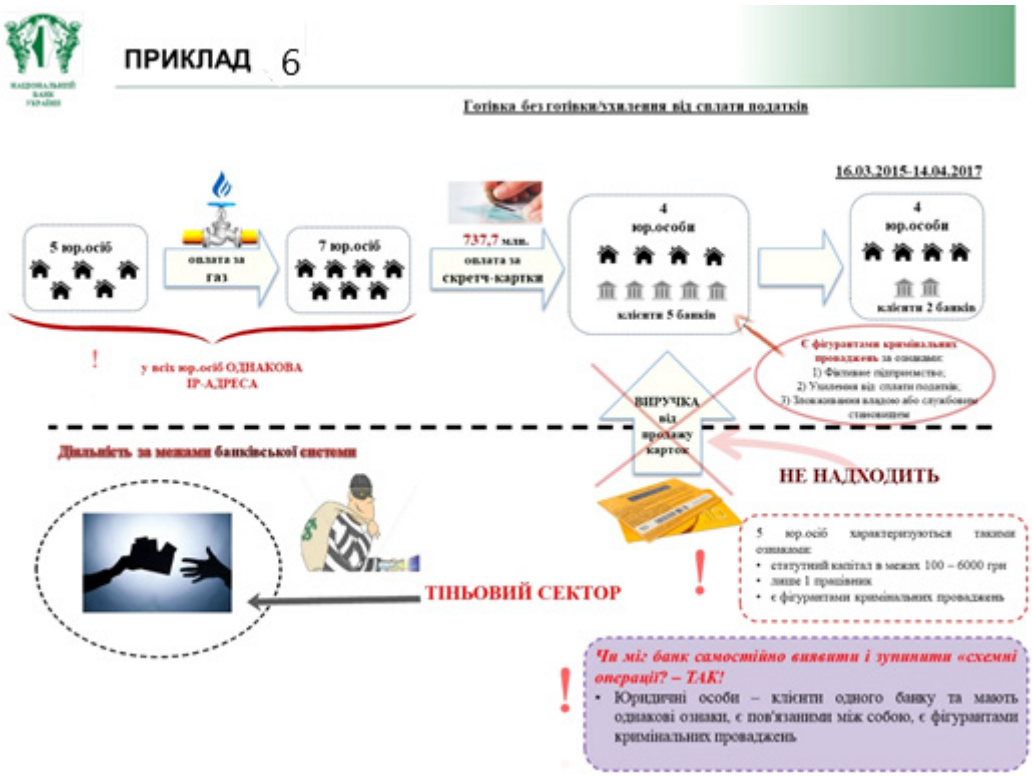

Рис.2.12. Схема «Готівка без готівки»

Схеми, які оприлюднив НБУ, стосуються не лише підприємств, які займаються відмиванням коштів, але й банків [4]. Згідно статистиці на початку 2018 року НБУ сформував та впровадив заходи впливу на окремі банки за порушення фінансового моніторингу. У 2019 році Національний Банк

здійснив перевірки відповідно до Постанови НБУ №197 «Про затвердження Положення про порядок організації та проведення перевірок з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом». Банківські системи постійно удосконалюють систему попередження легалізації доходів злочинним шляхом, за допомогою міжнародного співробітництва з провідними європейськими організаціями. FATF – провідна міжнародна група з протидії відмиванню незаконних доходів впроваджує заходи та стандарти боротьби з відмивання коштів на національному та міжнародному рівнях.

Боротьба з економічними злочинами забезпечується не тільки правоохоронними органами, але є ще інші державні організації та громадські формування, які сприяють подоланню цієї проблеми в країні. Згідно законодавства до правоохоронних органів, які приймають участь у боротьбі зі злочинами в економічному секторі, входять спеціальні державні органи.

Взаємодія суб'єктів, на яких покладено завдання ліквідації здійснення економічних злочинів сприяє ефективності нейтралізації відповідних чинників, які в свою чергу сприяють розвитку та зростанню злочинів в секторі економіки держави. Для боротьби з економічними злочинами діють такі закони України: «Про оперативно-розшукову діяльність», «Про запобігання та протидію корупції», «Про Національну поліцію» та ін.

2.4. Викриття нелегальних конвертаційних центрів правоохоронними органами України

Для відмивання грошей використовується багато зусиль і витрат, які ми проаналізували з поданих схем Національного Банку України, але одним із основних джерел проходження коштів незаконним шляхом у тіньовому обігу є використання послуг конвертаційних центрів. З роками, послуги конвертаційних центрів стали набагато ширшими та різноманітними, вони набули організованості у своїй роботі [18]. Через багату кількість вчинених

злочинів економічного характеру, країна страждає від ненадходження відповідної суми грошей до державного бюджету, які повинні надходити від податків, зборів, обов'язкових платежів, а також від прямого відтоку грошових ресурсів за кордон.

Конвертаційний центр можна охарактеризувати, як спеціалізоване злочинне угрупування з надання послуг незаконної конвертації грошей при використанні фіктивних фірм, імітації фінансово-господарських відносин, а також фальсифікації облікових та звітних документів. Якщо говорити простішою мовою, то це незаконні організації, які представляють послуги незаконного відмивання грошей.

У ролі організатора створення конвертаційних центрів виступають особи, які добре підготовлено економічно, юридично та організаційно, вони мають гострий ум та вміють швидко мислити. Конвертаційні центри існують протягом кількох років, потім вони ліквідуються і згодом створюються нові на вже існуючій базі, це такий один із засобів замітання слідів. Такі незаконні структури реєструються за допомогою підроблених чи крадених паспортів. Одним із головних завдань цих псевдокомерційних організацій є уникнення кримінальної відповідальності, тому як засновників та і директорів вони обирають осіб з числа малозабезпеченого населення, тобто шукають серед студентів, пенсіонерів, які готові за певну матеріальну суму грошей підписати необхідні папери. Але через саме це незнання та бажання швидких та легких грошей приходиться відповідати перед законом підставним громадянам, які нерідко навіть не підозрюють, що є власниками підприємств з багатомільйонними оборотами.

Схеми проведення відмивання грошей конвертаційних центрів дуже схожі зі схемами відмивання грошей, які були зазначені у другому розділі оприлюдненні НБУ. Тому перейдемо саме до головного: скільки, де та як ліквідовувались данні конвертаційні центри.

За даними офіційного порталу ДФС України у 2016 році ліквідовано 42 конвертаційні центри із загальною сумою проконвертованих коштів - більше

16,6 млрд.грн. Від такої протиправної діяльності втрати бюджету склали понад 2,9 млрд.грн. За результатами перевірок до бюджету додатково стягнуто понад 206 млн.грн. У 2017 році податківцями ліквідовано 65 конвертаційних центрів. Обсяг проконвертованих коштів становив 13,5 млрд грн.

У 2018 році ліквідовано 50 конвертаційних центрів. Обсяг проконвертованих коштів склав 11,3 млрд грн. Основним акцентом при проведенні заходів з документування протиправної діяльності «конвертів» є відшкодування завданих державі збитків.

Слідчі ДБР спільно з НАБУ та СБУ викрили незаконну діяльність конвертаційного центру, що діяв протягом 2018-2019 років у Львові. За даними правоохоронців, щомісячний тіньовий обіг центру складав 500 млн. грн. У травні 2019 року детективи ДБР та НАБУ провели обшуки у Головному управлінні ДФС Львівської області. Під час досудового розслідування правоохоронці виявили схему виведення у тіньовий сектор безготівкових коштів підприємств та державних коштів завдяки конвертації їх в готівку. Діяльність конвертаційного центру припинена [11].

У рамках розслідування кримінального провадження, відкритого за ч.3 ст.212 (ухилення від сплати податків, зборів, інших обов'язкових платежів) Кримінального кодексу України було встановлено, що група осіб через підконтрольні їм транзитно-конвертаційні та фіктивні підприємства надавала послуги з конвертації коштів з безготівкової форми у готівкову та формування податкового кредиту підприємствам реального сектора економіки переважно з м.Києва та Київської області [12].

Податковий кредит з ПДВ для фірм - учасників конвертаційного центру відображався за рахунок нібито придбаних товарів у сільгоспвиробника без фактичного перерахування грошових коштів на його рахунки. Крім того, реально діючі підприємства переказували безготівкові кошти на рахунки підконтрольних учасникам центру транзитних та фіктивних фірм за нібито придбані товарно-матеріальні цінності. Після цього частина коштів знімалася готівкою через касу банку під виглядом оплати за товари постачальникам.

Незаконно проконвертовані готівкові гроші за винятком 10-11%, які служили «винагородою», разом із підробленими первинними документами передавалася «клієнтам» - посадовцям фірм реального сектора економіки.

Також учасниками конвертаційного центру планувалося незаконне використання рахунків 16 благодійних організацій для переказу коштів підприємствам реального сектора економіки під виглядом надання допомоги інтернатам та організаціям для дітей-сиріт. Зловмисники планували імпортувати в Україну гуманітарну допомогу, що не оподатковується, але, за наявною інформацією, учасники конвертаційного центру збиралися реалізовувати одержані товари на внутрішньому ринку України з метою отримання прибутку [12].

У своїй протиправній діяльності учасники групи використовували розрахункові рахунки, відкриті у п'ятьох банківських установах. Загальний обсяг проконвертованих коштів становив понад 200 мільйонів гривень, можливі втрати бюджету - понад 30 мільйонів.

Внаслідок здійснених у Києві дев'яти обшуків було знайдено та вилучено 320 тисяч гривень, комп'ютерну техніку, первинну і бухгалтерську документацію, банківські картки та чорнові записи, 42 печатки, чотири з яких - печатки благодійних фондів. Усі вилучені під час проведення слідчих дій речі і документи долучено до матеріалів кримінального провадження як речові докази. Слідчі дії тривають [12].

Таким чином, розвиток України як незалежної європейської держави залежить від ефективного функціонування економіки. Вона являє собою життєдіяльність та розвиток людини, суспільства і держави, виступає важливою складовою національної безпеки, від якої залежить захищеність владі, її суверенітет, територіальна цілісність та обороноздатність, спокій людей та інше. Тому важливо розробити концепцію для ефективного функціонування забезпечення економічної безпеки. Головним питанням є ліквідація корупції, тіньової економіки, економічної злочинності та порушення цілісності економічної системи України. Данні чинники

призводять до негативних наслідків, які розповсюджуються на бізнес, державу та кожного громадянина.

Проблема захищеності економіки та її безпеки є ключовою для існування будь-якої держави. Головною метою економічної безпеки є захищеність національних інтересів держави, готовність усіх гілок влади створити механізм захисту економіки своєї держави, зберегти та поновити процес відтворення соціально-політичної стабільності суспільства.

До основних загроз в умовах глобалізації та внутрішньої нестабільності економічної безпеки України відносять: соціально-політичні конфлікти, велика кількість невдоволеного та агресивно налаштованого населення, високий рівень внутрішньої та зовнішньої міграції населення, високий рівень тінізації в економічному секторі, зростання безробіття, корупція та інше.

Впровадження до дієвого процесу ефективної моделі концепції державної політики економічної безпеки, передбачає захист національних економічних інтересів, протистояння загрозам різного характеру, захист та забезпечення економічних свобод суб'єктів підприємництва і населення, усунення негативних проявів економічної, соціальної та політичної глобалізації.

На даний час Україна тісно співпрацює з країнами європейського союзу для поліпшення рівня безпеки країни. Для України є важливим також розвиток та партнерство зі Сполученими Штатами Америки. Така співпраця сприяє укріпленню демократії та верховенства права, протидії корупції і проведення реформ в Україні, розвитку економічного стану та її адаптації на світовому ринку, підвищення обороноздатності, зміцнення безпеки, розвитку науки та технологій, а також розвиток національної економіки [7].

Забезпечення високого рівня економіки можливо за допомогою процесу активізації внутрішніх факторів та зменшення негативного впливу зовнішніх чинників на соціально-економічний аспект забезпечення економічного розвитку. Це передбачається застосуванням внеску до економіки держави фінансових ресурсів, за допомогою таких засобів, як:

- деофшоризація, сприяє формуванню правових засад захисту прав інвесторів, оптимізації зменшення податкового тиску на підприємницьку діяльність;
- боротьба із корупцією, відхід від збагачення шляхом зловживання людськими цінностями;
- залучення заощаджень населення в інвестиційні ресурси;
- зміцнення валютної системи;
- впровадження кредитної політики НБУ, яка сприяє зниженню облікової ставки з метою здешевлення кредитів для національного господарства;
- створення державних інвестицій, що в свою чергу допоможе удосконалити програмно-цільовий підхід в державному фінансуванні програм соціально-економічного розвитку, галузевих, регіональних та науково-технічних програм для реалізації механізмів державно-приватного партнерства [3].

Для держави під час формування політики економічної безпеки першочерговим значенням є визначення національних інтересів, так як від цього залежить створення ефективних заходів їх реалізації та захисту.

2.5. Стратегія сталого розвитку держави на період до 2030 року

Стратегія сталого розвитку України до 2030 року орієнтована на вектори, визначені в Стратегії сталого розвитку «Україна – 2020» [13]:

- *вектор розвитку* – забезпечення сталого розвитку країни, проведення структурних реформ, забезпечення економічного зростання екологічно невиснажливим способом, створення сприятливих умов для ведення господарської діяльності;
- *вектор безпеки* – забезпечення безпеки держави, бізнесу та громадян, захищеності інвестицій та приватної власності, забезпечення миру і захисту кордонів, чесного та неупередженого правосуддя, невідкладне проведення

очищення влади на всіх рівнях та забезпечення впровадження ефективних механізмів протидії корупції. Пріоритетом є безпека життя та здоров'я людини, що неможливо без ефективної системи охорони громадського здоров'я, надання належних медичних послуг, захищеності соціально вразливих верств населення, безпечного стану довкілля і доступу до якісної питної води й санітарії, безпечних і якісних харчових продуктів та промислових товарів;

- *вектор відповідальності* – забезпечення гарантій кожному громадянину, незалежно від раси, кольору шкіри, політичних, релігійних та 6 інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, мовних або інших ознак, мати доступ до високоякісної освіти, системи охорони здоров'я та інших послуг в державному та приватному секторах;
- *вектор гордості* – забезпечення взаємної поваги та толерантності в суспільстві, гордості за власну державу, її історію, культуру, науку, спорт [13].

Метою Стратегії є забезпечення високого рівня та якості життя населення України, створення сприятливих умов для діяльності та припинення деградації природних екосистем шляхом впровадження нової моделі економічного зростання, що базується на засадах сталого розвитку.

Економічне зростання буде пов'язане з широким застосуванням моделей «зеленої» економіки. Застосування заходів енергозбереження та енергоефективних технологій призведе до зростання екологічно чистої енергії, що сприятиме поліпшенню якості довкілля і здоров'я населення. Розвиток орієнтований на поліпшення якості життя населення, соціально-економічний розвиток, чисту екологію та здоровий стан життя. Високий інтелектуальний рівень потенціалу населення сприятиме зростанню конкурентоспроможності країни у майбутньому.

Реалізація Стратегії спрямована на подолання бідності шляхом ефективності зайнятості населення, високої вартості робочої сили, накопичення людського і соціального капіталу, розвитку підприємницької

активності населення, зміцнення середнього класу, підвищення соціальних стандартів і гарантій, а також надання необхідної соціальної підтримки вразливим групам населення [13].

Завданнями операційної цілі 1.2 «Сприяти інклюзивному енергоефективному та інноваційному промисловому розвитку» є:

1. До 2030 зменшити ступінь зносу до 40% та забезпечити оновлення основних засобів на 50% у таких видах економічної діяльності, як «транспорт, складське господарство, поштова та кур'єрська діяльність».

2. Сформувати організаційну інфраструктуру підтримки підприємництва у вигляді технопарків, бізнес-інкубаторів, мереж надання послуг підприємствам, зокрема на засадах державно-приватного партнерства; сприяти розвитку кластерних мереж.

3. До 2030 року модернізувати інфраструктуру і підприємства базових галузей промисловості, зробивши їх збалансованими за рахунок підвищення ефективності використання природних ресурсів та ширшого застосування енергоефективних і екологічно безпечних технологій чистого виробництва та інтегрованих систем управління згідно з міжнародними стандартами.

4. До 2030 року наростити частку реалізованої інноваційної продукції в обсязі промислової продукції до 15%.

5. Активізувати наукові дослідження, нарощувати технологічний потенціал промислових секторів, зокрема шляхом стимулювання інноваційної діяльності [13].

Ключовими показники у досягненні Стратегії розвитку є [13]:

1. Економічне зростання. Забезпечити щорічне зростання валового внутрішнього продукту (ВВП, %): 2021–2025 рр. – 106; 2026–2030 рр. – 107.

2. Структура експорту. Сприяти зростанню питомої ваги продукції та послуг з високою часткою доданої вартості в експорт.

3. Розвиток підприємництва:

✓ заохочувати розвиток мікро-, малих і середніх підприємств. Кількість зайнятих працівників на середніх і малих підприємствах, фізичних

осіб – суб'єктів малого підприємництва, (млн осіб): 2020 рік – 8,3; 2025 рік – 9,5% 2030 рік – 10,5;

✓ сформувати організаційну інфраструктуру підтримки підприємництва. Позиція у рейтингу легкості ведення бізнесу Doing Business: 2020 рік – 73; 2025 рік – 53; 2030 рік – 33.

4. Протидія корупції.

Показник сприйняття рівня корупції в державному секторі з боку ділових кіл та експертів («Індекс сприйняття корупції» за методологією Transparency International): 2020 рік – 40; 2025 рік – 50; 2030 рік – 60.

5. Наукові дослідження.

Активізувати наукові дослідження. Питома вага вартості виконаних наукових і науково-технічних робіт у ВВП, (%): 2020 рік – 1,0; 2025 рік – 2,5; 2030 рік – 3,0.

6. Промисловий розвиток.

Модернізувати інфраструктуру та підприємства базових галузей промисловості. Частка реалізованої інноваційної продукції в обсязі промислової продукції, (%): 2020 рік – 7,0; 2025 рік – 10,0; 2030 рік – 15,0.

Список використаних джерел до розділу 2

1. Military Strength Ranking 2018 (Рейтинг военной силы 2018 года). URL: https://www.globalfirepower.com/countries-listing.asp (дата звернення 08.11.2019).

2. Report To The Nations. 2018 Global Study On Occupational Fraud And Abuse. URL:https://www.acfe.com/report-to-the-nations/2018/#download (дата звернення 04.11.2019).

3. Tymoshenko, O. and Oleshko, A. (2018), "State policy of economic security of Ukraine in conditions of global instability", Ekonomika ta derzhava, vol. 9, pp. 30–33. DOI: 10.32702/2306-6806.2018.9.30 (Accessed 4 June 2019).

4. Державна служба статистики України. URL: http://www.ukrstat.gov.ua (дата звернення 03.11.2019).

5. Лекарь С.І. Поняття та зміст економічної безпеки: Форум права, 2012.

С. 399-402.

6.Офіційний портал Верховної ради України URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66516 (дата звернення 06.11.2019).

7. Середюк Н. Стратегічне партнерство Україна–США // Вісник Київського національного університету імені Тараса Шевченка №1 (46) 2017. С.34-38. URL: http://journals.iir.kiev.ua/index.php/knu/article/viewFile/3261/2936 (дата звернення 05.11.2019).

8. Скорук О. В. Економічна безпека держави: сутність, складові елементи та проблеми забезпечення. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/10961/1.pdf. (дата звернення: 06.11.2019).

9. Фінансовий портал Міністерства фінансів України. URL: http://index.minfin.com.ua/index/gdp. (дата звернення: 29.10.2019).

10. Як в Україні карають за економічні злочини та що з цим робити? Адвокатське об'єднання «Barristers». URL: https://barristers.org.ua/news/kozhen-p-yatyj-yak-v-ukrayini-karayut-za-ekonomichni-zlochyny-ta-shho-z-tsym-robyty. (дата звернення 07.11.2019).

11. Львівських податківців підозрюють у причетності до створення конвертаційного центру. URL : https://zaxid.net/lvivskih_podatkivtsiv_pidozryuyut_u_prichetnosti_do_konvertatsiynogo_tsentru_z_oborotom_500_mln_grn_n1480828.

12. Державна фіскальна служба України. Офіційний портал. URL : http://kyiv.sfs.gov.ua/media-ark/news-ark/print-261942.html

13. Проект стратегії сталого розвитку України до 2030 року. URL :http://sd4ua.org/wp-content/uploads/2015/02/Strategiya-stalogo-rozvytku-Ukrayiny-do-2030-roku.pdf

14. Офіційний сайт Міністерства економічного розвитку і торгівлі України. URL: http://www.me.gov.ua

15. Індекс сприйняття корупції-2019. Трансперенсі Інтернешнл. URL: https://ti-ukraine.org/research/indeks-spryjnyattya-koruptsiyi-2019/

16. Economic Data and Statistics on the World Economy and Economic Freedom. 2019 Index of Economic Freedom. URL: https://www.heritage.org/index/ranking

17. Рибальченко Л.В., Рижков Е.В., Косиченко О.О. Вплив тіньової економіки на економічну безпеку України / Л.В. Рибальченко, Е.В. Рижков, О.О. Косиченко // Науковий вісник Дніпропетровського державного університету внутрішніх справ. - 2019. - № 2 (99). – С. 175-183

18. Методичні рекомендації з виявлення конвертаційних центрів / І.В. Кокарєв, Л.В. Рибальченко, Е.В. Рижков, К.Г. Сидоренко. - Дніпро: ДДУВС, 2019. - 24 с.

19. Рибальченко Л.В. Вплив інфляційних процесів на фінансову безпеку держави / Л.В. Рибальченко // Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали Всеукр. наук.-практ. семінару (23 листопада 2018 р., м. Дніпро). – Дніпро: ДДУВС, 2018. – С. 77-78

20. Документування та викриття діяльності організованих злочинних груп, пов'язаної з мінімізацією доходів та легалізацією коштів / І.В. Кокарєв, Л.В. Рибальченко, Е.В. Рижков, К.Г. Сидоренко, С.М. Тютченко. – Дніпро : ДДУВС, 2019. – 32 с.

21. Rybalchenko L., Kosychenko O. Features of latency of economic crimes in Ukraine / L.Rybalchenko, O. Kosychenko // SCIENTIFIC BULLETIN OF THE DNIPROPETROVSK STATE UNIVERSITY OF INTERNALAFFAIRS. 2019. SPECIAL ISSUE № 1.- P.264-267

22. Рибальченко Л.В., Косиченко О.О. Проблеми безпеки персональних даних в Україні / Регіональна економіка та управління / Запоріжжя. 2019. – с.57-62

23. Рибальченко Л.В., Косиченко О.О. Латентність економічних злочинів як загроза безпеці підприємництва в Україні / Регіональна економіка та управління 3 (25) серпень 2019 р. – С. 68-73

РОЗДІЛ 3. ЕКОНОМІЧНІ ЗЛОЧИНИ ЯК ЗАГРОЗА БЕЗПЕЦІ ПІДПРИЄМНИЦТВА В УКРАЇНІ

3.1. Забезпечення економічної безпеки підприємства

Від надійності системи захисту від внутрішніх і зовнішніх загроз залежить ефективність функціонування підприємств. Все це надає підвищеної значущості та актуальності дослідженню проблеми управління економічною безпекою підприємництва в Україні. Перед підприємствами потреба у створенні системи економічної безпеки є особливо актуальною.

Економічна безпека фірми неможлива без створення, регулювання і підтримки державою сприятливих для цього умов. Зростання чисельності підприємств із високим рівнем економічної безпеки сприятиме зміцненню економічної безпеки України.

Економічну безпеку підприємства розглядають як стан ефективного використання його ресурсів та існуючих ринкових можливостей, які дають змогу відвернути внутрішні та зовнішні загрози і забезпечити його тривале виживання і стійкий розвиток на ринку щодо обраної місії. Для фірми, незалежно від її розміру, сфери діяльності існують загрози в розвитку, які виникають всередині підприємства або надходять ззовні. Система економічної безпеки покликана захистити фірму від внутрішніх і зовнішніх загроз, зберегти та ефективно використати її матеріальний і фінансовий потенціал.

Економічна безпека фірми – це захист від можливих матеріальних і фінансових збитків, здатних призвести до банкрутства і ліквідації фірми, тому безпека підприємницької діяльності тісно пов'язана з ризиками, які є складовою ринкової форми господарювання. Безпека підприємництва спрямована на зменшення чи усунення ризику економічних збитків [1].

Господарська діяльність малих підприємств є найбільш ризикованою. На величину ризиків малих підприємств впливають: недостатність фінансових ресурсів; короткий життєвий цикл; незначний асортимент продукції; повна

відповідальність за зобов'язання та борги як майном підприємства, так і всім особистим майном; інноваційно-інвестиційна діяльність [2].

Малі підприємства і громадяни-підприємці діють на локальному ринку, який характеризується високим рівнем невизначеності та стихійності. Основна суперечність малого бізнесу полягає в суперечності між низькою життєздатністю малого підприємництва і суспільною корисністю, тому система економічної безпеки малих підприємств підвищує життєздатність малого бізнесу, пом'якшує суперечність.

Забезпечення конкурентоспроможності підприємства можливе за умови створення ефективної системи управління. В основу побудови такої системи покладено науково обґрунтовану концепцію, що враховує, з одного боку, особливості діяльності підприємства, а з іншого – його становище на ринку і стан зовнішнього середовища. Спільна реалізація цих вимог може бути забезпечена в рамках стратегічного управління.

Економічний розвиток підприємства складається з двох взаємозалежних складових: економічної стабільності та стійкості підприємства та його економічної безпеки. Рівень економічної стабільності та стійкості може впливати на рівень економічної безпеки підприємництва і, навпаки, економічний стан підприємства при цьому буде залишатися незмінним, до зміни рівня останньої його складової [3].

Головними умовами і чинниками, які сприятимуть підвищенню ефективності функціонування підприємства, зростанню продуктивності праці, розвитку управління економічною безпекою є: людський капітал – природні здібності й талант, освіта, кваліфікація, стан здоров'я і здатність до виживання; залучення робітників до управлінських функцій; удосконалення тарифної системи оплати праці; розвиток соціальної інфраструктури підприємства; удосконалення системи стимулювання.

Підприємства з людським і соціальним капіталом стають основним джерелом конкурентоспроможних переваг. Сучасний персонал, управляючи людським ресурсом, повинен знати основи економіки, орієнтуватися в

соціальних і культурних тенденціях, трудовому законодавстві, у технологічних новинках, у політиці та в багатьох інших проблемах. Менеджмент персоналу повинен управляти і контролювати програми безпеки праці та здоров'я персоналу, медичного обслуговування, навчання персоналу і підготовку до виходу працівників на пенсію [1].

Гарантування економічної безпеки на підприємствах виконують різні структурні підрозділи. Правовий захист здійснює юридичний відділ, фінансову безпеку забезпечує бухгалтерія, за безпеку кадрів відповідає директор з питань персоналу тощо. Створити внутрішню службу безпеки мають можливість не всі підприємства. Зокрема, малі підприємства зазвичай користуються послугами зовнішніх спеціалізованих державних або приватних організацій. Якщо є можливість, то на малому підприємстві одна особа (здебільшого заступник директора) поєднує основну роботу з роботою з охорони підприємства.

Гарантування економічної безпеки малого бізнесу здійснюється такими економічними методами: організацією власної служби безпеки; раціональним інвестуванням; страхуванням майна і ризиків.

Отже, недооцінювання погроз, що знижують економічну захищеність підприємств, може призвести до руйнування економіки загалом. Потрібний постійний пошук засобів, які сприяли б економічному убезпеченню, особливо в умовах стійкого криміногенного впливу на економічну діяльність, що склалася тепер в Україні.

Сучасний етап соціально-економічного розвитку характеризується радикальними політичними, економічними, соціальними й екологічними змінами, стрімким розвитком науково-технічного прогресу, що проникає у всі сфери життєдіяльності людини. Наростання кризових явищ, посилення невизначеності та динамічності економічної ситуації вимагає від суб’єктів господарювання посилення уваги до питань власної економічної безпеки, виявлення та нейтралізації можливих загроз, небезпек та ризиків, здатних негативним чином вплинути на стан та результати їх діяльності.

Економічна безпека підприємства – це запобігання усіляких загроз діяльності господарюючого суб'єкта, ефективне використання ресурсів для того, щоб забезпечити стале функціонування комерційної структури. Правильно побудована система забезпечення економічної безпеки дозволить проводити постійний моніторинг за діяльністю організації з метою виявлення загроз і профілактики в діяльності конкурентів, а також дозволить побудувати ефективну методику боротьби з виникаючими проблемами. В даний час існує ряд можливих загроз безпеки. Дані загрози зазвичай діляться на внутрішні і зовнішні. До внутрішніх загроз можна віднести витік інформації, всілякі дії працівників організації, які можуть нашкодити діяльності організації, проблеми з партнерами фірми і так далі. До зовнішніх загроз відноситься недобросовісна конкуренція на ринку товарів і послуг, правопорушення законодавства з боку посадових осіб, а також постійна зміна законодавства. Для того, щоб правильно оцінити можливість виникнення такого роду загроз, необхідно проводити профілактичну роботу і боротьбу з подібними проблемами з метою побудови ефективної системи забезпечення економічної безпеки комерційної структури [4].

На наш погляд, на кожному підприємстві для того, щоб організувати ефективну систему забезпечення економічної безпеки необхідно створити спеціалізовану службу. Дана служба буде займатися як зовнішніми, так і внутрішніми загрозами, розробляти і здійснювати профілактичні заходи щодо захисту підприємства, збирати і зберігати інформацію про партнерів, перевіряти працівників організації, проводити захист інформації, охороняти територію і майно фірми, а також здійснювати всі необхідні операції.

Економічна безпека будується індивідуально для кожної організації в залежності від специфіки та області діяльності. Для створення такої служби необхідно досить високе фінансування, необхідно найняти досвідчених співробітників, які будуть постійно контролювати і проводити моніторинг безпеки організації, а також керівництво повинно усвідомлювати важливість і необхідність таких служб.

Існує наступний алгоритм побудови такої системи. Спочатку вивчається специфіка діяльності організації, визначається її місце на ринку товарів і послуг, моніторинг загроз безпеки, аналіз заходів, які можна застосувати для вирішення можливих загроз, створення абсолютно нової системи безпеки, впровадження і подальша оцінка ефективності роботи системи після впровадження.

Виділяють різні підходи, які використовуються для забезпечення економічної безпеки компанії: статистичні, ризикові, економіко-математичні [5].

Кожен підхід має свої певні позитивні сторони, але в даний час зазвичай не використовуються підприємствами у своїй діяльності. Статистичні та економіко-математичні ведуть до високого рівня дослідження, а також виключають особливості окремих фірм, так як використовують теорію великих чисел. Дані методи допомагають виробити спільну оцінку економічної безпеки підприємства. Таким чином, використання даних методів придатне для оцінки компаній в загальному, але не мають можливості оцінити підприємства в конкретній сфері діяльності. А також вони дуже складні для використання служби підприємства, яка займається оцінкою економічної безпеки.

Проведемо порівняльний аналіз усіх підходів до забезпечення економічної безпеки підприємств.

Згідно із статистичними методами, для підприємства задаються певні вхідні впливу, а далі проводиться аналіз вихідних параметрів. В результаті таких дій оцінюється вимірювання параметрів на виході, які показують зміни в діяльності фірми за допомогою факторного аналізу, а також планування і експерименту. Особливе значення відіграє застосування складних статистичних методів прогнозу.

Зміст економіко-математичного підходу полягає в тому, що за допомогою функціональних зв’язків серед найважливіших структурних

підрозділів підприємства, робота фірми описується на рівні узагальнення. В цьому методі застосовуються алгоритми по оптимізації стану всієї системи [6].

Наступний підхід – ризиковий. Суть підходу полягає в тому, що для того, щоб виміряти рівень загроз економічної безпеки, використовується шкала, в якій за одиницю виміру використовують одиниці ризику.

Розглянемо недоліки кожного з підходів.

Згідно статистичному методу, найголовніший недолік полягає в тому, що даний підхід дуже складний, тут невелика корисність в отриманні інформації, необхідно аналізувати величезну базу даних, відсутні критерії, які оцінюють стан економічної безпеки організації, а також дуже складно провести моніторинг економічної безпеки компанії. Цей метод практично не використовується на підприємстві, або використовується досить рідко.

В економіко-математичному методі, так само, як і в статистичному, дуже складно зробити оцінку рівня економічної безпеки, а також тут не враховуються умови розвитку фірми і зміни в структурі компанії і найважливіше – не здійснюється моніторинг економічної безпеки компанії. Даний метод, так само, як і статистичний підхід, на підприємстві використовується дуже рідко, або не використовується зовсім.

У ризиковому підході всі відомості складних проблем економічної безпеки зводяться до теорії ризиків, відсутні критерії оцінки економічної безпеки, і не здійснюється моніторинг. Даний метод можна використовувати на підприємстві дуже обмежено. Однак ризиковий підхід до економічної безпеки може зменшити проблеми до безпеки з позиції ризиків. З іншого боку, даний підхід не враховує зміни на підприємстві і, як вже було вказано, що не здійснює моніторинг за зміною стану економічної безпеки.

Для того щоб оцінити економічну безпеку, враховуючи всі ці методи, необхідно або залучати консультантів з боку, або збільшувати підрозділ, який займається забезпеченням економічної безпеки всієї організації в цілому.

На наш погляд, на кожному підприємстві для того, щоб організувати ефективну систему забезпечення економічної безпеки, необхідно створити

спеціалізовану службу, яка буде займатися як зовнішніми, так і внутрішніми загрозами, розробляти і здійснювати профілактичні заходи щодо захисту підприємства, збирати і зберігати інформацію про партнерів, перевіряти працівників організації, проводити захист інформації, охороняти територію і майно фірми, а також здійснювати всі необхідні операції.

Важливими завдання економічної безпеки підприємства виступає: оцінка ризиків підприємства та їх аналіз; уникнення можливих ризиків та прогноз стану захисту підприємства; захист конфіденційності інформації та комерційної таємниці; ефективне та стратегічне управління системою економічної безпеки підприємства. До останньої належить: захист комерційної таємниці та конфіденційної інформації, інформаційна безпека, внутрішня та зовнішня безпека, конкурентна розвідка, кадрова, виробнича, фінансова, податкова та силова безпеки, а також інші.

Корпоративне шахрайство – одна з актуальних проблем сучасності. За статистикою, 5% прибутку світові компанії втрачають щорічно через несумлінні дії своїх співробітників. В Україні цей показник ще більший – у різних випадках він досягає 10-15%. Ідеться тільки про ті втрати, які оприлюднені компаніями [7]. Ключовими ризиками, які провокують шахрайство у 2019 році є: відсутність систем внутрішніх контролів; самоусунення власника від прямого управління компанією; відсутність критеріїв виміру ефективності бізнесу; особисте небажання власника впроваджувати заходи протидії шахрайству; акцент на готівку при проведенні фінансових транзакцій.

Найкрупнішою у світі організацією по боротьбі із шахрайством ACFE досліджено, що у 2018 році у Східній Європі, а також Західній і Центральній Азії із 86 випадків найбільшим з професійних шахрайств є незаконне присвоєння активів, частка якого становить 83% від загальної частки усіх порушень. Ці випадки спричинили втрату у розмірі 150 000 доларів США. Фінансові схеми шахрайства були найменш поширеними і становили 10% від усіх випадків, а корупційні схеми траплялися у 60% випадків та спричинили у

середньому втрату 300 000 доларів США. До організацій, які є жертвами професійного шахрайства належать: приватні компанії – 50% (збитки 115 тис.дол.США), публічні компанії – 43% (збитки 155 тис.дол.США), урядові – 1; неприбуткові – 2%, інші – 3% [8].

На рис. 3.1 наведено кількість випадків професійного шахрайства (86) у Східній Європі, а також Західній і Центральній Азії у 2018 році. В Україні таких випадків 3, що менше, ніж середнє значення 4,3 з усіх випадків.

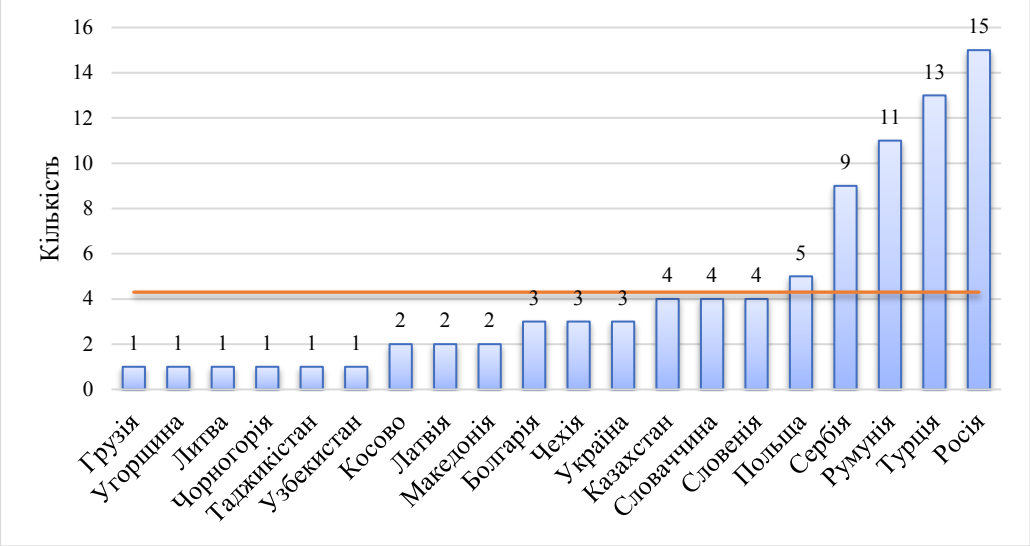

Рис. 3.1. Кількість випадків професійного шахрайства у Східній Європі, а також Західній і Центральній Азії у 2018 році

Найбільше випадків професійного шахрайства у Сербії (9), Румунії (11), Туреччині (13) та Росії (15).

Розглянемо, як розмір організації пов’язаний із ризиком професійного шахрайства. На рис. 3.2 видно, що найбільший відсоток випадків у Східній Європі, а також Західній і Центральній Азії належить підприємствам, в яких кількість працівників становить від 100 до 999 (32%). Ці організації зазнали найбільших втрат на 1 млн.дол.США. Організації з кількістю від 1000 до 9999 працівників становлять 31% випадків, мали середню втрату у розмірі 30 тис. доларів США. Великі організації, де понад 10 000 працівників, складали 26% від усіх випадків понесли в середньому втрату в розмірі 275 тис.дол.США.

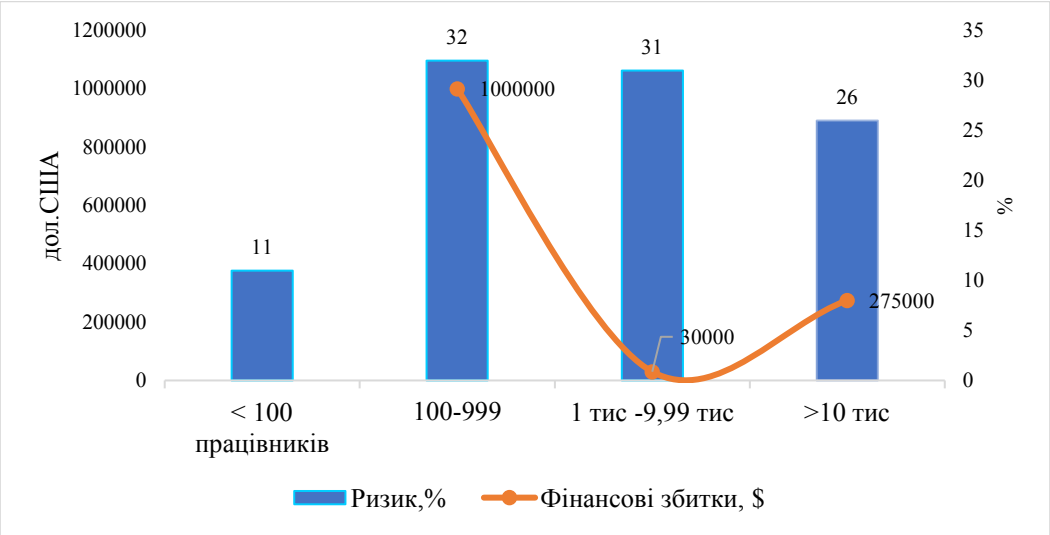

Рис. 3.2. Залежність розміру збитків від кількості працівників в компанії

Найбільша частка економічних злочинів на підприємствах України у 2018 році належала хабарництву та корупції 73%, яка зросла у порівнянні з 2016 р. і становила 56%. Для порівняння, світовий рівень хабарництва та корупції становить 25%.

Рівень економічних злочинів чи шахрайства у 2019 р. (61,5%) зріс у порівнянні з 2016 р. (43%) і навіть дещо перевищив світовий рівень 60,3% (рис. 3.3).

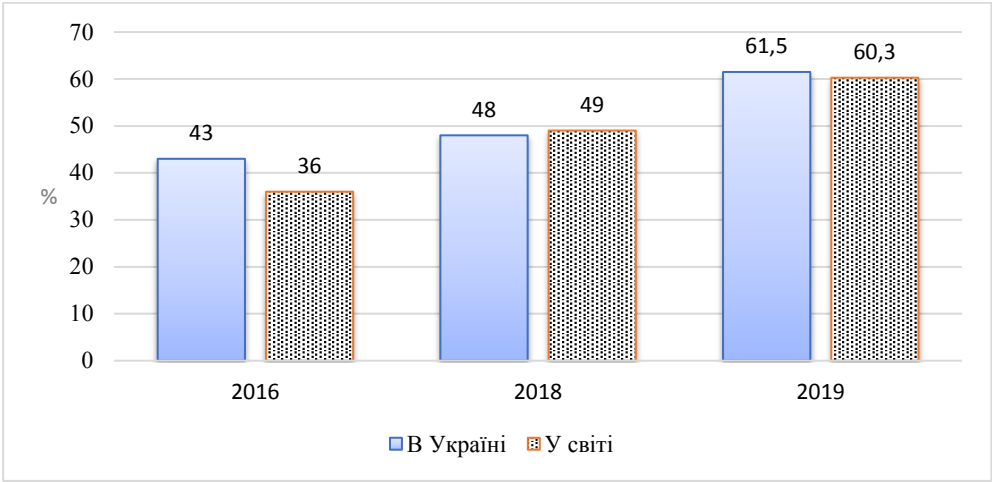

Рис. 3.3. Випадки економічних злочинів чи шахрайства в Україні та світі у 2016-2019 рр.

Згідно даним світової статистики, щорічно втрачається 6,3 трлн.дол.США внаслідок економічних злочинів і шахрайства. Підприємства

втрачають близько 5% свого прибутку внаслідок шахрайства. За рівнем корпоративного шахрайства Україна знаходиться на 5 місці в рейтингу країн світу.

Таким чином, для забезпечення економічної безпеки підприємства, необхідно застосування комплексного підходу, враховуючи виробничі, ринкові та правові ознаки, контроль всіх змін, які відбуваються в ході діяльності компанії, а також використання системи моніторингу, за допомогою якої можливо аналізувати всі зміни, які можуть вплинути на діяльність підприємства, без якого неможливо створити повноцінний підхід по забезпеченню економічної безпеки підприємства, економічної безпеки регіону та національної економічної безпеки [7].

3.2. Латентність економічних злочинів як загроза безпеці підприємництва в Україні

Однією з найгостріших проблем сучасності, що створює реальну загрозу проведення економічних перетворень в Україні, чинником соціальної дестабілізації є стійке зростання злочинних проявів у сфері економіки, збільшення в структурі економічної злочинності частки тяжких злочинів, розростання організованої злочинності і корупції [10].

Тіньова економіка – є однією з основних складових, яка перешкоджає конкурентоспроможності, підвищенню рівня життя населення та економічному розвитку України. Рівень тіньової економіки відображає корупційну складову державних органів, рівень злочинів в економічній та політичній сферах. Об'єктивна реальність є такою, що ні суспільство ні держава не можуть забезпечити належну реєстрацію злочинності.

Тому сьогодні латентна злочинність має наступні види: природна, штучна, прихована та невідома. Приховані (латентні) злочини в сфері економіки, як і злочинність в цілому, чинять негативний вплив на економіку країни, стримують розвиток зовнішньоекономічних зв'язків, динаміку спільної

господарської діяльності, надходження іноземних інвестицій. За масштабами заподіяння шкоди особливу групу економічних злочинів становлять зловживання в сфері кредитно-грошових відносин.

Процеси, що відбуваються в сфері фінансово-економічних відносин, призводять до того, що держава все більше втрачає контроль над економікою і сферою фінансів. За результатами Всесвітнього дослідження економічних злочинів та шахрайства у 2018 року, від випадків економічних злочинів та шахрайства постраждали 48% українських організацій (у 2016 році - 43%). Для порівняння, середній світовий рівень економічних злочинів становить 49%. Одними із основних видів економічних злочинів, на протязі багатьох років, залишаються хабарництво і корупція, негативний вплив яких зазнають 73% українських організацій, які стали їх жертвами.

На сьогоднішній день найбільш поширеними видами економічних злочинів та шахрайства є: незаконне привласнення майна, шахрайство у сфері закупівель, шахрайство у сфері управління персоналом та кіберзлочини пов’язані з економічною діяльністю. Україна в усьому світі вважається однієї із самих проблемних країн у сфері кіберзлочинів.

Із розвитком сучасних інформаційних технологій, з одного боку вони виступають як загроза для організації, з іншого стають її засобом захисту. Хоча українські організації застосовують сучасні інформаційні технології і методи для виявлення шахрайства і його моніторингу, але все ж таки вони відстають від решти світу. Багато вітчизняних організацій ще не в достатній мірі захищені від кібератак. З'ясовано, що лише третина організацій в Україні має програму кіберзахисту.

З 2016 по 2018 роки частка хабарництва та корупції на підприємствах України зросла з 56% до 73%. Якщо порівняти значення цього показника із світовим рівнем хабарництва та корупції, то від майже у три рази менше, ніж у 2018 році в Україні і становить 25%. Лише частка незаконно привласненого майна зменшилася, а всі інші економічні злочини зросли, серед яких

шахрайство у сфері управління персоналом з 4% у 2016 р. до 33% у 2018 р. Процвітає в країні і кіберзлочинність, обсяги якої становлять 31% (рис. 3.4).

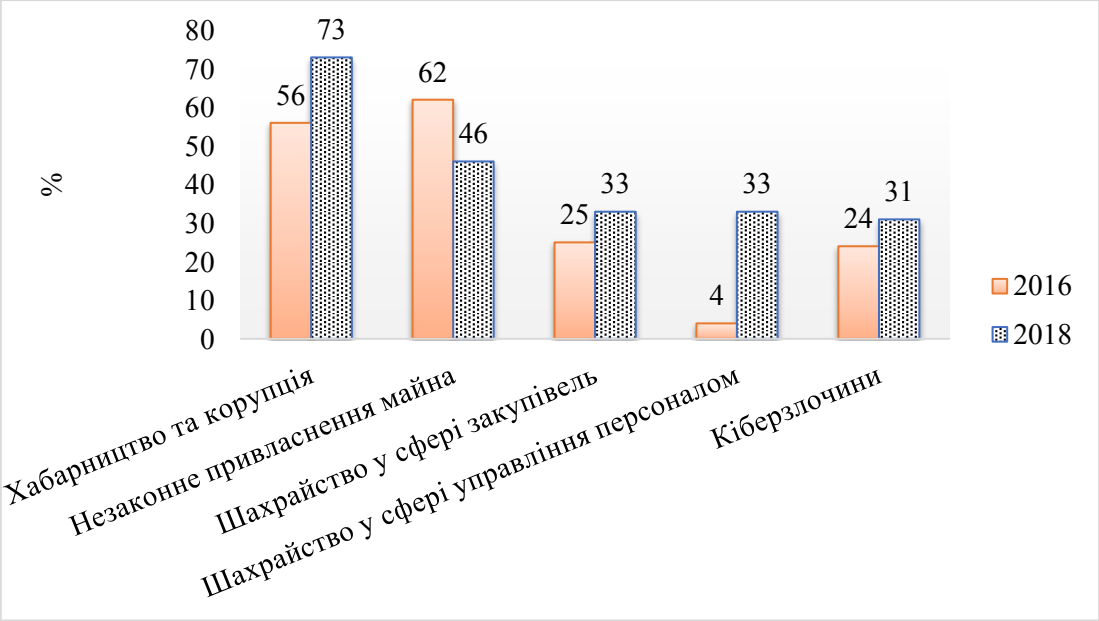

Рис. 3.4. Економічні злочини на підприємствах України

У 2018 р. 56% випадків шахрайства були скоєні співробітниками організацій і належали їх вищому керівництву (у 2016 р. їх було 27%), 36% випадків скоєні третьою стороною (тобто це агенти, постачальники та клієнти, з якими організація має регулярні та прибуткові відносини), а 8% утримались від відповіді. У 70% співробітників основною причиною, що спонукала їх в організації до вчинення шахрайства була можливість його скоїти, тобто не було захисту щодо шахрайства. 33% співробітників отримали хабар за шахрайство [10].

Зменшення випадків незаконного привласнення майна у 2018 році є наслідком ефективності посилення контролю у вітчизняних організаціях та збільшення коштів для його запобігання (рис. 3.4).

Кожна третя вітчизняна організація отримувала пропозицію дати хабара (33%). Занепокоєння викликає й факт, що 23% організацій прогнозують, що хабарництво та корупція, серед інших видів економічних злочинів та шахрайства, стане найбільшим з усіх фінансових збитків.

За даними рейтингу “Індекс сприйняття корупції 2018” за рівнем корупції Україна підвищила свої результати і набрала 32 бали і посідає 120 місце із 180 країн (у 2017 р. – 30 балів, 130-е місце) (рис. 3.5). Серед сусідів Україні вдалося обійти лише Росію, яка з 28 балами займає 138-е місце, Польща – 60, Словаччина – 50, Румунія – 47, Угорщина – 46, Білорусь – 44, Молдова – 33 бали [8].

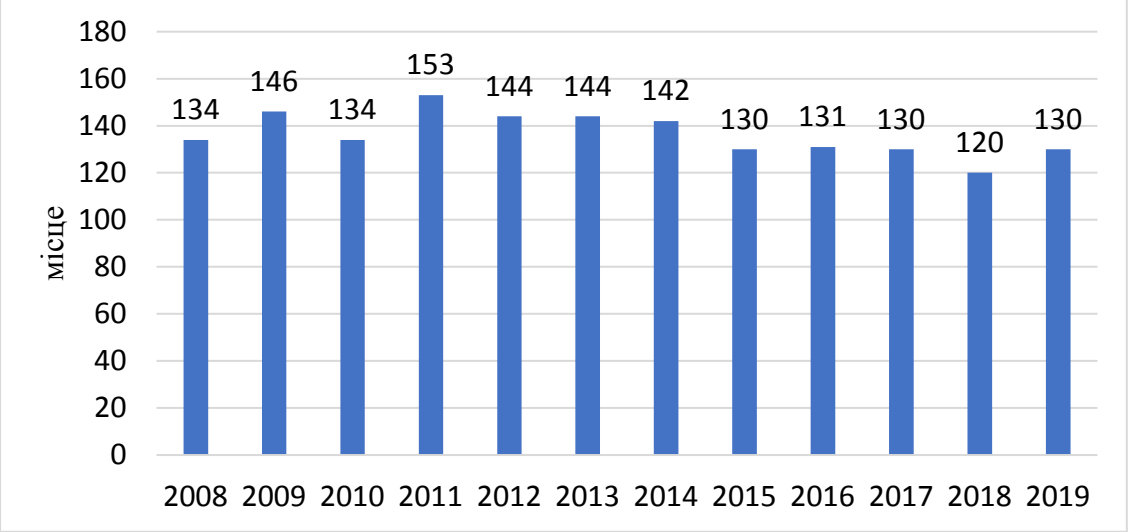

Рис. 3.5. Місце України у міжнародному рейтингу сприйняття корупції

Зовнішнє шахрайство здійснюється на підприємстві контрагентами або третіми особами, а *внутрішнє* здійснюється працівниками самого підприємства. Внутрішнє шахрайство більше впливає на підприємство, якщо брати до уваги втрату репутації та клієнтів, де "крадуть". У 2018 році 33% українських організацій стикалася з шахрайством у сфері закупівель, що на 11% більше, ніж у світі. Таке явище можна пояснити неефективним вибором постачальників, з якими укладаються договори на оплату за їх товари та надання послуг.

Кількість кіберзлочинів, пов’язаних з економічною діяльністю щороку зростає і несе високий ризик як для організацій комерційного, так і державного сектору. Зростання цього виду злочину з 24% у 2016 році до 31% у 2018 році свідчить про нові загрози для організацій із розвитком сучасних інформаційних технологій, серед яких: шкідливе програмне забезпечення,

фішинг, сканування мережі та атаки методом підбору паролю (наприклад, методом "брутфорс", основаним на повному переборі). Саме цьому виду економічних злочинів необхідно приділити максимальну увагу щодо зменшення наслідків від кіберзлочинів.

Незважаючи на збільшення витрат на боротьбу з економічними злочинами та шахрайством, багато українських організацій все ще не проводили профілактику шахрайства, а лише реагують або захищаються при наявності факту шахрайства.

Високий ризик економічних злочинів чи шахрайства вказує на те, що необхідно протидіяти і вживати ефективніші заходи протидії шахрайству, поки воно не стало системним.

Кібератаки стали поширеним явищем в усьому світі. Організації та державні структури у всьому світі потерпають від кібератак, профінансованих державами, здійснених хакерами з політичних чи ідеологічних мотивів, та вчинених терористичними організаціями.

Наслідком кібератак є: порушення діяльності держави, викрадення персональних даних та інтелектуальної власності, збір інформації про структуру інформаційних систем та програмного забезпечення, отримання даних для віддаленого доступу до важливої інфраструктури.

До основних економічних злочинів та шахрайства, від яких страждають організації внаслідок кібератак належать: порушення бізнес-процесів (51%), вимагання (38%), порушення прав інтелектуальної власності (19%), атаки з політичним мотивом (19%), незаконне привласнення майна (13%), інсайдерська атака (4%). Найпоширенішими технологіями кібератаки є: шкідливе програмне забезпечення (35%), фішинг (13%), сканування мережі (5%), атака методом підбору паролів (5%) та атака посередника (3%) [10].

Для подолання системної проблеми шахрайства, вчиненого вищим керівництвом організацій, необхідно розробити такі механізми контролю, які врахують можливість того, що керівництво зможе їх обійти, або вступити у змову в тому чи іншому напрямку. Шахрайство є результатом перетину

особистого вибору людини із порушенням роботи систем та контролів організації, тож вкрай важливо пам’ятати, що відчуття захищеності часто буває оманливим [10].

Таким чином, виявлення та попередження економічних злочинів чи шахрайства – це є комплексне та складне для організації завдання, яке передбачає пошук збалансованого комплексу заходів, які включають технології та людські ресурси, і побудовані на чіткому розумінні стимулів до шахрайських дій та обставин за яких ці дії вчинені.

3.3. Основні тенденції шахрайства на підприємстві

Шахрайство - це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою. Воно має кримінальне карання діяльності, відповідальність за яке в Україні передбачена Кримінальним кодексом України. Особливістю шахрайства є те, що воно може бути вчинено як стосовно майна, так і стосовно права на таке майно. Такий злочин карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на термін до двох років, або обмеженням волі на строк до трьох років.

Шахрайство, вчинене у великих розмірах або шляхом незаконних операцій з використанням інформаційних технологій - карається позбавленням волі на строк від трьох до восьми років. Злочин, вчинений в особливо великих розмірах або організованою групою, карається позбавленням волі на строк від п'яти до дванадцяти років з конфіскацією майна.

На рис. 3.6 показано галузі, де найпоширенішим було професійне шахрайство у 2019 році. Найбільша кількість випадків таких злочинів в Східній Європі і Західній / Центральній Азії відбулася в секторі банківських і фінансових послуг, на виробництві та сфері телекомунікацій. В сфері банківських та фінансових послуг жертвами стали 25% організацій, середній

збиток яких був у розмірі 48000 доларів США, в той час як на виробництві жертвами стали 19% організацій, середній збиток яких був у розмірі 150000 доларів США [7].

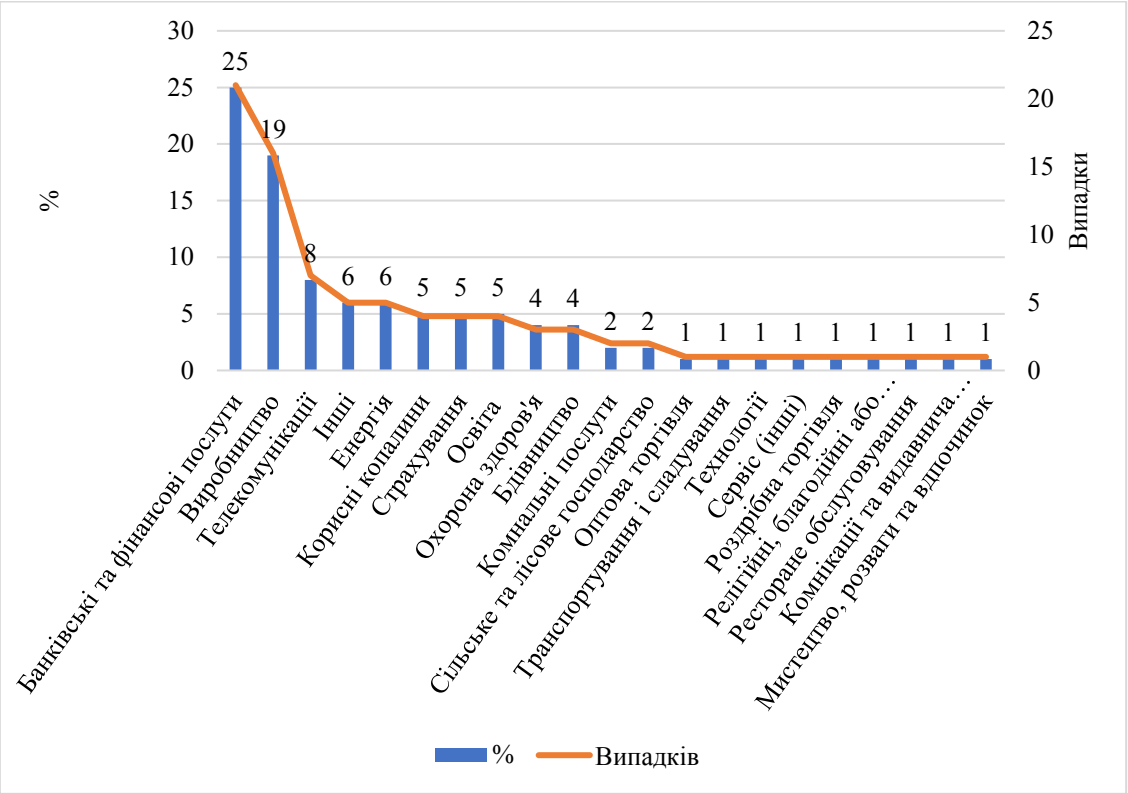

Рис. 3.6. Галузі професійного шахрайства на підприємствах у Східній Європі та Західній / Центральній Азії

Розглянемо заходи боротьби із шахрайством в Східній Європі і Західній / Центральній Азії (рис. 3.7). Практичний досвід вказує на те, що внутрішній контроль відіграє важливу роль у захисті організацій від шахрайства [8, 10].

У рамках нашого дослідження встановлено, що до найбільш поширених заходів у боротьбі із шахрайством є зовнішній аудит фінансової діяльності (95%), внутрішній аудит (91%), норми та правила поведінки на підприємстві (83%), сертифікація фінансової звітності (79%), управлінський нагляд (76%), дзвінки на гарячу лінію (75%) та інше. Частка працівників, які могли отримати винагороду за продаж конфіденційної інформації становила лише 5% [11].

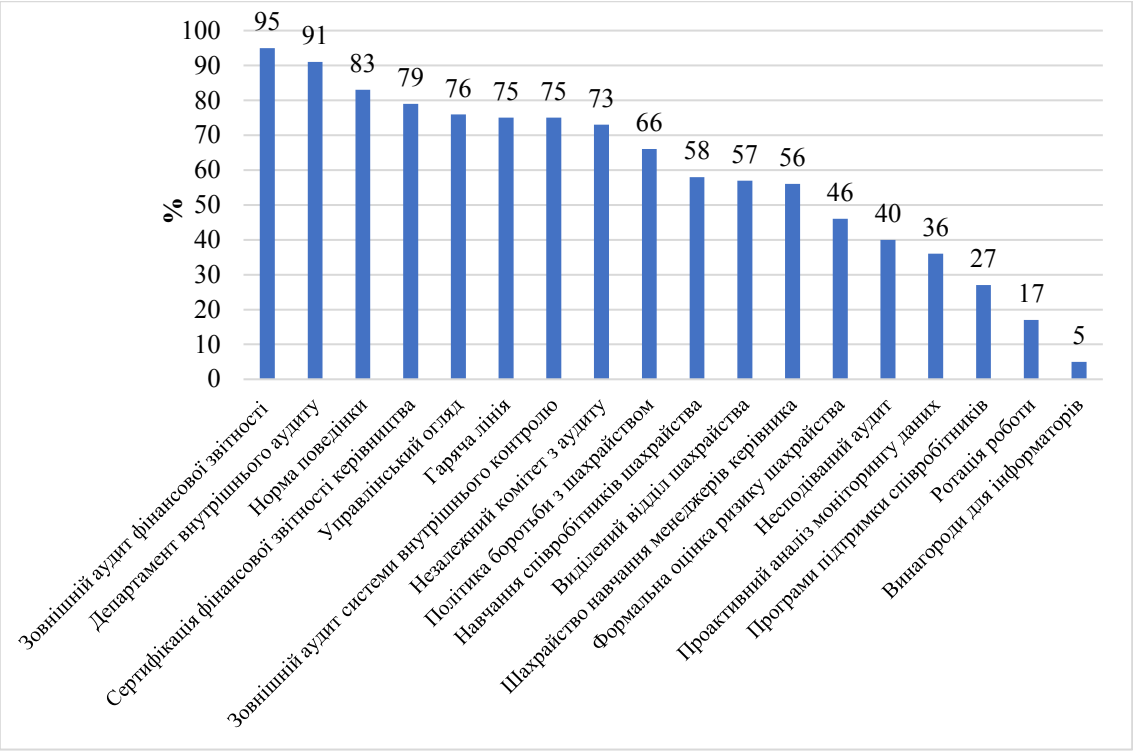

Рис. 3.7. Заходи боротьби із шахрайством, які найбільш поширені в Східній Європі і Західній / Центральної Азії

Таким чином, шахрайство у світі посідає високий рівень. Тому потрібно посилювати органи безпеки у різних сферах діяльності. Якщо не буде введено в дію жорстоких методів з боку органів безпеки, шахрайство буде посилюватися і може вийти на один з перших рівнів злочинів світу. Найефективнішим методом боротьби із шахрайством вважається створення у структурі МВС центру обліку й аналізу шахрайства, де правоохоронні органи будуть збирати та аналізувати виявлену інформацію. Цю інформацію можна застосовувати для встановлення кола потенційних жертв шахрайства, на основі виробленої „моделі" жертви.

Ще однією актуальною проблемою є крадіжки інформації через мережу «Internet». Зазвичай, метою крадіїв є особиста інформація: паролі, номера кредитних карток, номера соціального страхування, корпоративна інформація, технології та інше. Така інформація використовується зловмисниками для незаконних дій: отримання кредитів, здійснення онлайн-покупок, отримання

доступу до конфіденційної інформації, розвитку власної промисловості за рахунок використання інноваційних розробок тієї корпорації, у якої був витік інформації.

Крадіжками можуть бути не тільки наукові розробки, а й бази клієнтських даних. Конкуруючі фірми можуть використовувати таку інформацію для переманювання клієнтів шляхом покращення будь-яких умов договору, який був підписаний між клієнтом і фірмою, у якої дана інформація була вкрадена.

Загроза крадіжок постає не тільки зовні, бо часто інформацію «зливають» не доброчесні працівники, які можуть хотіти зіпсувати стан фірми, з якої її звільняють, саме тому навіть передові системи захисту від кібератак можуть не захистити інформацію. Отже, конфіденційність інформації залежить також від людського фактору.

У наш час набуває стрімкого поширення промислове шпигунство – вид економічної конкуренції, в основі якого полягає шпіонаж, спрямований на отримання інформації та отримання переваг на ринку [12].

Захистити будь-яку фірму від подібних крадіжок може ретельний підбір працівників, розумно прописана система праці (потрібно, щоб працівники мали доступ тільки до тієї інформації, яка безпосередньо є частиною їх роботи).

Не так давно у світі був шквал зламів аккаунтів соціальних мереж та хмарних сховищ зірок. Одним з найпростіших способів отримати доступ до усіх даних людини – зламати аккаунт будь-якого онлайн сховища (хоч ці системи дуже захищені), бо це - інтернет-сервіси, у яких всі користувачі зберігають усі свої дані (фото, паролі, контакти, нотатки і т.і.).

Також дані зловмисники отримують, з серверів «Google», бо всі користувачі сервісів цієї компанії діляться конфіденційною інформацією з даною корпорацією, починаючи з історії та закінчуючи місцем знаходження.

Зараз метою зловмисників зазвичай є сторінки у соціальних мережах, бо користувачі зазвичай зберігають там усе, що стосується їх життя.

Засобом захисту від витоку особистої інформації може бути використання функції, яка є у кожному сервісі, це можливість не надсилати свої дані компаніям. Також велику роль відіграє складність паролів. Але зрозуміло, що найдієвішим способом є відмова від соціальних мереж.

Дослідження, проведені у США у 2019 році з питання запобігання шахрайству виявили, що збитки, які було нанесено споживачам шляхом викрадення даних, становили близько 23,6 мільярдів доларів [12].

Зараз на території нашої країни чинний Закон «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 08.07.2018. Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [9].

У висновку зазначимо, що хоч зараз проблема крадіжок інформації є актуальною, існують шляхи забезпечення особистої безпеки. Дані дії є незаконними та передбачають покарання, отже, маємо надію, що такий вид злочинства у найближчий час вдасться взяти під контроль.

Список використаних джерел до розділу 3

1. Реверчук С.К. Малий бізнес: методологія, теорія і практика / С.К. Реверчук. – К. : Вид-во ІЗМН, 2016. – 198 с.

2. Венедіктова В.М. Гендерна характеристика сучасного трудового законодавства України / В.М. Венедіктова // Право і безпека : науковий журнал. – 2016. – № 5. – С. 85-88.

3. Пекін А. Економічна безпека підприємств як економіко-правова категорія / А. Пекін // Економіст : наук. журнал. – 2017. – № 8. – С. 23-25.

4. URL: http://www.atkspb.ru

5. URL: http://economy-lib.com

6. URL: http://ekonomicheskaya-bezopasnost.intelectos.ru

7. Rybalchenko L. Ensuring enterprise economic security / L.Rybalchenko, E. Ryzhkov // Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. - 2019. - Special Issue № 1 (102). – P. 268-271

8. Report To The Nations. 2018 Global Study On Occupational Fraud And Abuse. [Електронний ресурс]. – Режим доступу: https://www.acfe.com/report-to-the-nations/2018/#download

9. Закон України «Про основні засади забезпечення кібербезпеки України» №2163-VIII від 08.07.2018. Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19/conv

10. Rybalchenko L. Features of latency of economic crimes in Ukraine / L Rybalchenko, O. Kosychenko // Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. - 2019. - Special Issue № 1 (102). – P. 264-267

11. Рибальченко Л.В., Буцанова К.Г. Основні тенденції шахрайства на підприємстві / The 1st international scientific and practical conference “science, society, education: topical issues and development prospects” (December 16-17, 2019) SPC “Sci-conf.com.ua”, Kharkiv, Ukraine. 2019. P. 648-651

12. Рибальченко Л.В., Тодоренко І.О. Основні тенденції шахрайства на підприємстві / The 1st international scientific and practical conference “science, society, education: topical issues and development prospects” (December 16-17, 2019) SPC “Sci-conf.com.ua”, Kharkiv, Ukraine. 2019. P. 651-653

РОЗДІЛ 4. МЕТОДИ ОЦІНКИ РІВНЯ ЕКОНОМІЧНОЇ ТА ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМНИЦТВА

4.1. Методи оцінки рівня економічної безпеки підприємства

На основі аналізу результатів фінансово-господарської діяльності підприємств здійснюється оцінка функціональних і сумарних критеріїв його економічної безпеки, розраховуються їх відхилення від планових значень, аналізуються причини виникнення цих відхилень. Після цього виробляються рекомендації щодо корегування набору корпоративних ресурсів, систем стратегічного і поточного планування фінансово-господарської діяльності підприємства, а також системи оперативного управління його діяльністю.

Рівень економічної безпеки підприємства можна оцінювати на основі визначення сумарного критерію, що розраховується на основі оцінок кваліфікованих експертів за частковими функціональними критеріями економічної безпеки підприємства.

Розрахунок сумарного критерію економічної безпеки підприємства здійснюється за формулою[1]:

$$I = \sum_{i=1}^{n} K_i * D_i \quad (1)$$

де:

K_i - значення часткових функціональних критеріїв економічної безпеки;

D_i - питома вага значущості функціональних складових економічної безпеки (при цьому сума усіх питомих ваг D_i для усіх функціональних складових, по яких ведеться розрахунок, дорівнює 1).

Для визначення вагового значення кожного показника використовується формула Фішберна, в основі якої лежить принцип ранжування показників [2]:

$$K_i = \frac{2*(m-i-1)}{m*(m+1)} \quad (2)$$

Найбільший вплив на економічну безпеку мають показники фінансової стабільності підприємства, оскільки відображають залежність підприємства від зовнішніх чинників. Вони характеризують захищеність підприємства від зовнішніх загроз, пов’язаних із нестабільністю банківського сектора та можливістю неплатоспроможності підприємств-партнерів.

Кожному із показників за допомогою експертного методу, надається свій ранг залежно від впливу показників на фінансову безпеку промислового підприємства, при цьому найменше значення рангу означає найбільший вплив, а найбільше – найменший. Ранг повинен переглядатися залежно від стану ринкової кон’юнктури, ситуації як на фінансовому ринку, так і в реальному секторі, а також ураховувати специфіку діяльності галузі або самого підприємства, його стратегію та цілі [3].

Крім цього, часткові функціональні критерії економічної безпеки підприємства по кожній з її складових можна розраховувати на основі оцінки збитків економічної безпеки підприємства і ефективності заходів щодо їх запобігання.

До функціональних складових сумарного критерію економічної безпеки підприємства відносяться: фінансова, інтелектуальна, кадрова, техніко-технологічна, політико-правова, інформаційна, екологічна, силова.

Даний метод розрахунку сумарного критерію економічної безпеки підприємства містить значну частку суб'єктивного фактору оцінки експертів. Це відбивається як в оцінці, так і в процесі розподілу питомої ваги функціональних складових при розрахунку цього критерію. Але, саме відсутність чітко заданих параметрів оцінки дозволяє найбільш ефективно адаптувати даний метод оцінки діяльності підприємства на специфіку конкретного підприємства.

Аналіз рівня економічної безпеки підприємства проводиться на основі порівняння значення сумарного критерію економічної безпеки підприємства з отриманими раніше значеннями, або з розрахованими для порівняння значеннями цього критерію для аналогічних підприємств даної галузі. Крім того,

порівнюються поточні і минулі оцінки часткових функціональних критеріїв і виявляються ступені впливу зміни стану функціональних складових на зміну значення сумарного критерію економічної безпеки підприємства .

Для оцінки впливу кожної зі складових необхідно визначити приватний функціональний критерій. Він розраховується як відношення сукупного запобігання шкоди по даній складовій економічної безпеки підприємства до суми витрат на реалізацію заходів щодо запобігання збитків від негативних впливів і загального понесеного збитку за складовою. Приватний функціональний критерій розраховується за формулою [2]:

$$P = \frac{Z}{S+Y} \quad (3)$$

де:

P-приватний функціональний критерій рівня забезпечення функціональної складової економічної безпеки підприємства;

Z- сукупний збиток по складовій;

S - сумарні витрати в аналізованому періоді на реалізацію заходів щодо запобігання збитків по даній функціональній складовій економічної безпеки підприємства;

Y - загальний понесений збиток по даній функціональній складовій економічної безпеки підприємства.

Розрахований сукупний критерій економічної безпеки порівнюється з аналогічними критеріями економічної безпеки споріднених підприємств галузі. Якщо критерій досліджуваного підприємства вище, ніж у його конкурентів, можна вважати, що підприємство знаходиться в стані відносної економічної безпеки. Цей критерій в подальшому може бути використаний для отримання прогнозів фінансово-економічного стану фірми, які служать для практичного маркетингу, управління фінансами, фінансового менеджменту, а також при поточному управлінні фірмою [3].

Розрахунок показників економічної безпеки підприємства є важливим елементом для швидкого реагування на можливі недоліки в управлінні підприємством, що можуть бути перешкодою ефективному протистоянню

зовнішніх та внутрішніх загроз підприємства та оперативному внесенню відповідних коректив щодо усунення слабких місць. Лише за цих умов можливий стабільний економічний розвиток промислового підприємства, що функціонує в умовах мінливого та нестабільного зовнішнього середовища.

4.2. Механізм забезпечення фінансової безпеки підприємств

Останнім часом економіка України перебуває в умовах складного реформаційного періоду. Підприємства функціонують у динамічному зовнішньому середовищі, в умовах постійних змін та часткової невизначеності. Через це виникають загрози його розвитку та ефективній діяльності. Задля підтримки стабільного розвитку і функціонування фінансової системи в умовах нестійкого зовнішнього середовища потрібно безперервна розробка, впровадження та вдосконалення адаптивних механізмів забезпечення фінансової безпеки підприємства. Отже, внаслідок цього оцінка фінансової безпеки вітчизняних підприємств нині є дуже актуальною.

Механізм фінансової безпеки надає підприємству наступні можливості [4]:

- самостійно розробляти та впроваджувати власну фінансову стратегію;
- забезпечувати залучення і використання фінансових ресурсів підприємства;
- забезпечити фінансову незалежність підприємства;
- вчасно ідентифікувати внутрішні і зовнішні загрози та небезпеки фінансовому стану підприємства;
- забезпечити фінансові інтереси власника підприємства.

Зовсім нещодавно в сучасній економіці з’явилась категорія «фінансова безпека підприємств» як самостійний об’єкт управління. Вона є головною складовою економічної безпеки, бо у будь-якій економічній системі фінанси виконують провідну функцію. Фінансова безпека -це кількісно та якісно

детермінований рівень фінансового положення підприємства, який забезпечує захищеність його фінансових інтересів від реальних і потенційних внутрішніх та зовнішніх загроз. Для стійкого зростання підприємства визначають параметри на основі фінансової філософії й конструюють необхідні умови фінансової підтримки.

Вдосконалення механізму забезпечення фінансової безпеки підприємства необхідне для того, аби пом'якшити або уникнути дії загроз, які можуть негативно вплинути на розвиток підприємства та реалізацію фінансової стратегії.

Забезпечення фінансової безпеки – це системний процес, який поєднує в собі три основних компоненти: оцінку та діагностику фінансово-господарської діяльності підприємства; доцільне та своєчасне застосування антикризових (стабілізаційних) заходів для уникнення внутрішніх і зовнішніх загроз діяльності підприємства; формування заходів та рекомендацій щодо забезпечення фінансового розвитку і конкурентоспроможності підприємства за всіма етапами його життєвого та операційного циклів .

Досягнення безперебійного та безперервного процесу перетворення капіталу в капітальні блага забезпечує зростання фінансової незалежності, рівня майнового положення, рентабельності, ринкової та ділової активності.

Важливим елементом економічної безпеки підприємства є його ресурсне забезпечення. Можна визначити критерії оцінки ресурсів, що в умовах конкуренції забезпечують його переваги . До основних критеріїв відносяться [4]:

- цінність;
- раритетність;
- неповторність;
- замінність.

Найважливішою складовою ефективного розвитку підприємства є забезпечення його фінансової безпеки. В сучасних ринкових економічних умовах підприємству потрібно створювати власну систему безпеки, яка

допоможе своєчасно виявляти зовнішні та внутрішні загрози і ліквідовувати їх; вдосконалювати контролюючу систему діагностики фінансового стану підприємства для забезпечення стабільності та стійкості.

4.3. Організаційне забезпечення фінансової безпеки підприємництва

Здатність підприємства до стабільного стійкого розвитку окреслюється ступенем захисту від внутрішніх і зовнішніх загроз, який дозволяє швидко реагувати на зміну в середовищі функціонування і характеризує рівень його фінансової захищеності. Розвиток підприємства неможливий без надійної системи фінансової безпеки. В умовах сучасної нестабільності економічної системи кожне підприємство повинно створювати сприятливі умови для забезпечення високого рівня своєї фінансової безпеки, що дає можливість розробляти та запроваджувати самостійну фінансову стратегію, підтримувати достатній рівень досконалої конкуренції на ринку.

Реалізація фінансового механізму фінансової безпеки підприємництва вимагає певного керування та організації. В основі організації має бути цільовий підхід щодо забезпечення основного призначення фінансової безпеки. З огляду на визначення механізму фінансової безпеки як системи важелів, інструментів та методів функціонування суб’єкта підприємницької діяльності, що постійно забезпечує його фінансові інтереси, останні можуть бути покладені в основу такої організації у якості мети, що має бути досягнута. Економічне середовище існування підприємства, зокрема наявність зовнішніх та внутрішніх загроз при цьому не обумовлюються, однак така сталість функціонування має бути досягнута, в тому числі, в умовах кризових процесів та явищ. Крім того, слід виходити з аксіом фінансової безпеки, а саме, загальності, унікальності та відкритості [5] .

Фінансово-економічний механізм управління фінансовою безпекою підприємства у науковій літературі розглядається як сукупність управлінських, економічних, фінансових способів гармонізації інтересів

підприємства з інтересами суб'єктів зовнішнього середовища. Кінцевим результатом роботи зазначеного механізму є вплив на процес розробки та реалізації управлінських рішень з урахуванням особливостей діяльності підприємства, що забезпечує зростання ринкової вартості підприємства та максимізацію отриманого ним прибутку [6]. Механізмом забезпечення фінансової безпеки підприємства називають сукупність чітко визначених дій зі створення умов гарантування його захисту від негативного впливу внутрішніх і зовнішніх загроз. Ці дії можуть містити в собі сукупність організаційних, фінансових і правових методів впливу з боку суб'єктів управління фінансами підприємства, спрямованих на своєчасне виявлення, попередження, нейтралізацію та ліквідацію загроз фінансовій безпеці даного суб'єкта підприємництва. Тобто, механізм управління забезпеченням фінансової безпеки підприємства передбачає вплив суб'єктів фінансової безпеки на об'єкт – фінансову діяльність підприємства, що впливає перш за все на стан його фінансових ресурсів з урахуванням дії фінансових ризиків та загроз.

Отже, фінансово-економічний механізм управління забезпеченням фінансової безпеки є складовою частиною комплексної системи управління підприємством, дія якої спрямована на [6] :

– сприяння стабільному розвитку, підвищенню ефективності й конкурентоспроможності підприємства;

– формування та збільшення його фінансово-економічних ресурсів зі створенням системи захисту від зовнішніх та внутрішніх чинників.

До основних елементів фінансово-економічного механізму управління забезпеченням фінансової безпеки підприємства слід віднести три блоки :

– інформаційно-організаційний блок – це система, що складається з організаційного, інформаційно-аналітичного, нормативно-правового та програмно-технічного забезпечення;

– функціонально-аналітичний блок – згруповує елементи, призначені для діагностування фінансової безпеки підприємства, здійснення оцінки управління безпекою та проведення на підставі отриманих даних, виявлення ризиків та загроз;

– контрольно-моніторинговий блок – контроль процесу реалізації стратегії управління фінансовою безпекою підприємства, її коригування на основі оцінки ефективності стратегії управління фінансовою безпекою.

Використання запропонованого фінансово-економічного механізму управління забезпеченням фінансової безпеки підприємства допоможе обрати оптимальну стратегію управління фінансовою безпекою, засвідчувати критерії оцінки її ефективності на підставі належного інформаційно-аналітичного забезпечення.

4.4. Методи оцінки фінансової безпеки підприємства

Забезпечення стабільності результатів діяльності підприємства, досягнення цілей, що відповідають інтересам власників та суспільства в цілому, неможливі без розробки та проведення відповідної стратегії суб’єкта господарювання, яка визначається наявністю надійної системи його фінансової безпеки. Важливим елементом управління фінансовою безпекою підприємства є об'єктивне і своєчасне визначення її рівня, що дозволить своєчасно виявити проблеми у фінансовому стані та виправити їх без загрози втрати фінансової стійкості та платоспроможності у майбутньому.

Рівень фінансової безпеки підприємства визначається наступними групами показників:

– оцінка рівня фінансової безпеки як складової економічної безпеки підприємства;

– оцінка рівня фінансової безпеки на основі визначення фінансового стану підприємства;

– оцінка рівня фінансової безпеки на основі інтегральних показників.

До першої групи відносяться наступні функціональні складові: бюджетна безпека, грошово-кредитна, зовнішньоекономічна, банківська, страхова, фондова, інвестиційна. Для кожного конкретного підприємства використовуються лише ті елементи фінансової безпеки, які відповідають його виду економічної діяльності.

Ряд науковців пропонують оцінювати фінансову безпеку підприємства на основі визначення та оцінки загального стану фінансової діяльності підприємства, а саме: горизонтальний, вертикальний, порівняльний, інтегральний аналізи та аналіз фінансових коефіцієнтів. Комплексно оцінити фінансовий стан підприємства та стан його фінансової безпеки можливо, використовуючи наступні групи показників: майнового стану, ліквідності та платоспроможності, дебіторської та кредиторської заборгованостей, ділової активності, рентабельності підприємства та фінансової стійкості [7] .

Із всієї множини фінансових коефіцієнтів експертами було виділено найбільш значимі, які б не дублювали одне одного і найбільш повно характеризували стан фінансової безпеки підприємства [7]. Кожен з них має нормативне значення .

1) Показники майнового стану: коефіцієнт зносу основних засобів (≤ 0,5).

2) Показники ліквідності та платоспроможності: коефіцієнт абсолютної ліквідності (0,2 – 0,5); коефіцієнт загальної ліквідності (≥1).

3) Показники дебіторської та кредиторської заборгованостей: залежність від дебіторської заборгованості (≤0,4); залежність від кредиторської заборгованості (≤0,4).

4) Показники ділової активності: коефіцієнт оборотності власного капіталу; коефіцієнт оборотності активів.

5) Показники фінансової стійкості: коефіцієнт незалежності (автономії) (≥0,5); коефіцієнт самофінансування (>1); коефіцієнт фінансової стійкості (≥0,75).

6) Показники прибутковості (рентабельності): рентабельність загальних активів (>0,05); рентабельність необоротних активів (>0,1); рентабельність оборотних активів (>0,1); рентабельність власного капіталу (>0,15); рентабельність інвестицій (>0,1).

Отже, проаналізувавши фінансову звітність підприємств та розрахувавши коефіцієнти, можно сформувати інтегральний показник оцінки стану фінансової безпеки підприємства. Він формується із суми бальних оцінок коефіцієнтів за кожною групою показників. Розрахованим значенням показників оцінки фінансової безпеки підприємства присвоюється відповідна бальна оцінка рівня показника від одного до п’яти. Виділяють п’ять станів фінансової безпеки підприємства: оптимальний, високий, середній, низький та кризовий [8] .

Здійснені розрахунки дають змогу оцінювати стан фінансової безпеки підприємства загалом та в розрізі окремих груп.

Але, оцінка фінансової безпеки підприємства не може зводитись до простого аналізу фінансового стану підприємств. Про високий рівень фінансової безпеки можуть свідчити такі критерії як: технологічна незалежність підприємства, висока ефективність менеджменту підприємства, ефективність його організаційної структури, високий рівень кваліфікації персоналу підприємства та його інтелектуального потенціалу, якісна правова захищеність усіх аспектів діяльності підприємства, забезпечення захисту інформаційного середовища підприємства, комерційної таємниці та досягнення високого рівня інформаційного забезпечення діяльності усіх його служб та підрозділів, забезпечення безпеки персоналу підприємства, його капіталу, майна та комерційних інтересів.

Отже, дуже важливим при оцінці фінансової безпеки підприємства є поєднання традиційних та нетрадиційних методів. Нетрадиційні методи базуються на оцінці рівня розвитку та управління, оцінці ризиків та ринкової вартості підприємства.

Така діагностика фінансової безпеки підприємства дозволить з мінімальними втратами часу та максимальною ефективністю приймати управлінські рішення. Адже, за сучасних економічних умов оцінка рівня фінансової безпеки є невід'ємною частиною управління підприємством. Вона дає можливість керівництву та менеджерам підприємств ефективніше вирішувати проблеми забезпечення фінансової безпеки, обирати ефективні шляхи мінімізації фінансових втрат.

4.5. Фінансові ризики як деструктивні чинники впливу на фінансову безпеку підприємства

Прибуток – це матеріальний показник ефективності економічної діяльності підприємства, який залежить від багатьох факторів та має на нього безпосередній вплив. Фінансова діяльність підприємства пов'язана з багатьма транзакціями, операціями, угодами, що несуть за собою не лише можливість збагачення, а й значні фінансові ризики. Саме тому для забезпечення фінансової стабільності на підприємстві необхідно розробляти концепцію безпеки та стратегію управління з урахуванням ризиків, що супроводжують діяльність підприємства. Ризики, що пов'язані із можливістю виникнення неочікуваних матеріальних витрат, зниженням або відсутністю прибутку, втратою частини капіталовкладень для підприємства класифікуються як фінансові ризики. Ці ризики виникають на будь-якому етапі господарської діяльності в результаті відносин з фінансовими структурами та підприємствами [9] .

Причини виникнення фінансових ризиків різноманітні й можуть з'явитися непередбачено в процесі діяльності підприємства. Вони поділяються на зовнішні та внутрішні. До основних зовнішніх причин формування фінансових ризиків можна віднести наступні: слабку і нестабільну економіку країни; економічну кризу; інфляцію; підвищення рівня конкурентної боротьби; зниження цін на світовому ринку; політичні чинники

та ін. Усі ці причини мають зовнішнє, щодо підприємства, походження і тому підприємство їх контролювати не може. До внутрішніх причин формування фінансових ризиків можна віднести: підвищення витрат на підприємстві, низький рівень управління, відсутність планування, незадовільну фінансову політику підприємства та ін [9].

Для подальшої регуляції та уникнення всіх фінансових ризиків має бути налагоджена внутрішня фінансова політика, яка залежить лише від внутрішніх факторів організації підприємства. Цілеспрямоване використання ресурсів підприємства, узгодження процесу виробництва та реалізації, виконання актуальних завдань в сукупності і являє собою фінансову політику компанії. Варто відзначити, що установлювати та регулювати її мають право лише засновники, уповноважені ними особи та володар контрольного пакету акцій.

Учасники фінансового ринку, в ході реалізації фінансових ризиків, можуть зазнати масштабних збитків або ж втратити абсолютно весь капітал. Ось чому, так важливо вміти ідентифікувати ризики та уникнути їх. Виявити їх можна методом безпосереднього аналізу кожної операції, та співставленні її з кожним можливим ризиком. При цьому, важливим інструментом регуляції ризиків є правильно встановлена належність їх до конкретного середовища.

На рис. 1 відображено основні види фінансових ризиків.

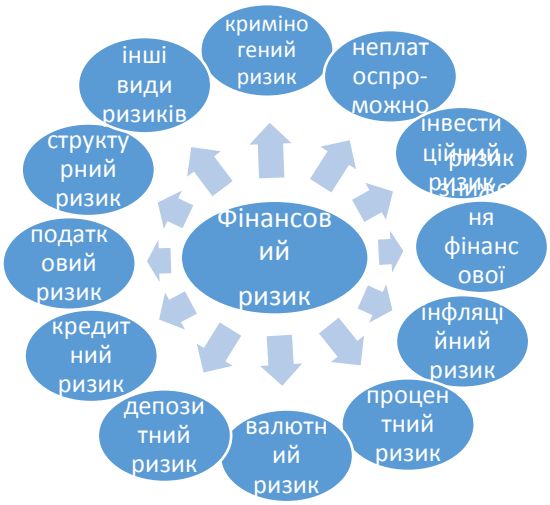

Рис. 4.1. Основні види фінансових ризиків

Фінансові ризики зосереджені в багатьох сферах фінансового впливу на підприємство. І в незалежності від того, які за станом ризики-пасивні чи активні, вони несуть собою загрозу цим сферам. Адже їх реалізація – це лише питання часу, і в будь-якому випадку вони наноситимуть шкоду системам підприємства, якщо їм ефективно не протидіяти методом ідентифікації, профілактики, оцінювання та страхування.

Все вищеперераховане і є основним аспектом фінансової безпеки підприємства, яка класифікується як фінансовий стан, який характеризується:

- по-перше, збалансованістю і якістю сукупності фінансових інструментів, технологій і послуг, що використовуються підприємством;

- по-друге, стійкістю до внутрішніх і зовнішніх загроз;

- по-третє, здатністю фінансової системи підприємства забезпечувати реалізацію його фінансових інтересів, місії і завдань достатніми обсягами фінансових ресурсів;

- по-четверте, забезпечувати ефективний і сталий розвиток цієї фінансової системи [3] .

Якщо визначити фінансові ризики, як деструктивні чинники фінансової безпеки, тобто ті, які виводять з ладу всю систему функціонування даної структурної одиниці (в перекладі з латинського destructivus «руйнівний», від дієслова destruere «ламати; руйнувати»), можна зробити висновки, що управління та регуляція ризиків, з точки зору підприємства, є необхідними для продуктивної роботи та отримання максимального прибутку.

Деструктивність ризиків полягає у тому, що вони є впливовим фактором, який може як і мотивувати організацію, так і пригнічувати. Звернемо увагу, на те, що ризики можуть сприйматися підприємством у три етапи: виклик, загроза, небезпека. І на останньому етапі дуже важливо прийняти відповідні заходи забезпечення фінансової безпеки. В першу чергу для цього необхідно визначити стратегію та тактику підприємства і вже відштовхуючись від них, забезпечувати розвиток розробки концепції фінансової безпеки, які базуються на:

- забезпеченні високого ступеню узгодження та гармонізації фінансових інтересів підприємства з інтересами оточуючого середовища та інтересами його персоналу;

- наявності на підприємстві стійкої до загроз фінансової системи, яка спроможна забезпечувати реалізацію фінансових інтересів, місії і завдань;

- збалансованості і комплексності фінансових інструментів і технологій, які використовуються на підприємстві;

- зростанні постійності і динамічності розвитку фінансової системи (підсистеми) підприємства [9] .

Отже, ризики дійсно впливають на фінансову безпеку підприємства, наражаючи на небезпеку її функціонування, шляхом впливу на всі сфери фінансової діяльності. Для боротьби з ризиками, перш за все, необхідна відповідна стратегія і тактика та налагоджена система менеджменту підприємства.

Список використаних джерел до розділу 4

1. URL:https://ela.kpi.ua/bitstream/123456789/16376/1/Ekonomizna_bezpeka.pd

2. URL:https://web.posibnyky.vntu.edu.ua/fmib/33nebava_ekonomichna_bezpeka_pidpriyemstva/rozd2.html

3. Тютченко С.М. Методи оцінки рівня економічної безпеки підприємства. Матеріали Всеукраїнського науково-практичного семінару "ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ» (23 листопада 2018 р., м. Дніпро). – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. – 150 с., с.87

4. Тютченко С.М. Механізм забезпечення фінансової безпеки підприємств. Матеріали Всеукраїнського науково-практичного семінару "ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В

ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ» (23 листопада 2018 р., м. Дніпро). – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. – 150 с., с.91

5. Ставерська Т.О., Шевчук І.Л., УДК 339.9. Механізм управління забезпечення фінансової безпеки підприємства. Харківський державний університет харчування та торгівлі. URL: https://conf.ztu.edu.ua/wp-content/uploads/2017/09/253.pdf

6. Тютченко С.М. Організаційне забезпечення фінансової безпеки підприємництва. Матеріали Всеукраїнського науково-практичного семінару "ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ» (23 листопада 2018 р., м. Дніпро). – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. – 150 с., с.116

7. Малик О.В. ПОКАЗНИКИ ОЦІНКИ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВ: КРИТЕРІЇ ТА ДЕТЕРМІНАНТНІ ХАРАКТЕРИСТИКИ. Вісник Хмельницького національного університету 2013, №5, Т. 1 URL:elar .khnu.km.ua/jspui/bitstream/123456789/1183/1/MALYK.pdf

8. Тютченко С.М. Кокарєв І.В Використання сучасних інформаційних технологій діяльності національної поліції України: матеріали всеукраїнського наук.-практ. семінару, м. Дніпро: ДДУВС. 2017

9. Тютченко С.М. Козлова Д.С. ФІНАНСОВІ РИЗИКИ ЯК ДЕСТРУКТИВНІ ЧИННИКИ ВПЛИВУ НА ФІНАНСОВУ БЕЗПЕКУ ПІДПРИЄМСТВА. Матеріали Всеукраїнського науково-практичного семінару "ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ» (23 листопада 2018 р., м. Дніпро). – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. – 150 с., с.110 http://er.dduvs.in.ua/bitstream/123456789/2494/1/20.pdf

РОЗДІЛ 5. МІЖНАРОДНИЙ ДОСВІД В ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ДЕРЖАВИ ТА ПІДПРИЄМНИЦТВА

5.1. Аналіз досвіту країн ЄС в забезпеченні економічної безпеки держави

Світові фінансові та економічні кризи є знаковими етапами в міжнародній системі політичних, економічних відносин, та відносин у сфері безпеки. У цих умовах надзвичайно важливим є реальне бачення місця і ролі кожної країни в глобальному світі, що динамічно змінюється. Як показує світовий досвід, забезпечення економічної безпеки - це гарантія незалежності країни, умова стабільності й ефективності життєдіяльності суспільства, досягнення успіхів в усіх сферах розвитку. Тому забезпечення економічної безпеки належить до числа найважливіших національних пріоритетів більшості країн світу, а аналіз і подальша адаптація успішного досвіду такого забезпечення є однією з найбільш ефективних механізмів досягнення стабільності та ефективності національної економіки.

Досвід країн ЄС свідчить, що забезпечення національної економічної безпеки має вирішальний вплив на одержання державою визначного місця в глобальному просторі, яке відповідало б його стратегічним цілям та потенціалу. Адаптація досвіду країн Євросоюзу щодо забезпечення економічної безпеки повинна стати одним з пріоритетних напрямів зовнішньої політики країн не тільки з точки зору досягнення стійкості та ефективності національної економіки, а й з позиції довгострокової стратегії національного розвитку. [1]

В Європейському Союзі термін «економічна безпека» відноситься до позиції об'єднання в світовій економічній системі. ЄС диктує важливість європейської інтеграції з метою досягнення високого рівня конкурентоспроможності в умовах глобалізації. Окремо кожна країна ЄС має набагато менше економічних ресурсів, ніж інші розвинені країни.

Взаємообмін ресурсами визначає здатність Європейського союзу забезпечувати високий рівень конкурентоспроможності і економічної безпеки. Кінцевою метою забезпечення економічної безпеки в Європейському Союзі є формування повністю інтегрованої Європи з однаковим рівнем життя в усіх країнах-учасницях [2].

Концепцію економічної безпеки ЄС необхідно розглядати в контексті економічної безпеки кожної окремої держави, національних доктрин, програм і концепцій забезпечення національної безпеки.

У Німеччині державна філософія економічної безпеки на практиці реалізується переважно через закони, що регламентують найбільш важливі сфери ринкової діяльності і наділяють державу істотними контрольними функціями. Німеччина бачить забезпечення своєї економічної безпеки в підтримці економічного і соціального прогресу, демократизації в Європі і в усьому світі, захисту від економічного шантажу, забезпеченні свободи торгівлі і доступу до сировинних ресурсів та ринків в рамках справедливої світової економічної системи. У внутрішньоекономічних планах поставлена мета підвищувати господарський розвиток країни, матеріальний та соціальний стан населення. У цьому питання головний акцент робиться на стабільності та вдосконаленні ринків збуту.

Основними методами безпечного розвитку економіки в Німеччині є функції з підтримки правового характеру ринкових відносин, створення цивільних умов для конкуренції, недопущення монополізації в окремих галузях і підтримання стабільності національної валюти.

Під економічною безпекою у Франції розуміється попередження і запобігання економічним загрозам шляхом створення нових схем, адаптації норм і структур міжнародної безпеки та створення мережі співпраці, зокрема між державним і приватним секторами та між державами. У Франції основним державним документом, в якому відбиваються окремі положення забезпечення економічної безпеки, є Закон «Про національну безпеку». Поняття національної трактується як створення сприятливих внутрішніх і

зовнішніх умов для підвищення національного добробуту і зміцнення економічного потенціалу країни. Економічна безпека в широкому сенсі забезпечується всією сукупністю інструментів господарського регулювання. З цією метою у Франції в процесі прийняття економічних рішень використовуються критерії, пов'язані із зниженням уразливості господарської системи і збереженням економічного фундаменту самостійної зовнішньої політики. До таких критеріїв належать [1]:

- усунення серйозних диспропорцій в рівнях економічного розвитку суб'єктів господарювання;
- недопущення надмірної зовнішньої залежності в найважливіших секторах економіки:
- зведення до мінімуму ризиків, пов'язаних із залежністю від зовнішнього світу [3].

Політика в галузі забезпечення безпеки в Великобританії тісно пов'язується з оборонною політикою: обидві вони ґрунтуються на оцінках національних інтересів і реалізуються через їх захист. Під «національними інтересами» в сфері економіки розуміються народногосподарські інтереси всього суспільства в цілому, мають пріоритет по відношенню до інших форм громадських інтересів [3].

Загрози національній економічній безпеці поділяють на зовнішні і внутрішні і ранжуються за ступенем важливості та ймовірності настання, що дозволяє концентрувати зусилля по прогнозуванню та запобіганню найбільш небезпечних, з точки зору національної економічної безпеки та ризиків. В сфері запобігання економічних загроз уряд традиційно опирається на приватний бізнес, надаючи йому максимальну підтримку. Крім того, в країні існує розгалужена мережа інститутів, що забезпечує ефективну взаємодію парламенту, уряду і великого бізнесу при розробці та реалізації рішень, що відносяться до забезпечення національної економічної безпеки.

Концепція економічної безпеки розглядається в Іспанії в значній мірі в контексті економічної безпеки всього Європейського Співтовариства. Разом з

тим, створена ефективна система забезпечення національних інтересів в економічній області. Її основу складають:

- гнучка законодавчо-нормативна база;
- чітке розмежування компетенції міністерств, відомств і організацій в реалізації нормативних положень, що стосуються економічного розвитку;
- наявність на кожному етапі розвитку законодавчо затвердженої програми економічних пріоритетів;
- наявність спеціальних державних служб контролю [1].

В системі забезпечення економічного добробуту та сталого розвитку країни важливе місце займає визначення приорітетних галузей національної промисловості; регулювання процедури стимулювання інвестицій; валютний контроль; розроблене законодавство про акціонерні товариства.

В Італії держава приділяє велику увагу зовнішньоекономічній експансії, яка здійснюється через економічну і технологічну прив'язку Італії до її закордонних партнерів. При цьому найбільш перспективними серед них можна назвати розвинуті країни та країни, що розвиваються: Африки, Азії, Латинської Америки. Акцент робиться також на італійську присутність за кордоном через розвиток міжнародної промислової кооперації і диверсифікацію постачальників енергоносіїв . Разом з тим держава в правових рамках використовує всі доступні механізми захисту інтересів власних виробників на внутрішньому і зовнішньому ринках.

Аналіз досвіду таких країн Західної Європи як Нідерланди, Бельгія, Данія, Люксембург, Швейцарія по забезпеченню економічної безпеки доводить, що їх основною стратегічною метою захисту національних економічних інтересів є забезпечення сталого економічного зростання та модернізації економіки відповідно до умов конкурентної боротьби на світовому ринку [2].

Політика забезпечення економічної безпеки Чехії, Польщі, Словаччини та країн Балтії базується на зближенні національних інтересів з загальноєвропейськими інтересами, а також політичної, економічної та

інституціональної трансформацією відповідно до західноєвропейських стандартів. На початку 90-х років ці країни обрали практично однакову модель забезпечення економічної безпеки, яка включала такі дії: оцінку геополітичної ситуації в регіоні; визначення вектора і стратегії розвитку; вибудовування і реалізацію моделі поведінки, в тому числі в сфері економіки, відповідно до домінуючими тенденціями регіонального та світового еволюційного процесу; співвіднесення базових кількісних і якісних показників розвитку з загальносвітовими і регіональними стандартами; коригування курсу економічних реформ [1].

Даючи загальну характеристику поточного стану розвитку сектора економічної безпеки в усіх розглянутих країнах, можна окремо виділити відносно стабільні економічні системи (Італія, Іспанія, Нідерланди, Німеччина, Франція). Ці країни переважно зосереджені на підвищенні ефективності економіки і одночасно підтримують існуючий рівень особистої економічної безпеки своїх громадян.

Адаптація будь-якого зарубіжного досвіду до умов конкретної країни трудомістка і являє собою не копіювання всієї системи регулювання, а лише поетапне впровадження окремих елементів, інструментів, методів, програм. Досвід зарубіжних країн варто запозичати, грунтуючись на схожості завдань, цілей, пріоритетів національних стратегій. Необхідно враховувати рівень економічного розвитку, розвитку інститутів управління, забезпечення та контролю над безпекою, використовуючи системний підхід і порівняльний аналіз. Моделі, які можна запропонувати за результатами вивчення досвіду країн Європейського Союзу, не тільки теоретично, але і практично можуть бути дієвими в будь-якій державі.

5.2. Світовий досвід розвитку служб безпеки підприємництва

Для розробки концепції підвищення національної безпеки будь-якої держави важливим є використання досвіду розвитку служб безпеки підприємництва в різних країнах світу.

Досвід Польщі. Сфера забезпечення безпеки підприємництва в Польщі регулюється трьома основними нормативними актами. Контрольні функції на ринку послуг безпеки здійснюють Міністерство внутрішніх справ і цивільна адміністрація. Державний контроль над ринком послуг безпеки в Польщі є одним з найжорсткіших у Європі. Відповідно до польського законодавства міністр внутрішніх справ і громадянська адміністрація за погодженням з головою Польського національного банку спільними постановами визначають принципи і порядок охорони, зберігання та перевезення грошових цінностей підприємцями.

Для здійснення господарської діяльності в сфері безпеки бізнесу компанії потрібна ліцензія, яка видається МВС. Недержавним суб'єктам господарювання на ринку послуг безпеки закон дозволяє надавати досить широкий спектр послуг, а саме:

- захист власності;
- особистий захист;
- відеоспостереження;
- інкасація;
- розробка, монтаж і обслуговування систем сигналізації;
- детективні послуги, юридична підтримка та ін. [5].

Отже, польський досвід доцільно застосувати в Україні для підвищення ефективності координації зусиль правоохоронних структур і органів регіонально-адміністративного менеджменту (органи місцевого самоврядування та місцеві державні адміністрації) з метою системного розвитку індустрії безпеки і забезпечення економічної безпеки малого підприємництва.

Досвід Чехії. У Чеській республіці не існує спеціального законодавства в галузі безпеки підприємництва та діяльності охоронних структур. Всі відносини регулюються законами в сфері малого підприємництва. Відомством, яке контролює ринок послуг безпеки, є Міністерство економіки Чеської республіки. Спеціальні питання безпеки підприємництва

контролюються Міністерством внутрішніх справ. Чехія, одна з восьми країн ЄС, де кількість працівників охоронних компаній перевищує кількість поліцейських. Процедура відкриття охоронної фірми в Чехії не складніше, ніж для будь-якого іншого підприємства. Всі вимоги відповідають положенням законодавства про державну реєстрацію підприємств .

Досвід Чехії є цінним в сфері державної реєстрації господарської діяльності суб'єктів безпеки, а також організації взаємодії державних і приватних структур в забезпеченні економічної безпеки малого підприємництва.

Досвід Угорщини. В Угорщині діяльність приватних структур безпеки регулюється актом IV від 1998 року і наказом міністра внутрішніх справ (24/1998 (VI.9) BM rendelet). Контроль діяльності приватних охоронних служб здійснює поліція. Законодавчими та директивними актами регулюються такі види діяльності підприємств в сфері безпеки підприємництва:

- охорона об'єктів;
- інкасація;
- охорона громадських заходів;
- особиста охорона;
- електронна розвідка і спостереження;
- приватні детективні послуги.

За кількістю приватних фахівців в сфері безпеки Угорщина займає перше місце в Європі. В Угорщині, з одного боку, діє досить проста процедура реєстрації приватного бізнесу в галузі безпеки, з іншого - до професійного рівня таких підприємців пред'являються суворі вимоги:

- господарська діяльність може здійснюватися тільки після видачі ліцензії поліцією;
- персонал повинен мати свідоцтва, видані поліцією;
- фірму необхідно зареєструвати в професійній палаті і т.д.

Професійна палата перевіряє суб'єкта господарювання, який має намір отримати ліцензію на відповідність ліцензійним вимогам і видає сертифікат.

Далі перевірку проводить поліція (протягом 30 днів), і тільки за результатами перевірки видає ліцензію.

Підготовка охоронців регламентується наказом міністра внутрішніх справ, її тривалість становить 320 годин. Курс навчання включає профільні теоретичні та практичні заняття, вивчення законодавства і ряду інших дисциплін, включаючи способи самооборони. По закінченню навчання співробітникам видається сертифікат відповідності. Кожен кандидат повинен пройти обов'язковий медичний огляд і психологічний тест (для тих, кому дозволено використання зброї). В разі порушення вимог до власників компаній можуть бути застосовані санкції: відкликання ліцензії, штрафи [4].

Отже, досвід Угорщини може бути корисним в сфері підготовки кадрів для індустрії безпеки підприємництва, а також в розробці ліцензійних вимог для суб'єктів ринку послуг і засобів безпеки.

Для визначення орієнтирів і шляхів розвитку ринку послуг і засобів безпеки будь-якої держави в перспективі, корисним буде досвід розвинених країн: США, Великобританії, Німеччини, Франції, Японії.

Досвід США. Досвід забезпечення економічної безпеки підприємництва в Сполучених штатах Америки є корисним для України, в першу чергу, в сфері організації взаємодії державних і недержавних структур безпеки. У США головну увагу в діяльності державних правоохоронних органів, громадських і приватних охоронно-детективних агентств направлено на реалізацію програми профілактики та протидії широкому спектру зловживань в сфері бізнесу . Така співпраця державних органів з недержавними структурами має тривалий характер і високу результативність, завдяки чому реалізація вищезазначених програм протидії правопорушенням у сфері бізнесу матеріалізується в мінімізацію втрат для підприємництва. На ринку послуг безпеки бізнесу США значне поширення набули адвокатські контори, приватні розшукові, детективні бюро і тому подібні суб'єкти господарювання. Послугами зазначених служб користуються не тільки приватні особи, а й державні органи. Діяльність таких організацій вигідна для держави, оскільки

вони не беруть з бюджету коштів, а навпаки, поповнюють його, сплачуючи податки. Також заслуговує на увагу для впровадження в Україні досвід США по створенню широкомасштабної системи колективної безпеки американського бізнесу, яка сформувалась з початку 90-х рр.

Досвід Великобританії. Великобританія має один з найбільш розвинених і найбільших ринків послуг безпеки в світі. За даними Британської асоціації охоронної індустрії (BSIA), в країні більше 8000 підприємств безпеки. Найбільшою часткою ринку (39%) сьогодні є послуги охоронних служб. Електронні системи безпеки займають приблизно 30% загального ринку безпеки, і являють собою сектор ринку, який найбільш динамічно розвивається. Інша джерело зростання ринку індустрії безпеки - системи спостереження за дорожнім рухом. Великобританію називають «державою камер». За даними BSIA, там встановлено понад мільйон камер, і попит на продукцію для відео спостереження продовжує рости. Після того, як установка відеокамер в громадських місцях по всій країні зменшила число злочинів і актів вандалізму, уряд планує збільшення асигнувань на такий вид послуг безпеки як відео спостереження.

Другий великий сектор ринку послуг безпеки - послуги приватної детективної діяльності. Приватні детективи розгорнули свою діяльність там, де дії правоохоронних органів заборонені і вважаються незаконними. Приватні детективні агентства здійснюють такі види діяльності:

- розробка заходів безпеки за контрактами з урядовими органами;
- ведення переговорів з терористами, які захопили заручників;
- виконання завдань клієнтів по спостереженню за їх близькими родичами; виявлення фактів подружньої зради;
- з'ясування фінансового стану та кредитоспроможності майбутніх партнерів по бізнесу [4].

Разом з тим в Великобританії взагалі відсутні спеціальні нормативні акти, які вимагають обов'язкової реєстрації приватних детективів. В цілому,

керівники приватних детективних агентств ставлять перед фахівцями досить складні завдання. Наприклад:

- приватні розслідування правопорушень, пов'язаних з комп'ютерними системами і шахрайством;
- забезпечення безпеки службових приміщень, автотранспорту, домашнього житла;
- виявлення техніки для прослуховування в цих приміщеннях;
- організацію особистої охорони керівництва, окремих клієнтів і працівників фірм і т. д.

Значний досвід, накопичений в Великобританії в сфері безпеки вантажних і пасажирських перевезень, завдяки чому транспортні компанії розробляють спільні заходи з протидії нападів на інкасаторів, аварій, а також заходи спостереження на маршрутах перевезення цінностей і т. п.

Досвід Великобританії корисний в сфері формування системи профілактичних заходів в діяльності служб безпеки суб'єктів підприємництва. Зазначена система включає в себе як окремі, так і загальні профілактичні заходи.

Досвід Німеччини. Для сприйняття і застосування успішного досвіду в галузі недержавного забезпечення економічної безпеки малого підприємництва в Україні особливо цікавими є процеси, що відбуваються в секторі ринку приватних послуг безпеки в Федеративній Республіці Німеччині. Спектр послуг безпеки, які пропонуються німецькими фірмами, є досить широким - від контролю над безпекою в окремому житловому будинку або кварталі до забезпечення безпеки і охорони окремих підприємств, концернів, аеропортів, громадських приміщень, перевезення цінностей і грошей.

Приватні служби безпеки в Німеччині діляться на дві групи:

1) агентства, які надають фірмам і державним установам послуги з забезпечення фізичної безпеки об'єктів і осіб;

2) служби охорони виробництва, створені самими фірмами і установами.

Для відкриття приватної служби безпеки, а також укладення приватним охоронним підприємством контракту з будь-яким замовником (відомством, підприємством, фірмою), відповідно до закоу про приватні підприємства, необхідно мати спеціальний дозвіл влади. У дозволі може бути відмовлено, якщо приватна служба не забезпечує належного рівня охорони або не має для цього достатніх професійних, фінансових, технічних та інших можливостей.

Досвід Франції. Останнім часом як основну тенденцію розвитку системи економічної безпеки підприємництва у Франції слід виділити стрімке нарощування діяльності служб безпеки в промислово-торговельних фірмах і фінансових інститутах. Функції контролю над діяльністю приватних структур безпеки віднесені до компетенції МВС Франції. Ринок послуг безпеки охоплює наступні сфери: фізичний захист, перевезення цінностей, електронна безпеку, безпеку в аеропортах. Відповідно до законодавства, основними вимогами до співробітників підприємств, які надають послуги на ринку безпеки, і службам безпеки фірм є: наявність ліцензії, яку видає поліція; заборона іншої діяльності; відсутність судимостей; обов'язкове навчання. У Франції створена система навчальних закладів для підготовки співробітників приватних служб безпеки, приватні, національні та внутрішні програми навчання. Великий досвід Франція має в сфері кібербезпеки. В інформаційній сфері діють десятки правових актів, які детально регулюють статус суб'єктів інформаційної діяльності, режим інформаційного обміну.

Досвід Японії. Експертами відзначається інтенсивний розвиток протягом останнього десятиліття приватних служб безпеки Японії. Діапазон послуг приватних служб безпеки досить широкий. У зв'язку із зростанням економічних злочинів приватні служби безпеки підприємств Японії приділяють підвищену увагу створенню систем комплексного захисту. Корпоративний захист забезпечує ефективний контроль над усією діяльністю підприємства, починаючи від ділових зв'язків з партнерами і аж до персоналу, захист від промислового шпигунства і шахрайства з боку своїх співробітників, партнерів по бізнесу. Заходи корпоративного захисту забезпечують також

конфіденційність інформації про вжиті управлінням підприємствах рішеннях; планування і проведення регулярних перевірок робочих і службовців.

Особливе значення надається розробці стратегій і програм діяльності в кризових ситуаціях. Особливе місце в забезпеченні безпеки японських фірм займає проведення інформаційно-аналітичної діяльності. Вона має метою створення інформаційної бази даних по певній тематиці за рахунок обробки офіційних джерел і накопичення відомостей, отриманих від контактів і зв'язків з числа місцевих громадян. Аналітична обробка цих інформаційних масивів з урахуванням оперативної інформації дозволяє оцінити стабільність економічної ситуації, обстановки в певному регіоні або країні і ймовірність безпосередньої загрози для корпорації [5, с.13-20].

В Японії створений центр кібернетичної безпеки, яка координує зусилля держави і приватного підприємництва в цій сфері, включаючи підготовку спеціалістів.

Тож досвід Японії в забезпеченні економічної безпеки підприємницької діяльності може бути застосований в Україні в процесі формування національної системи економічної безпеки та кібербезпеки малого підприємництва, а також, комплексних систем безпеки підприємств.

Отже, аналіз світового досвіду розвитку індустрії безпеки підприємництва, дозволив зробити висновки і узагальнення, які доцільно використовувати для розвитку такої індустрії в Україні.

По-перше. Функціонування індустрії безпеки підприємництва регламентується законодавством в сфері охоронної, детективної (розшукової) діяльності, обороту зброї тощо. Держава встановлює правила ліцензування, професійні вимоги та інші нормативи приватної господарської діяльності на ринку послуг безпеки.

По-друге. На ринку послуг безпеки, який є за своєю економічною природою ринком монополістичної конкуренції, з одного боку - тісно взаємодіють, а з іншого - конкурують між собою суб'єкти державної і недержавної форм власності. Форми і види взаємодії і конкуренції

визначаються рівнем розвитку ринку послуг безпеки, рівнем правової культури і національною специфікою. Природне призначення такої взаємодії і конкуренції - забезпечення безпеки бізнесу, суспільства, навколишнього середовища.

По-третє. Система економічної безпеки малого підприємництва може бути дієвої тільки в межах широкомасштабної системи безпеки бізнесу, яка створюється зусиллями держави, приватних суб'єктів безпеки бізнесу, суб'єктів підприємницької діяльності, громадських організацій, суспільства в цілому.

Таким чином, використання конструктивного зарубіжного досвіду, з урахуванням специфіки державного і ринкового регулювання суспільних відносин в Україні, дозволить значно прискорити формування ефективної індустрії безпеки підприємництва.

5.3. Сучасний стан національної безпеки Польщі

Під системою національної безпеки в Республіці Польща (РП) розуміється сукупність держструктур і нормативно-правових актів, що стосуються даної сфери, а також комплексу взаємопов'язаних заходів політичного, економічного, організаційного, правового, ідеологічного та іншого характеру, спрямованих на захист життєво важливих інтересів особистості, суспільства і держави.

В умовах сучасної геополітичної обстановки польським військово-політичним керівництвом (ВВР) вироблені підходи до забезпечення національної безпеки, які знайшли своє відображення в конституції країни, "Стратегії національної безпеки Республіки Польща" 2014 року, міжнародно-правових актах, укладених за участю РП, а також в ряді документів стратегічного характеру.

На стан національної безпеки Польщі в XXI столітті значний вплив мають світові глобальні процеси, які характеризуються високою динамікою і

наявністю нетрадиційних загроз, найбільшу небезпеку з яких представляють тероризм, міжнародна організована злочинність, економічна нестабільність, масова міграція населення з неблагополучних регіонів світу, правопорушення в комп'ютерній сфері (кіберпросторі).

Забезпечення зовнішньої безпеки республіки, зміцнення її військового та економічного потенціалу нерозривно пов'язані з розвитком військово-політичної обстановки (ВПО) в світі. Аналіз сучасних загроз зумовлює вдосконалення національних сил і засобів безпеки в напрямку інтеграції до міжнародної системи безпеки, яка дозволяє одночасно задіяти елементи оборони держави та кризового управління. Єдине планування і підготовка військових і цивільних компонентів на кожному рівні реагування, комплексний підхід до своєчасного вирішення різнорідних проблем, а також створення стабільних механізмів фінансування цих процесів є основою зміцнення обороноздатності держави та ефективними інструментами його розвитку.

До головних загроз внутрішньої безпеки польське керівництво відносить [6]:

- виникнення різного роду кризових ситуацій, які можуть привести до дестабілізації політичної системи управління державою;
- порушення функціонування економічних і суспільних механізмів;
- недотримання конституційних прав громадян;
- погіршення соціального становища населення;
- розвиток демографічних проблем;
- забруднення навколишнього середовища;
- виникненя стихійних лих , техногенних катастроф;
- виникнення дефіциту водних та енергетичних ресурсів, корисних копалин та інших серйозних наслідків.

Згідно "Стратегії національної безпеки" відношення Польщі до Північноатлантичного та Європейського союзів надає гарантії безпеки

держави, забезпечує можливість її всебічного розвитку, а також сприяє посиленню позицій РП на міжнародній арені.

Найбільш важливим фактором забезпечення національної безпеки польське керівництво вважає членство країни в НАТО. Варшава підтримує плани подальшого просування альянсу до кордонів Росії і прагне до виконання взятих на себе союзницьких зобов'язань щодо посилення присутності блоку в різних регіонах світу. Підкреслюючи провідну роль США в забезпеченні стабільності і безпеки в Європі, Польща виступає за збереження американської військової присутності на континенті в цілому і на своїй території зокрема.

Однією з пріоритетних завдань зовнішньої політики країни є зміцнення її позицій в Європейському союзі. Варшава розглядає поглиблення політичної та економічної інтеграції, а також проведення узгоджених дій в рамках організації в якості інструментів, що сприяють досягненню національних цілей і забезпеченню захисту державних інтересів.

В інтересах формування комплексної системи національної безпеки, прийнято рішення про перегляд підходів до її формування. У зв'язку з цим президент країни в 2013 році затвердив розроблену урядом країни "Стратегію розвитку системи національної безпеки Республіки Польща до 2022 року". Вона визначає основні напрями взаємодії різних інститутів державної влади, органів місцевого самоврядування та громадських організацій щодо забезпечення захисту національних інтересів, безпеки особистості, суспільства і держави. Крім того, в документі враховані основні положення Стратегічної концепції НАТО та Європейської стратегії безпеки.

Головною метою Стратегії є підвищення ефективності і цілісності системи безпеки країни, яка повинна бути здатна забезпечити своєчасне розкриття і ліквідацію джерел загроз державі, а також готова до усунення наслідків цих загроз.

Досягти цієї мети планується шляхом реалізації п'яти напрямків, які мають важливе значення для забезпечення безпеки держави [6].

1. ***Участь Польщі у формуванні стабільної системи міжнародної безпеки.*** Пріоритетну увагу планується приділити підвищенню ролі країни в системі глобальної та регіональної безпеки за рахунок активізації діяльності в НАТО і ЄС, а також належного виконання коаліційних зобов'язань шляхом участі в наступних заходах:

- забезпеченні колективної оборони;
- операціях кризового врегулювання;
- програмах з розвитку бойових можливостей збройних сил;
- формуванні багатонаціональних бойових тактичних груп;
- заходах щодо вдосконалення військової інфраструктури;
- зміцненні енергетичної та інформаційної безпеки.

Одночасно передбачається розвивати стратегічне партнерство з США, Великобританією, Німеччиною, Францією, Угорщиною, Словаччиною, Чехією та з країнами Балтії на двосторонній основі, а також в рамках міжнародних і регіональних організацій.

Крім того, Польща продовжить свою діяльність по зміцненню ролі та ефективності ООН і ОБСЄ в області моніторингу за дотриманням норм міжнародного права, а також з підтримки режимів нерозповсюдження зброї масового ураження і контролю над звичайними озброєннями.

2. Зміцнення обороноздатності держави. Головним завданням визначено посилення військового потенціалу національних збройних сил в інтересах їх участі у забезпеченні оборони держави і коаліційних операціях кризового врегулювання в різних регіонах світу. При цьому основні зусилля планується спрямувати на практичну реалізацію сучасних підходів до планування, будівництва, підготовки та застосування ЗС, в тому числі вдосконалення їх організаційно-штатної структури, а також системи оперативної і бойової підготовки відповідно до вимог НАТО. В якості важливих факторів розглядаються вдосконалення інформаційно-аналітичної та розвідувальної діяльності в інтересах інформування ВВР країни, а також

розвиток державних наукових організацій, здатних забезпечити потреби національної оборони за рахунок ефективної координації НДДКР.

3. Підвищення стійкості критичної інфраструктури держави до погроз різного характеру. Основні зусилля передбачається зосередити на забезпеченні більшої захищеності життєво важливих елементів інфраструктури держави від впливу військових і невійськових загроз, що сприяють порушенню їх безперервного функціонування. Для цього необхідне налагодження ефективної взаємодії сил і засобів з охорони критично важливих об'єктів інфраструктури із залученням держави. Крім того, необхідно створити сучасні системи стратегічних резервів, охорони держкордону, особистих даних і секретної інформації, своєчасного попередження про стихійні лиха і ряд інших систем, а також забезпечити умови для безпечного розвитку національної атомної енергетики.

4. Соціально-економічний розвиток держави в інтересах зміцнення національної безпеки. Велике значення має розширення взаємодії силових структур з органами державної влади та місцевого самоврядування з метою реалізації оборонної політики РП невідривно від здійснення програм регіонального розвитку, підвищення якості середньої та вищої освіти з урахуванням вимог до забезпечення національної безпеки, патріотичного виховання молоді, підвищення привабливості та престижу військової служби серед населення.

При цьому заплановано забезпечити участь фахівців військового відомства в розробці стратегій розвитку воєводств, проектуванні комплексних програм вдосконалення інфраструктури регіонів, а також у виробленні підходів до спільного використання об'єктів і територій військового і цивільного призначення (аеродромів, морських і річкових портів, військових містечок, транспортних вузлів, ділянок місцевості та ін.).

Важливим моментом є організація перепідготовки по затребуваним цивільними спеціальностями військовослужбовців, що проходять військову

службу за контрактом, з подальшим їх працевлаштуванням при звільненні з військової служби.

5. Створення умов для розвитку інтегрованої системи національної безпеки. Своєчасне реагування на зміни, що відбуваються у військово-політичній обстановці вимагає від органів державної влади постійного розвитку системи управління національною безпекою. Необхідними умовами для цього є вдосконалення нормативно-правової бази, реалізація комплексу заходів в інтересах безперервного функціонування та координації дій всіх суб'єктів системи, а також забезпечення і підтримання взаємозв'язку між процесами планування, контролю та оцінки стану захищеності держави.

Структура системи національної безпеки включає дві підсистеми - управління і виконавчу. До першої входять органи державної влади Польщі, відповідальні за формування політики в галузі зміцнення обороноздатності, забезпечення зовнішньої і внутрішньої безпеки держави -адміністрації президента, парламент і Рада міністрів. Виконавча підсистема включає до свого складу сили і засоби, які залишаються в розпорядженні уряду, міністерств і відомств, спеціальних служб, інших державних інститутів і відповідальних суб'єктів, регіональних органів управління (адміністрацій воєводств) і органів місцевого самоврядування.

Головними суб'єктами виконавчої підсистеми, які несуть відповідальність за зміцнення обороноздатності, а також за забезпечення зовнішньої і внутрішньої безпеки, в Стратегії визначено МЗС, МО та спеціальні служби.

Основними напрямками діяльності зовнішньополітичного відомства в системі міжнародних відносин є: реалізація національних інтересів в сфері захисту суверенітету і територіальної цілісності держави; сприяння його соціально-економічного розвитку, формування позитивного образу Польщі у світі; надання всебічної консульської допомоги польським громадянам за кордоном, а також охорона культурної спадщини. При цьому необхідно

забезпечити і нарощувати національну присутність у всіх міжнародних структурах, і в першу чергу на керівних постах.

Одним з основних елементів системи національної безпеки є система оборони держави, провідна роль в якій відводиться збройним силам РП. Вони покликані підтримувати і зміцнювати обороноздатність країни, своєчасно і ефективно реагувати на зовнішні та внутрішні військово-політичні загрози, виконувати союзницькі зобов'язання в рамках членства в НАТО і ЄС, а також брати участь в міжнародних операціях з кризового урегулювання відповідно до мандату ООН.

В інтересах вирішення цих завдань необхідно забезпечити безперервний розвиток бойових можливостей ЗС, виконання вимог керівництва НАТО щодо оптимізації їх організаційної структури і системи управління, підвищення якості оперативної і бойової підготовки військ (сил) і професійного рівня особового складу, переоснащення сучасними видами озброєння і військової техніки, а також всебічне забезпечення діяльності армії та флоту.

Особливе місце в системі національної безпеки Польщі займають спеціальні служби, головним обов'язком яких є завчасне надання керівництву країни інформації, що має значення для прийняття політичних рішень стратегічного характеру, формуванню позицій в міжнародних організаціях, розвитку військового потенціалу держави та його економічного зростання.

Пріоритетну увагу спецслужб необхідно направити на попередження та запобігання терористичній загрозі, припиненню діяльності міжнародної і національної організованої злочинності. До завдань спецслужб входить також охорона, розвідувальне та контррозвідувальний забезпечення польських зарубіжних представництв і контингентів збройних сил у складі міжнародних миротворчих місій і угруповань військ , які беруть участь в операціях з кризового урегулювання.

Невід'ємною частиною системи національної безпеки є система кризового управління держави, яка повинна забезпечувати завчасне прогнозування,

своєчасне реагування на кризові ситуації різного масштабу, а також оперативне усунення їх наслідків з залученням усіх наявних сил і засобів.

Згідно з планами, після удосконалення даної системи кризові штаби і центри органів державної влади, місцевого самоврядування, міністерств і відомств, силових структур, а також економічних суб'єктів стратегічного значення увійдуть в єдиний інформаційний простір, що дозволить ефективно вирішувати поставлені завдання в області кризового управління.

Координатором з питань реалізації Стратегії є міністр оборони Польщі, який діє від імені голови уряду країни. Виконання запланованих заходів буде оцінюватися за результатами щорічних звітів, підготовлених на основі даних від міністерств, відомств, інших державних інститутів і відповідальних суб'єктів, регіональних органів управління і органів місцевого самоврядування.

Для забезпечення якісного розвитку системи національної безпеки передбачається раз в чотири роки проводити уточнення положень Стратегії з внесенням до неї змін і доповнень відповідно до розвитку ВПО в світі і соціально-економічної ситуації в країні.

В цілому аналіз "Стратегії розвитку системи національної безпеки до 2022 року" свідчить про те, що польське керівництво має намір продовжити діяльність по зміцненню своїх позицій в рамках міжнародних організацій, в першу чергу в НАТО і ЄС. При цьому силові структури держави вважаються одним із головних інструментів реалізації її політичних та економічниї інтересів.

5.4. Загрози безпеці Польщі на сучасному етапі

На початку двадцять першого століття загрози безпеки Польщі були істотно

переглянуті, і вони продовжують змінюватися. З'явилися нові джерела потенційного конфлікту, які можуть стати серйозними викликами і

представляти велику загрозу національній. Щоб зустріти ці виклики і ефективно нейтралізувати загрози системі національної безпеки, польському керівництву необхідно визначити, які з загроз за своїм характером є найбільш фундаментальними і які мають другорядне значення.

Дилеми держави, що стосуються питань безпеки, в літературі зазвичай називаються викликами національній безпеці. Ці виклики можна прийняти або знехтувати ними, і будь-яке з цих рішень може створити як додаткові можливості, так і додаткові загрози.

Зараз швидко розвивається явище, яке наражає на небезпеку польські національні інтереси, причиною яких є транскордонна організована злочинність. Цей тип преступності пов'язаний з контрабандою зброї, небезпечних матеріалів, людей, наркотиків, з використанням таких методів як відмивання грошей і корупція. Потенційна загроза полягає в потенціалі масової міграції окремих людей або трансграничного транспорту матеріалів, які можуть стати загрозою для безпеки Польщі. Центральне розташування Польщі на європейському континенті збільшує існуючі ризики в цій сфері, хоча ймовірність масової міграції такого типу на даний момент обмежена. Зараз Польща повинна враховувати економічні та соціальні наслідки міграційних процесів і нейтралізувати їх негативні наслідки.

В наші дні головним викликом для державних служб безпеки всередині Польщі є істотний масштаб економічної міграції. Територія Польщі завдяки географічному розташуванню і відносній доступності може так само служити зручною логістичної базою, де можна проводити підготовку і звідки можливо вживати дії проти громадян, інституцій та компаній в інших країнах. Це включає ймовірність того, що Польща може служити розподільчим центром (а не просто коридором) для незаконного обігу наркотиків та торгівлі людьми.

В останні роки в Польщі спостерігається збільшення активності транснаціональних кримінальних груп, що призводить до різноманітних соціальних патологій. Це серйозна загроза для Польщі. Але саме людські дії, безпосередньо чи опосередковано, є найбільш серйозними загрозами для

польської національної безпеки. Наряду з природними небезпеками суборганіческого характеру ці загрози включають технічні, соціальні та екологічні ризики.

Найбільш часто зустрічається загроза, що виникає безпосередньо в результаті людської недбалості, навмисних дій, або побічно через незнання правил, принципів захисту або через відмову обладнання.

Хімічне забруднення є серйозною загрозою національній безпеці. Токсичні промислові речовини супроводжують розвиток металлургійної і автомобільної промисловості, виробництво каучуку, добрив, фарб та лаків, як і багатьох інших галузей промисловості.

Інша категорія загроз включає технічні ризики, пов'язані зі будівельними і транспортними аваріями. Вони можуть відбуватися в житлових будинках і промислових спорудах, на об'єктах і засобах транспорту.

Соціальні ризики є іншим видом загроз для національної безпеки і їх причиною є безпосередньо або побічно людина . Основні причини, що лежать в основі цих ризиків- це зубожіння суспільства, бідність, зростаюча нерівність між бідними і багатими, гендерна дискримінація, безробіття і зростаючий дисбаланс між кількістю працюючих і кількістю пенсіонерів.

Крім того, загрози, що виникають від комп'ютерних систем і мереж - кіберзлочини і кібертерроризм, теж входять в категорію соціальних загроз з очевидною тенденєю до зростання. Соціальні наслідки таких загроз впливають на ключові фактори в системі національної безпеки: на особистості, соціальні групи і організації, які у все більшій мірі залежать від інформаційних технологій. У Польщі ця небезпека загрожує мільйонам громадянам, а в глобальному масштабі ризику піддаються як мінімум два мільярди людей.

Окрім цього, непряма загроза національній безпеці Польщі надходить від колапсу світових держав, від їх нестабільності та від ризиків, пов'язаних з авторитарними і тоталітарними режимами, які підтримують ескалацію міжнародного тероризму. У таких країнах соціально-економічна недорозвиненість є причиною соціального невдоволення і економічної

міграції. Деякі з економічних мігрантів можуть приїхати в Польщу через поліпшенням економічної ситуації в їх країні. Можна припустити, що не всі з них встигнуть соціально адаптуватися до життя в Польщі та деякі можуть стати ризиковими факторами.

Енергетичні загрози, зумовлені різними причинами, включаючи недостатність диверсифікації поставок енергоресурсів, зокрема нафти і природного газу, також є серйозною проблемою для безпеки Польщі.

Крім того, її безпека може опинитися під загрозою через зрив світової торгівлі і певних дій з боку наших сусідів зі Сходу, пов'язаних з прийняттям стандартів вільної торгівлі.

Розвиток інформаційних технологій і систем комунікацій, пов'язаних з ринками капіталу, викликає появлення нових загроз, які можуть порушити стабільність фінансової ситуації в Польщі.

Екологічні небезпеки також є дуже важливою категорією для національної безпеки Республіки Польща. В якості основних причин таких загроз являються демографічні, географічні, технічні, економічні та соціально-культурні. Всі ці джерела, кожен по-своєму, викликають погіршення стану навколишнього середовища, в кінцевому підсумку загрожуючи життю, здоровью і суспільному добробуту.

Збільшується кількість людей, які проживають в Польщі, в тому числі і тих, які мігрували з авторитарних і тоталітарних держав. Вони можуть підірвати екологічний баланс і здатність інфраструктури держави забезпечувати існування зростаючого населення. В свою чергу, географічної розрив між кількістю природних ресурсів, необхідних для життя людини, і реальними можливостями даної географічної області, сприймається як загроза екологічній катастрофі. Така ситуація призводить до збільшення забруднення в процесі отримання необхідних ресурсів.

Екологічні технічні ризикові чинники виникають в основному від використання в Польщі застарілих технологій, які зазвичай виробляють значну кількість вуглекислого газу, що забруднює атмосферу. Джерела

еколого-економічних ризиків пов'язані з розміщенням на території Польщі таких видів виробництва, що становлять підвищену екологічне навантаження для більш розвинених країн. Ці явища, поряд з відсутністю законодавчих заходів для регулювання процесів, що забруднюють навколишнє середовище в країнах, що розвиваються, знижують рівень екологічної безпеки країни.

Крім того, екологічні соціально-культурні небезпеки являються наслідком факту того, що Польща розвивається швидкими темпами, але поки недостатньо інвестує в охорону навколишнього середовища. Це може перетворитися в істотну загрозу. Найбільш небезпечними явищами, які знижують екологічну безпеку, є глобальне потепління, виснаження озонового шару, кислотні дощі.

Отже, сучасна система національної безпеки повинна відповідати багатьом викликам і загрозам на адресу держави. Найбільш важливі виклики і загрози безпеці Польщі, які існують в даний час:

1. Економічна глобалізація і регіоналізація, в результаті чого відбувається вільний руху капіталів, товарів, інформації та людей;

2. Процеси демократизації в соціально-політичній і економічній сфері;

3. Міжнародний тероризм;

4. Неконтрольоване розповсюдження зброї масового знищення і системи його доставки;

5. Організована злочинність;

7. Збільшення міграції населення;

8. Комп'ютеризація всіх сфер життя;

9. Забезпечення енергетичної безпеки (в основному поставок нафти і природного газу);

10. Зміни клімату, викликані глобальним потеплінням, пов'язаним з забрудненням навколишнього середовища.

Сучасні виклики і загрози вимагають поглиблення взаємозалежності національних інтересів в сфері безпеки різних країн, про що свідчить тенденція відходу від національних систем державної безпеки до міжнародних

систем. У зв'язку з динамікою і масштабами змін у Європі та світі, польська система безпеки потребує адаптації до динамічних світових вимог (умовам, стандартам, очікуванням).

5.5. Приклад організації системи безпеки масового заходу футбольного клубу згідно польського законодавства

Разом із зростанням економічної та соціальної значимості спорту футбол став найпоширенішим видом спорту в світі та найбільш популярним видом спорту у багатьох країнах. Футбол має велику кількість фанатів, що різняться від лояльних, які щотижня відвідують гру свого клубу, до пасивних, які спостерігають за грою вдома біля телевізора. Футбол може виступати не лише джерелом прибутку, але й інструментом місцевого економічного розвитку, соціальної єдності, освіти, особистого розвитку та передачі людських та культурних цінностей.

Зважаючи на міжнародний характер футболу, актуальним є обговорення дій футбольного клубу як конкретного суб’єкту, на який поширюються положення польського Закону про масові заходи. Погляд на футбольний клуб як на підприємство, яке в своїй діяльності стає організатором масового заходу, яким є футбольний матч, вимагає особливого дослідження прав та обов'язків, покладених на нього у цій справі. Спеціальні зобов'язання включають забезпечення безпечного проведення масових заходів.

1. Футбольний клуб як підприємство відповідно чинного законодавства

Згідно з правом Європейського Союзу, спортивні організації, зокрема спортивні клуби, а серед них - футбольні клуби, безперечно, вважаються за підприємство. Хоча ні договір про утворення Європейського Союзу, ні Договір про функціонування Європейського Союзу не містить визначення

поняття підприємство, цей термін пояснюється в підзаконних актах Європейського Союзу і був роз'яснений в рішеннях Європейського Суду.

Відповідно до ст. 1 Додатку до Першого Загального Розпорядження Європейської Комісії № 800/2008 від 6 серпня 2008 року, підприємство - це суб'єкт господарювання, який здійснює господарську діяльність, незалежно від його правової форми. Це стосується, зокрема, зайнятих осіб та сімейних підприємств, а також компаній чи консорціумів, які регулярною займаються підприємницькою діяльністю [7].

Тобто немає значення, яку правову форму згідно з національним законодавством повинно мати підприємство, коли воно діє на ринку. У своєму рішенні у справі C-222/04 Європейський суд зазначив, що будь-яка діяльність, що полягає у пропонуванні товарів чи послуг на даному ринку, є економічною діяльністю [8]. Сумніви щодо того, чи є спортивний клуб підприємством, були однозначно вирішені Судом Європейського Союзу в рішенні від 12 грудня 1974 року в справі № 36,74 Walrave [9].

В епоху професіоналізації та комерціалізації спортивні клуби, щоб вижити та розвинути свій соціальний напрям діяльності - пропагування фізичної культури, керуються не лише елементом соціалізації, а й необхідністю здобути конкурентну перевагу, яка необхідна всім підприємством, що конкурують за увагу покупців [9].

Таким чином, прийняття рішення Європейським Судом стало необхідним, оскільки законодавство ЄС про конкуренцію не містить конкретних правових положень, що стосуються конкуренції у галузі спорту. На думку Європейського Суду, цю сферу охоплюють загальні правила конкуренції, за умови, що вона є економічною діяльністю [9].

Це і наступні рішення, а також практика Європейської комісії підтверджують, що спортивні клуби, спортивні об'єднання, національні та міжнародні спортивні федерації є підприємством в межах змісту статті 101 та 102 Договору про функціонування Європейського Союзу.

Як аматорські, так і професійні спортивні клуби, а також фізичні особи вважатимуться підприємствами, якщо вони здійснюють економічну або комерційну діяльність, що полягає у пропонуванні товарів чи послуг, навіть якщо ця діяльність приносить невеликі прибутки або її мета - не отримувати прибуток взагалі.

Діяльність спортивних клубів включає, серед іншого, продаж квитків на спортивні матчі або угоди про трансфер гравців. Розмір спортивного клубу не має значення, бо економічний успіх не залежить від його форми власності.

Як приклад джерела доходу для спортивних організацій, Європейська комісія наводить клубні збори, продаж квитків, рекламу і спонсорство, права ЗМІ, перерозподіл доходу в спортивних федераціях і державне фінансування. Нарешті, самі гравці отримують винагороду за надані ними послуги. Спортивні клуби, готові запропонувати якомога більшу суму для даного гравця, не тільки впливають на його діяльність щодо досягнення спортивних досягнень, але й сприяють збільшенню комерційного потенціалу клубу [7].

З вищевикладеного очевидно, що футбольний клуб є підприємством, незалежно від того, приносить його діяльність реальні зиски чи ні.

Таким чином, футбольний клуб, як підприємство, використовує повноваження, надані йому відповідно до національного та міжнародного права, але також несе відповідальність за виконання обов'язків, покладених на нього відповідно до законодавства, зокрема обов'язків забезпечення безпеки його діяльності.

2. Обов'язки футбольного клубу, як підприємства, по забезпеченню безпеки масового заходу - футбольного матчу

З точки зору теми даної статті, важливо, що футбольний клуб в Польщі є одним із суб'єктів, у якого є спеціальні обов'язки щодо забезпечення безпеки його діяльності, як підприємства. Мова йде про Закон про безпеку масових заходів від 20 березня 2009 року (далі: Закон), а також про Правила, що стосуються безпеки під час змагань, організованих польською футбольною

асоціацією та Ekstroklasy S.A. (далі: Правила безпеки) і Дисциплінарні Правила Польської футбольної асоціації (далі: Дисциплінарні правила).

Особливе значення має згаданий вище закон про безпеку масових заходів. Він визначає:

1) правила поведінки, необхідні для забезпечення безпеки масових заходів, в даному випадку - футбольного матчу;

2) умови безпеки масових заходів;

3) правила та порядок видачі дозволів на проведення масових заходів;

4) правила обробки інформації щодо безпеки масових заходів, включаючи персональні дані;

5) відповідальність організаторів за шкоду, заподіяну у зв'язку з організацією масових заходів [10].

Відповідно до положень цього закону масовим заходом є, зокрема, масовий спортивний захід, в тому числі футбольний матч [10].

Під поняттям «футбольний матч» слід розуміти масовий спортивний захід з метою змагання з дисципліни футбол, який організовано на стадіоні або в інший спортивній споруді, де кількість наданих організатором місць для людей визначена відповідно до положень будівельного законодавства і нормативних актів з пожежної безпеки, і є не менше 1000 місць [10].

Особливе значення має також пояснення поняття ризикованого масового заходу (ризикованого футбольного матчу), тому що, якщо масовий захід вважається за ризикований, на організатора цього заходу - футбольний клуб - покладаються додаткові спеціальні обов'язки по забезпеченню його безпеки. Тому ризиковим масовим заходом є масовий захід, під час якого, згідно з інформацією про передбачувані загрози чи минулий досвід щодо поведінки учасників, існує страх перед діями насильства чи агресії [10]. Як відповідні приклади слід вказати на матчі, що відбулися між Лехом Познань та Легією Варшава , ФК « Barcelona» та «Real Madryt».

Коли футбольний клуб є організатором футбольного матчу, він зобов’язаний до виконання обов’язків, накладених зазначеними вище

законодавчими актами. Обов’язки є різні в залежності від розміру масового заходу і осіб, що беруть участь в ньому. Однак організатор футбольного матчу в будь якому випадку зобов’язаний забезпечити проведення масового заходу. Забезпечення проведення масових заходів означає узгоджені дії, які здійснюються з метою забезпечення громадської безпеки та порядку в зв'язку з масовим заходом.

Безпека масових заходів включає дотримання організатором таких вимог:

1) забезпечення безпеки осіб, які беруть участь у заході;

2) охорона громадського порядку;

3) медичне забезпечення;

4) забезпечення відповідного технічного стану будівельних конструкцій разом з технічними установками та пристроями, що обслуговують ці об’єкти, зокрема пожежно-санітарні [10].

Футбольний клуб, який організовує матч, зобов’язаний розпочати дії з забезпечення проведення масового заходу ще до його початку, так як, щоб зорганізувати футбольний матч, організатор не пізніше, ніж за 30 днів до запланованої дати його початку:

1) подає органу (голова громади, міський голова) запит на дозвіл щодо проведення масового заходу;

2) звертається до керівництва районної поліції та муніципального коменданта Державної пожежної служби, диспетчера медичних рятувальних бригад та державного санітарного інспектора із запитом про надання висновку про кількість сил та ресурсів, необхідних для забезпечення масового заходу, заперечення щодо технічного стану об’єкта та передбачуваних загроз;

3) повідомляє місцевих командирів відділення прикордонної служби у разі проведення масового заходу в прикордонній зоні, командирів військової поліції, у разі проведення масового заходу на територіях, підпорядкованих Міністру національної оборони [10].

Місцеві - начальник поліції, комендант Державної пожежної служби, диспетчер бригад екстреної медичної допомоги та державний санітарний інспектор видають висновки, які потім стають підставою для видачі чи відмови у видачі дозволу на проведення масового заходу [11].

Закон детально визначає наступні зобов'язання організатора, які включають:

1) дотримання вимог, указаних, зокрема, положеннями будівельного закону, санітарних та протипожежних норм;

2) участь служб безпеки, інформаційних служб та менеджера з безпеки;

3) надання медичної допомоги;

4) забезпечення засобами гігієни та санітарії;

5) призначення шляхів евакуації та доріг, що забезпечують доступ транспортним засобам рятувальних служб та поліції;

6) приготування рятувального та протипожежного обладнання та засобів пожежогасіння, необхідних для проведення масового заходу;

8) забезпечення окремими кімнатами для служб управління масовими заходами [10].

Кількість членів служби безпеки визначається таким чином:

1) у разі проведення масового заходу, який не є масовим заходом високого ризику (ризиковим), - щонайменше 10 членів служби безпеки на 300 осіб, які можуть бути присутніми на масовому заході, і щонайменше 1 член служби безпеки на кожні наступні 100 осіб;

2) у разі масового заходу з високим рівнем ризику - не менше 15 членів служби безпеки для 200 осіб, які можуть бути присутніми на масовому заході, і щонайменше 2 члени служби безпеки на кожні наступні 100 осіб [10].

Закон також передбачає детальні регламенти щодо місць, наданих у разі масових заходів високого ризику. У випадку організації масового заходу, кваліфікованого як масовий захід масового ризику, кількість місць, передбачених організатором, повинна становити не менше 200 [11].

Крім того, для організатору футбольного матчу, якщо ним є клуб, який бере участь у змаганнях одного з трьох вищих змагальних класів змагань серед чоловіків (тобто Екстракласа, I ліга, II ліга), незалежно від виду змагань (національних чи міжнародних), забезпечує ідентифікацію людей, які беруть участь у цій події. Продаж вхідного квитка на футбольний матч або іншого документа, який уповноважує дану особу бути присутньою на заході, відбувається лише після отримання основних персональних даних цієї особи відповідно до документа, що посвідчує особу (посвідчення особи, тимчасове посвідчення особи, паспорт, посвідчення водія, або інший документ, що підтверджує особу із зображенням обличчя та адресом проживання). Цікаво, що такий обов'язок був покладений лише на футбольний клуб, який організовує футбольний матч. Організатори інших масових заходів, ніж футбольний матч, під час продажу квитків на заходи можуть вимагати від покупця пред'явити документ, що посвідчує його особу, але то ні є обов'язковим [10].

Що стосується міжнародних футбольних матчів, включаючи футбольні матчі, організовані на території Республіки Польща у рамках матчів Міжнародної федерації футболу (FIFA) або Союзу європейських футбольних асоціацій (УЄФА), вищезазначені правила не поширюються на іноземних учасників, якщо квиток або інший документ, який дає їм право перебувати на футбольному матчі, вони отримують за межами території Республіки Польща, відповідно до законодавства, що діє в місці видачі квитка [10].

Організатор матчу має право, якщо це необхідно, обговорити з поліцією та іншими службами, які заходи повинні бути прийняті проти продажу під стадіоном квитків сторонніми особами, особливо маючи на увазі, що це може спонукнути до розділення вболівальників на групи. Такими діями можуть бути наприклад, обмеження кількості квитків проданих одній людині. Такі додаткові зобов'язання футбольного клубу вказані в Правилах безпеки [12].

У квитку або в іншому документі, який дає змогу брати участь у футбольному матчі, повинен бути вказаний номер місця. Організатор

футбольного матчу може надати учасникам постійні місця за умови дотримання наступних правил:

1) кількість доступних місць для стояння не може перевищувати 25% від загальної кількості місць на стадіоні, визначеної відповідно до положень будівельного законодавства та правил пожежної охорони;

2) одне місце для сидіння може бути перетворене лише на одне стояче, зберігаючи можливість відновлення попереднього стану;

3) організатор футбольного матчу може забезпечити місця стояння для вболівальників команди приймаючої сторони та гостей у співвідношенні 4:1, гарантуючи, що такі стоячі місця, передбачені для обох груп вболівальників, будуть відокремлені один від одного таким чином, щоб мінімізувати можливість спричинити небезпеку під час футбольного матчу [10].

Вхід на футбольний матч неповнолітнього до 13 років здійснюється лише під опікою дорослої людини, що організатор теж зобов’язаний перевірити.

Організатор також має ряд зобов'язань щодо забезпечення безпеки команди гостей і приїздних вболівальників. Такі обов'язки включають в себе дії, щоб організатор матчу співпрацюючи з Поліцією гарантував безпеку команді гостей та представникам його клубу на стадіоні [12].

Якщо прибуття уболівальників гостей створює загрозу для безпеки, організатор матчу і клуби, які беруть в ньому участь, повинні робити все можливе, щоб запобігти приїзду уболівальників. Якщо очікується більш ніж 500 уболівальників, які збираються на виїздний матч, рекомендується, щоб клуб визначив відповідно кількість представників, які будуть супроводжувати вболівальників під час їх поїздки на матч та з матчу і співпрацювати зі службами безпеки [12].

Організатор матчу повинен забезпечити безпеку гравців, суддів та інших осіб проти вторгнення уболівальників у ігрову зону. Це може бути досягнуто за рахунок використання наступних заходів, в залежності від індивідуальних обставин:

1) наявність представників клубу в безпосередній близькості від ігрового поля,

2) наявність ровів відповідної ширини та глибини,

3) розташування першого ряду сидінь на правильну висоту над ігровим майданчиком, що робить вторгнення неможливим,

4) нездоланний бар'єр або паркан, який може бути встановлений на постійній основі, або бути зйомним, коли його використання не видається необхідним [12].

Організатор матчу разом з керівництвом поліції або керівником служби безпеки повинен запобігати будь-яким діям глядачів провокаційного характеру на стадіоні та в його найближчому оточенні (провокація гравців чи вболівальників виїзної команди через словесні утиски, расистську поведінку, провокаційні прапори чи транспаранти тощо) [6].

Футбольний клуб, який є організатором матчу, додатково зобов'язаний виконати положення додатку № 1 до Правил безпеки, тобто 10 пунктів УЄФА щодо запобігання расизму. Відповідно до положень цього додатку, обов'язки організатора матчу включають:

1) видати заяву про те, що расизм і будь-які інші форми дискримінації не будуть допускатися, і вказати, які заходи будуть прийняті щодо тих, хто пропагандує расистські ідеї. Заява повинна бути надрукована в усіх програмах матчів та розповсюджена на стадіоні,

2) зробити оголошення, засуджуючи расистські гасла під час матчу,

3) вимагати для покупки квитків підписання заяви, що вболівальник не приймає участь в расистських діях,

4) приймати заходи проти поширення контенту расизму на стадіоні і в його оточенні,

5) застосувати дисциплінарні заходи проти гравців, поведінка яких є расистською,

6) контактувати з іншими клубами для підтвердження того, що вони знають політику клубу в відношенні расизму,

7) ввести стратегію боротьби служб безпеки та поліції з расистською поведінкою,

8) видалити зі стадіону всі расистські графіті,

9) здійснювати співробітництво з усіма групами та агенціями, такими як футбольні асоціації, уболівальники, школи, благодійні організації, молодіжні клуби, спонсори, місцеві компанії, поліція та інші організації для розробки програм інформування про кампанії проти расизму та дискримінації [13].

3. Права футбольного клубу як підприємства по забезпеченню безпеки масового заходу - футбольного матчу

З метою забезпечення безпеки футбольного матчу, підприємство, яке його організує, тобто футбольний клуб, має багато правових інструментів.

Наприклад, організатор футбольного матчу вправі відмовити у продажу квитка або іншого документа, що дозволяє бути на заході:

1) особі, проти якої винесено рішення:

а) заборони відвідування масових заходів,

б) про зобов'язання утримуватися від перебування в місцях масових заходів, видане судом проти засудженого у зв'язку з умовним припиненням позбавлення волі або проти неповнолітньої відповідно до положень Закону про неповнолітніх від 26 жовтня 1982 року ;

2) особі, проти якої винесено рішення про так звану заборону клубову (див. нижче);

3) особі, яка обґрунтовано підозрюється, що на місці та під час масового заходу може загрожувати безпеці масового заходу .

Футбольний клуб, організовуючи матч має також право фіксувати хід масового заходу, зокрема поведінку людей, які беруть участь у ньому, використовуючи пристрої для запису відео та звуку. Матеріали, зібрані під час запису масового заходу, які можуть становити докази, що дозволяють порушити кримінальне провадження чи провадження у справах про правопорушення, або докази, які можуть мати значення для такого провадження, організатор негайно пересилає прокурору або поліції, в разі необхідності, разом з заявою про порушення кримінальної справи .

Слід підкреслити, що це право в деяких випадках стає обов'язком. Воєвода провінції за погодженням з керівником поліції та командиром пожежної команди та після консультації з відповідною польською спортивною асоціацією складає перелік стадіонів, споруд чи майданчиків, на яких запис масового заходу із застосуванням відео- та звукозаписуючих пристроїв є обов'язковим .

Організатор масового заходу також зобов'язаний фіксувати хід масового заходу, зокрема поведінку людей, які беруть участь у ньому, використовуючи пристрої для запису відео та звуку, в разі, організації «ризикового» матчу [10].

Організатор футбольного матчу також може використовувати і накладати на осіб так звану клубову заборону. Клубова заборона практикується в Англії давно, а в Польщі вона була введена в 2009 році. Введення клубової заборони переважно отримало позитивні відгуки. На приклад, Річард Муха, директор по безпеці польського футбольного клубу Заглембе Любін, відмітив, що це є перевірена процедура, яка поліпшить безпеку, а в цей момент (тобто до введення клубової заборони, або стадіонної заборони), на його думку, технічні заходи доступні на стадіонах не дозволяють знаходити і запобігати участі тим вболівальникам, яким заборонено відвідувати матчі [14].

Клубова заборона забороняє брати участь у масових заходах, які проводяться організатором футбольного матчу. Вона накладається цим організатором на особу, яка порушила внутрішні правила, що діють на території стадіону, або правила проведення масового заходу. Накладена клубова заборона стосується також наступних масових заходів, що проводяться за участю команди організатора, який цю заборону наклав, поза місцем організаторів. Період дії клубової заборони не може бути більшим за 2 роки з дати видачі .

Конституційний суд Польщі перевірив згідність положень Закону, що дозволяють клубу заборонити вхід на футбольний матч уболівальникам, які порушили внутрішні правила, що діють на території стадіону, або правила проведення масового заходу, тобто застосовувати клубову заборону, з положеннями Конституції Республіки Польща від 2 квітня 1997 року.

Уповноважений з громадянських прав (Омбудсмен) подав заяву, щоб така перевірка була здійснена Конституційним Судом Польщі. Оспорював, що конкретні ситуації, коли організатор може накласти клубову заборону містяться во внутрішніх правилах, а не вказані у законі [15].

Намір Уповноваженого з громадянських прав не був таким, щоб позбавити організаторів матчів можливості зниження частки людей, які порушують громадський спокій і порядок. Ідея полягала в тому, щоб структура заборони клубу відповідала конституційним стандартам і включала процедурні гарантії захисту прав людини. За словами Омбудсмена, заборона клубу вимагає роз'яснення положень в законі, що обмежить самовілля в його застосуванні. Він зазначив, що клубова заборона накладається не судом - як заборона брати участь в масових заходах, - а суб'єктом (футбольним клубом), який не є державним органом. Внутрішні правила не є загальнообов'язковим законом. Але визначають, серед інших, порядок перегляду справи правопорушником (потім він може звернутися до адміністративного суду).

Крім того, закон не визначає, за яку поведінку може бути накладена клубова заборона, а окремі внутрішні правила відрізняються одне від одного .

19 червня 2018 року Конституційний суд визнав, що стаття 14 Закону є відповідною правовою основою для застосування заборони. Конституційний суд визнав цю статтю згідною з ст. 87 Конституції, яка передбачає, що джерелами загальнообов'язкового права є: Конституція, статути, ратифіковані міжнародні угоди та внутрішні правила. Постанова була прийнята одноголосно.

4. Контроль за підприємством щодо виконанням зобов'язань з безпеки

Як і діяльність будь-якого підприємства, футбольний клуб, якщо він організовує футбольний матч, підлягає контролю з точки зору дотримання вимог безпеки щодо організації масового заходу. Важливо, що контроль дотримання вимог безпеки щодо організації масового заходу підвищеного ризику є обов'язковим. Перевірка проводиться органом, який видав дозвіл на проведення масового заходу. Орган може також, хоча це не є обов'язковим, контролювати масовий захід, який не є масовим заходом підвищеного ризику та проводиться згідно з умовами, зазначеними у дозволі на проведення масового заходу.

У зв'язку з проведеним аудитом орган має право:

1) вимагати від організатора інформацію, документи та дані, необхідні для здійснення контролю;

2) мати вільний доступ до місця проведення масових заходів та інших приміщень, безпосередньо пов'язаних із місцем проведення масового заходу;

3) просити від осіб, які діють від імені організатора, надати усну та письмову інформацію [10].

Якщо підчас контролю буде встановлено, що умови, зазначені у дозволі на проведення футбольного матчу, не були виконані, орган видає рішення про заборону проведення масового заходу, якщо після видачі дозволу виявить, що умови безпеки, які спричиняють його видачу, були порушені. Маючи на увазі ризик порушення безпеки у випадку припинення масового заходу, орган може також прийняти рішення про негайне припинення масового заходу. Таке рішення може бути винесено воєводою в якості адміністративного рішення, якщо подальший хід матчу може загрожувати життю чи здоров'ю людей чи майну значних розмірів, а дії, які вживає організатор, є недостатніми для забезпечення громадської безпеки та порядку [11].

У разі негативної оцінки стану безпеки та громадського порядку у зв'язку із запланованим або проведеним масовим заходом, воєвода за допомогою адміністративного рішення може:

1) забороняти проведення масових заходів за участю громадськості на всьому об'єкті або в окремих його секторах;

2) запровадити на визначений чи невизначений термін заборону на проведення масових заходів у воєводстві чи його частині [12].

5. Відповідальність футбольного клубу, як підприємства, яке організовує футбольний матч

Футбольний клуб, який організовує масовий захід також несе цивільну відповідальність за шкоду, заподіяну в зв'язку з охороною масових заходів і кримінальну за невиконання своїх зобов'язань щодо забезпечення безпеки.

Цивільно-правову відповідальність несе лише організатор масового заходу, участь у якому є платна, за збитки, пов'язані з еквівалентом знищеного або пошкодженого майна поліції, військової поліції, Державної пожежної служби та іншими підрозділами пожежної охорони та службами охорони здоров'я у зв'язку з їх діяннями на місці та під час проведення масового заходу. Тому положеннями Закону передбачено, що організатор масового заходу,

участь в якому підлягає сплаті, зобов'язаний укласти договір страхування цивільної відповідальності за шкоду, заподіяну особам, які беруть участь у ньому [4].

Кримінальну відповідальність в основному несуть ті, хто організовують масовий захід без необхідного дозволу або всупереч умовам, викладеним у дозволі, або проводять його проти виданої заборони його проведення. У цьому випадку застосовується штраф у розмірі не менше 240 щоденних ставок, обмеження волі або позбавлення волі від 6 місяців до 8 років (що не виключає відповідальність організатора масового заходу за вчинення інших злочинів або правопорушень, перелічених в Кримінальному кодексі) [12].

Дуже широкий перелік штрафних санкцій також випливає з Дисциплінарних правил.

За відсутність належного порядку чи безпеки на стадіоні до, під час або після матчу, клуб може бути покараний:

1) штрафом,

2) рішенням переграти матч,

3) грати матч без вболівальників,

4) забороною грати певний час або певну кількість матчів за участю глядачів на частині або на всьому спортивному об'єкті в місцевості, яка є місцем розташування клубу,

5) забороною поїздки організованих груп вболівальників на футбольні матчі,

6) проведенням матчу на нейтральному стадіоні,

7) забороною грати матч на певному стадіоні,

8) забороною грати визначений час або певну кількість матчів на стадіоні, що є місцем розташування клубу,

9) втриманням дії і позбавленням ліцензії [13].

Більшість цих штрафних санкцій, за винятком рішення переграти матч, також можуть бути накладені на клуб за невиконання зобов’язань, встановлених правилами безпеки на футбольних майданчиках, навіть якщо

жодного порушення порядку чи безпеки не сталося до, під час змагань або після них. Йдеться про так звану загальну та специфічну профілактику, тобто вплив покарання на навколишнє середовище та на суб'єкт, на який воно було накладено.

Спортивний клуб та його вболівальники несуть відповідальність не лише за відсутність порядку чи безпеки на стадіоні, а й під час виїзду організованої групи вболівальників. За відсутності порядку чи безпеки під час поїздки організованої групи прихильників на футбольний матч клуб, який відвідує, та група, карається забороною виїзду організованих груп прихильників на футбольні матчі [13].

У разі невиконання зобов'язання щодо забезпечення порядку чи безпеки на стадіоні відповідальними фізичними особами до, під час змагань або після них дисциплінарний орган накладає дисциплінарну кару у вигляді:

1) застереження,

2) нагани,

3) штрафу від 500 злотих,

4) тимчасової дискваліфікації від 1 місяця до 2 років [13].

Дисциплінарний статут також містить сурову (кваліфіковану) форму цього злочину, коли в результаті невиконання зобов'язання щодо забезпечення порядку чи безпеки на стадіоні мало місце серйозне порушення порядку та безпеки на стадіоні до, під час і після матчу. У такому випадку не можна застосовувати застереження, а найнижча фінансова санкція не може бути нижчою 5000 злотих. Також в такому випадку дискваліфікація повинна бути накладена на строк не менше 3 місяців. Останнє покарання в цьому переліку - заборона на участь в будь-якій діяльності, пов'язаною з футболом.

Спеціальні правила щодо штрафних санкцій супроводжують застосування правил щодо порушень безпеки та порядку у футбольних спорудах. Згідно з першим із них, всі покарання за відсутність належного забезпечення порядку на стадіоні, крім рішення переграти матч та

фінансових штрафних санкцій, підлягають негайному виконанню, якщо дисциплінарний орган не вирішить інше.

У разі, якщо порушення є результатом поведінки осіб, відповідальність за яких несе футбольний клуб-гість, карається цей клуб.

Важливою є встановлена в Правилах дисциплінарних так звана презумпція уболівальників сектора клубу-гість, яка полягає в тому, що приймається - уболівальники які знаходяться в секторі стадіону, який є призначеним для шанувальників клубу відвідувача, є уболівальниками цього клубу. Якщо вболівальники, які вчинили вищенаведені правопорушення, не можуть бути визначені, то буде покараний клуб, який організовує матч [13].

Висновок. Вищевикладене наочно підтверджує, що діяльність підприємства у формі футбольного клубу пов’язана не тільки з численними привілеями, але і з великою кількістю обов'язків забезпечення безпеки в організації заходу, яким є футбольний матч. Такі обов’язки є набагато суворими, ніж ті, які стосуються інших підприємств, що організовують інші масові заходи. Тому організатори футбольних матчів часто вказують інформацію, що конкретний матч не є масовим заходом і для продажу уболівальникам виділяється тільки 999 вхідних квитків. Але слід зазначити, що невиконання зобов’язань, встановлених правилами безпеки на футбольних майданчиках тягне за собою дуже серйозні наслідки, як фінансові, так і пов'язані з кримінальною відповідальністю, які можуть зруйнувати діяльність підприємства, футбольного клубу, - припинити, чи принаймні значно перешкодити в діяльності цього підприємства.

5.6. Організація безпеки діяльності польського підприємства шляхом контролю службової електронної пошти

У сучасний час майже кожне підприємство створює або наказує створити своїм працівникам так звану службову електронну пошту, як правило це - поштова скринька, пов’язана з доменом підприємства, яка здатна, в першу

чергу, допомогти ідентифікації співробітників з компанією в відносинах з іншими підприємцями. Ця електронна адреса, на жаль, може бути використана не тільки для того, щоб працівник виконував обов'язки в рамках контракту з підприємством, але може бути застосована для інших цілей - приватних, що може привести до негативних наслідків для підприємства. Щоб уникнути ситуації, в якій працівник використовує службову електронну пошту та може завдати шкоди репутації компанії, роботодавець повинен мати інструменти, які дозволяють йому перевіряти, з якою метою працівник використовує свою службову електронну пошту. Це необхідно зробити так, щоб право на приватне життя і таємницю кореспонденції працівника не було порушено. Принцип пропорційності повинен характеризувати дії підприємства при прийнятті будь - яких важливих рішень, і зокрема цей принцип має важливе значення, якщо заради безпеки компанії, роботодавець поставить на меті перевірити кореспонденцію співробітника. Якщо не вживати таких заходів підприємство може отримати як фінансові збитки так і негативні наслідки в області його безпеки.

Контроль службової електронної пошти працівників підприємства. Відповідно до польського законодавства, роботодавець має право перевіряти кореспонденцію, що надсилають його працівники, які використовують службову електронну пошту. Оскільки працівник веде кореспонденцію саме від імені роботодавця - тому природно, що роботодавець має право знати її зміст.

Тому контроль службової електронної пошти працівників підприємства є правом підприємця як роботодавця. Це можливо відповідно до ст. 223 частина 1 Трудового кодексу Республіки Польща, згідно якого – в разі необхідності забезпечити організацію роботи, що забезпечує повноцінне використання робочого часу та належне використання інструментів праці, наданих працівникові, роботодавець може запровадити контроль за службовою електронною поштою працівника (моніторинг електронної пошти) [16].

Отже, контроль ділової електронної пошти є можливий, але він повинен мати чітко визначену мету, яка полягає в тому, щоб прагнути до повної ефективності роботи працівників і перевірити, чи використовують вони інструменти, надані їм роботодавцем [17].

Положення, що дає підприємцю право контролювати службову електронну пошту працівників, було внесено до Трудового кодексу Республіки Польща.

Раніше не було норм, які б давали право роботодавцю контролювати кореспонденцію працівників, і це питання викликало значні контраверсії. Моніторинг електронної пошти був однією з найбільш суперечливих форм моніторингу. Це пов’язано з тим, що таємниця кореспонденції захищена польською конституцією особливим чином. Відповідно до ст. 49 Конституції Республіки Польща гарантується свобода та захист таємниці кореспонденції, а її обмеження може відбуватися лише у випадках, визначених Законом, та у спосіб, визначений ним. Тому законодавець надає особливого значення таємниці кореспонденції. Слід зауважити, що реалізація конституційних прав і свобод може бути обмежена, якщо це необхідно в демократичній державі для її безпеки чи громадського порядку, охорони навколишнього середовища, охорони здоров'я та моралі чи свобод та прав інших осіб, за умови, що ці обмеження не порушують сутність цих свобод та прав (стаття 31 частина 3 Конституції Республіки Польща). Таким чином обмеження свободи таємниці кореспонденції має бути *expressis verbis* визначено в Законі. Законодавець повинен безпосередньо визначити необхідність обмеження свободи таємниці кореспонденції, вказавши обставини та спосіб цього обмеження. Тільки тоді порушення права таємниці кореспонденції вважатиметься допустимим [18].

Суперечливим питанням було насамперед моніторинг службової електронної пошти. Не було жодних принципових сумнівів щодо того, що особиста кореспонденція працівника - територія виключена із сфери контролю роботодавців [19].

З іншого боку, стосовно службової кореспонденції, було важко визначити обсяг таємниці кореспонденції, зокрема вирішити, хто крім осіб, які беруть участь у спілкуванні, уповноважені контролювати цю кореспонденцію. Вказано, що оскільки працівник здійснює спілкування від імені та на користь роботодавця, то роботодавця слід трактуватись як особу, яка уповноважена на доступ до такої кореспонденції [19]. З іншого боку, сфера таємниці кореспонденції охоплює лише учасників спілкування, тобто працівника та його співрозмовника. Це важливо, оскільки таємницю кореспонденції також забезпечує кримінально-правовове законодавство. Відповідно до ст. 267 п. 1 Кримінального кодексу Республіки Польщі злочин проти таємниці інформації вчиняється тими, хто без дозволу отримує доступ до інформації, не призначеної для нього, шляхом відкриття закритого листа, підключення до телекомунікаційної мережі або електронної пошти [20]. Кримінальна відповідальність поширюється також на тих, хто незаконно отримує доступ до всієї або частини ІТ-системи (пункт 2 статті 267 Кримінального кодексу Республіки Польща), а також до тих, хто приймає або використовує прослуховуючи пристрої, візуальний пристрій чи інші пристрої, або програмне забезпечення для отримання інформації, до якої він не має права доступу (пункт 3 статті 267 Кримінального кодексу) [21].

Тому вирішення зазначеної дилеми, безумовно, вимагало втручання законодавця. Йому довелося внести зміни, щоб підприємство не піддавалося кримінальній відповідальності за дії, спрямовані на створення умов для його безпечного функціонування та перевірки діяльності осіб працюючих на цьому підприємстві [19].

Неприпустимість відсутності правових підстав для перевірки електронної пошти працівника підтверджує досвід законодавства інших країн. Наприклад, Британський закон прямо передбачає винятки із заборони підслуховування роботодавцем телефонної розмови працівника та читання його електронних листів (без згоди відправника та одержувача повідомлення). Роботодавець має право контролювати та фіксувати повідомлення в певних

обставинах, у тому числі для забезпечення того, щоб працівники відповідали стандартам підприємства, запобігали чи виявляли злочин, розслідували чи виявляли несанкціоноване використання телекомунікаційної системи або забезпечували безпеку системи або її ефективне функціонування [22]. У свою чергу, Фінський закон про захист конфіденційності в професійному житті регулює правила контролю роботодавцем електронної пошти працівника, а саме відновлення та відкриття повідомлень, що надсилаються на електронну адресу працівника підприємства та повідомлення, надіслані працівником з цієї адреси [23].

Отже, не викликає сумнівів, що доступ роботодавця до кореспонденції, що надсилається працівником від імені роботодавця, був спірним, незважаючи на службовий характер цього повідомлення та факт, що це повідомлення здійснюється за допомогою інструментів, наданих працівником роботодавцем [18].

Тому необхідно позитивно оцінити встановлення положення, яке уповноважує роботодавця відповідно до права контролювати службову електронну пошту працівника. Вони легітимізують підприємство дбати про його безпеку також у сфері діяльності, яку здійснюють його працівники [19].

Обмеження контролю електронної пошти працівників підприємства. Дозволяючи контролювати електронну пошту працівника, законодавець посилається на правило пропорційності. Зважаючи на вищезазначене регулювання, роботодавець може ввести контроль за службовою електронною поштою працівника, якщо це необхідно для організації роботи, що забезпечує повноцінне використання робочого часу та належне використання інструментів праці, наданих працівникові. Вибираючи умови для підпорядкування працівника контролю в цьому відношенні, було зазначено два завдання щодо організації праці, які дозволяють повноцінно використовувати робочий час працівниками та належним чином використовувати службові інструменти службовцями. Законодавець використовує в даному випадку сполучення "та", тобто підкреслює зв'язок

вищезазначених цілей контрольної діяльності роботодавця. Як результат, це означає, що відповідні умови повинні дотримуватися одночасно [19].

Отже, моніторинг офіційної електронної пошти працівника є допустимим, якщо це необхідно для забезпечення як належної організації роботи (що дозволяє повною мірою використовувати робочий час), так і належного використання інструментів праці, наданих працівникові.

Ці умови не завжди поєднуються. Працівник може використовувати службові інструменти таким чином, що не відповідає їх призначенню але використовуючи робочий час (наприклад, коли це відбувається під час перерви на роботі). Проте слід зазначити, що необхідність дотримання обох вимог, зазначених у коментованому положенні, підвищує рівень захисту працівників від здійснення роботодавцем надмірного контролю, хоча це також може бути джерелом зловживань, вчинених працівником [19].

У розглянутих джерелах наголошується, що при контролі службової електронної пошти працівника, роботодавець повинен керуватися такими принципами:

а) принцип необхідності;

б) принцип захисту гідності та особистих прав працівника;

в) принцип свободи та незалежності профспілок.

Згідно з принципом необхідності, моніторинг електронної пошти працівника допустим, коли це необхідно для забезпечення такої організації роботи, що дозволяє в повній мірі використовувати робочий час і робочі інструменти, доступні співробітникам (повинні бути виконані спільно) [24].

Під критерієм необхідності слід розуміти те, що роботодавець зобов'язаний вказати, що вищезазначені цілі не можуть бути досягнуті інакше, як лише шляхом обраної форми моніторингу працівників. Обставини, що мають значення для цієї оцінки, - це вид роботи, її характер та посада, яку займає працівник.

Принцип необхідності додатково обмежується принципом захисту гідності та особистих прав працівника. Використання моніторингу

відповідності допускається, але таким чином, щоб не порушувати особисту власність працівника, в тому числі таємниці кореспонденції (ст. 223 § 2 і 4 Трудового кодексу Республіки Польща).

Згідно з принципом свободи та незалежності профспілок підкреслюється, що моніторинг без будь-яких винятків не може не включати кімнати (за аналогією - електронної адреси), які використовується профспілковою організацією.

Крім того, з ст. 222 § 6-10 та ст. 223 § 4 Трудового кодексу Республіки Польща видно, що будь-яка форма моніторингу працівників є законною, якщо вона була здійснена у порядку, зазначеному в ньому.

Ці принципи відповідають вимогам принципу прозорості обробки персональних даних [19].

Елементами цього принципу є такі вимоги:

а) цілі, обсяг та спосіб застосування моніторингу визначені в колективному трудовому договорі чи нормативно-правових актах з праці або в повідомленні, якщо роботодавець не укладає колективні трудові договори (частина 6 статті 222 Трудового кодексу Республіки Польща);

б) роботодавець інформує працівників про здійснення моніторингу у спосіб, прийнятий роботодавцем, не пізніше ніж за 2 тижні до його початку (частина 7 статті 222 Трудового кодексу Республіки Польща);

с) роботодавець, перш ніж дозволити працівникові працювати, надає йому письмову інформацію про цілі, обсяг та спосіб використання моніторингу (частина 8 статті 222 Трудового кодексу Республіки Польща) [24].

Зобов'язання підприємства щодо контролю службової пошти своїх працівників. Щоб поважати особисті права працівника контролюючи їх кореспонденцію принципове значення має дотримання принципу прозорості. Працівник повинен бути повідомлений про моніторинг роботодавцем службової електронної пошти працівника. Працівник, який не був проінформований роботодавцем про моніторинг службової пошти, має

законне підстави сподіватися, що його приватне життя і комунікація захищені [17].

При введенні цієї форми контролю роботодавець зобов'язаний інформувати працівників в порядку, прийнятому у даного роботодавця за 2 тижні до початку перевірки (ст. 22 § 7 в поєднанні з ст. 22 § 3 Трудового кодексу Республіки Польща). При прийнятті на роботу нового працівника підприємство повинно надати йому письмову інформацію про цілі, обсяги та способи моніторингу пошти, перш ніж дозволити йому виконувати роботу (ст. 22 § 8 в поєднанні з ст. 22 § 3 Трудового кодексу Республіки Польща). Крім того роботодавець повинен ввести відповідні позначення на поштових скриньках працівників, чітко вказуючи, що електронна пошта контролюється підприємством. Позначення комп'ютера чи іншого пристрою, які використовується для електронної пошти, не видається достатнім, якщо з цього позначення не слідує, що електронна пошта також контролюється [24].

Також відповідно до ст. 222 § 6 у зв'язку з ст. 223 § 3 Трудового кодексу Республіки Польща: цілі, обсяг та спосіб застосування вищезазначеної форми моніторингу повинні бути вказані в колективному трудовому договорі чи нормативно-правових актах з праці або в повідомленні, якщо роботодавець не охоплюється колективним трудовим договором або не зобов'язаний встановлювати правила праці. Тому роботодавець повинен визначити цілі моніторингу, точно вказавши обсяг здійснення контрольної діяльності в обговорюваній області. Крім того, слід визначити масштаб моніторингу і, таким чином, визначити, які дані будуть збиратися в результаті його використання. Обсяг даних повинен відповідати цілі моніторингу. Тому, якщо достатньо отримати інформацію про відправників та одержувачів зв'язку, а також дату та час надсилання та отримання повідомлень, а також тему повідомлення, підприємство не повинно аналізувати зміст кореспонденції. Проте працівника необхідно попередити, який конкретний обсяг даних буде збиратися в рамках контрольної діяльності. Предметом домовленостей також повинен бути спосіб використання моніторингу, а отже, визначення засобів

здійснення контролю електронної пошти та правил їх використання. Зокрема, слід визначати обставини та періодичність проведення контролю [24].

Контроль службової електронної пошти працівників підприємства та таємниця кореспонденції. Відповідно до ст. 22 § 2 Трудового кодексу моніторинг електронної пошти не може порушувати таємницю кореспонденції і право на приватність життя [16].

Відповідно рішення Європейського суду - таємниця кореспонденції охоплює всі засоби спілкування, хоча термін "кореспонденція" асоціюється із спілкуванням через листи. Аналогічну точку зору висловлює Європейський суд з прав людини, вказуючи, шо термін "кореспонденція" застосовується також до спілкування за допомогою електронних засобів зв'язку, наприклад, електронної пошти [25].

Безперечно, право працівників до таємниці кореспонденції може бути порушеним внаслідок використання електронної пошти для моніторингу. Хоча право дозволяє контролювати лише службові повідомлення, існує ризик навіть випадково знайти приватні повідомлення в службовій поштовій скриньці працівника.

Як підкреслюється в дослідженнях, навіть якщо роботодавець забороняє використовувати службову пошту в приватних цілях і наштовхується на приватну кореспонденцію працівника, який не виконав цієї заборони, він не може прочитати її повністю [19].

Тому закон, який забороняє порушити таємницю кореспонденції вважається цілком виправданим, що показано в юридичній літературі. З точки зору бізнесу, таке обмеження потенційно піддає підприємцю ризику понесення відповідальності за заходи, вжиті для забезпечення безпеки компанії. Щоб уникнути ненавмисного входу в приватний простір працівника, пропонується ввести відповідні визначення приватних повідомлень працівника. Однак видається, що заборона використовувати офіційну пошту в приватних цілях є менш клопітким заходом [25].

Контроль службової електронної пошти працівників підприємства та таємниці кореспонденції й право на повагу до приватного життя. Розглянемо моніторинг роботи працівника та втручання в їхнє право на повагу до приватного життя. Використання положень Закону, що дозволяють це робити, повинно здійснюватися з урахуванням необхідності збалансувати ці суперечливі цінності та інтереси обох сторін трудових відносин, що означає, що моніторинг як вид контролю роботодавця з боку роботодавця повинен враховувати потребу поважати особисті права працівників, включаючи право на приватне життя. У зв'язку з цим стандарти, встановлені прецедентною практикою Європейського суду з прав людини за ст. 8 Конвенції про захист прав людини і основоположних свобод, що є гарантією вищезазначеного права на повагу до приватного життя (зокрема, судові рішення від 9.01.2018 р., 1874/13 та 8567/13, Лопес Рібальда та інші проти Іспанії, LEX № 2418052 від 11.28.2017 р., 70838/13 Antović і Mirković проти Чорногорії; LEX №2398411; рішення Великої палати 05.09.2017 р., 61496/08 Bărbulescu проти Румунії, LEX №2347233; 03.04.2007 р., 62617/00 Copland проти Великобританії, LEX № 527588 від 2 серпня 1984 р., 8691/79 Malone проти Великобританії, LEX № 80974) [19].

У цьому контексті особливої уваги заслуговує рішення у справі "Барбулеску проти Румунії" (рішення Великої палати від 5 вересня 2017 року, заява № 61496/08).

На прохання свого роботодавця Богдан Барбулеску, громадянин Румунії, створив обліковий запис у загальнодоступному месенджері, який повинен був використовуватися для зв'язку зі своїми клієнтами. Під час моніторингу змісту повідомлень, надісланих Барбулеску, його роботодавець виявив, що месенджер також використовується для приватних контактів працівника. Роботодавець розірвав трудовий договір з паном Барбулеску. Працівник звинуватив роботодавця у необґрунтованому звільненні та надмірному втручанні у приватне життя, а потім передав справу до суду. Суд погодився с підприємством. У 2008 році Богдан Барбулеску передав справу до

Європейського суду з прав людини, вказавши на порушення ст. 8 Конвенції про захист прав людини і основоположних свобод. Ця стаття стосується права на повагу до сімейного життя, дому та кореспонденції [26].

Європейський суд з прав людини відзначив, що кореспонденція заявника на роботі охоплюється поняттями "приватне життя" та "кореспонденція" і тому ст. 8 Конвенції має застосовуватися.

Суд вважав, що її потенційне порушення потрібно розглядати з точки зору позитивних зобов'язань держави. Що стосується сфери трудового права, то слід було оцінити, чи вимагається в цьому випадку від держави створити правову базу для захисту права заявника на повагу до свого приватного життя та кореспонденції в контексті його професійних стосунків з підприємством-роботодавцем. Трудове законодавство має специфічні особливості, які потребують розгляду. Відносини роботодавець - працівник є договірними, включають специфічні права та обов'язки обох сторін, які суттєво відрізняються від загальноприйнятих у відносинах між особами. З нормативно-правової точки зору, законодавство про працю залишає місце для переговорів між сторонами трудового договору. Отже, загалом, самі сторони визначають значну частку своїх відносин [27].

Суд зазначив, що свобода регулювання відносин у цій сфері не може бути необмеженою. Національні органи влади повинні забезпечити, щоб впровадження роботодавцем заходів моніторингу листування та інших засобів комунікації, незалежно від їх обсягу та тривалості, супроводжувалось адекватними та достатніми гарантіями проти зловживань.

Суд вказав, що у цьому контексті слід враховувати такі важливі фактори:

- чи було повідомлено працівника про можливість роботодавця контролювати кореспонденцію та здійснення моніторингу. Хоча в практиці працівники можуть бути повідомлені різними способами залежно від обставин справи. Суд вважає, що впровадження таких заходів, які відповідають вимогам ст. 8 Конвенції, як правило, вимагає, щоб повідомлення чітко вказувало характер моніторингу та було дано працівникові до його проведення;

- обсяг моніторингу та ступінь втручання в приватне життя працівників. У зв'язку з цим слід розрізняти моніторинг потоку кореспонденції та її зміст. Слід також врахувати, чи контролювалася вся кореспонденція, а також, чи моніторинг був обмежений у часі та скільки людей мали доступ до його результатів;

- чи представило підприємство обґрунтовані причини, які виправдовують моніторинг кореспонденції та дізнання її фактичного змісту. У ситуації, коли моніторинг кореспонденції за своєю суттю є явно більш інвазійним методом, він потребує більш серйозного обґрунтування;

- чи можна було створити систему моніторингу на основі методів та заходів, які є менш суворими, ніж прямий доступ до вмісту кореспонденції працівників. Необхідно, з огляду на особливі обставини, оцінити, чи можна досягти мети підприємства без прямого доступу до повного змісту кореспонденції працівника;

- наслідки моніторингу для працівника та спосіб використання підприємством результатів моніторингу, зокрема, чи він слугував для досягнення його заявленої мети;

- чи використовував працівник відповідні гарантії, особливо коли моніторинг з боку роботодавця був суворим. Зокрема, він повинен перешкоджати доступу до фактичного змісту кореспонденції, про який йде мова, за винятком випадків, коли працівник раніше не був повідомлений про застосування моніторингу [27].

Влада повинна забезпечити, щоб працівник, кореспонденцію якого було відстежено, отримав доступ до суду, який має юрисдикцію перевірити, принаймні, наскільки виконуються вказані вище критерії.

Європейський суд з прав людини повинен вже оцінити спосіб, яким національні суди, в які подавав звернення заявник, розглядали його твердження про порушення роботодавцем права на повагу до приватного життя та кореспонденції [27].

У цій справі румунські суди звернули увагу лише на те, чи роботодавець розкрив зміст листування колегам заявника. Суд зазначив, що цей аргумент недостатньо обґрунтований у матеріалах справи та що заявник не надав жодних інших доказів. Тому вони вважали, що звинувачення стосувалося звільнення заявника з роботи за результатами моніторингу, що проводився роботодавцем.

Європейський суд з прав людини вказав, що в цьому випадку необхідно було, щоб суд Румунії більш конкретно відповів, чи підприємство використовувало моніторинг відповідно до вимог статті 8 Конвенції, а право заявника на повагу до свого приватного життя та кореспонденції не було порушено.

Таким чином, завдання Європейський суду з прав людини полягає в тому, щоб встановити, чи, зважаючи на всі обставини, компетентні органи – суди мають хороший баланс конкуруючих інтересів у випадку, якщо моніторинг застосовується до заявника. Він визнав, що роботодавець має законний інтерес до ефективної роботи компанії, що може бути здійснено за допомогою механізму перевірки, чи виконують працівники свої професійні обов'язки належним чином і з необхідною ретельністю [27].

З цієї причини Суд вирішив спочатку перевірити, як національні суди у цій справі встановили відповідні факти. Вивчаючи цю справу, Суд повинен був визначити, чи національні суди діяли відповідно до вимог Конвенції.

Суд нагадав, що стосовно фактичних висновків він усвідомлював допоміжний характер свого завдання та його зобов'язання проявляти обережність, приймаючи на себе роль фактичного суду, якщо це не є неминучим. Суд не може замінити оцінку фактів, викладених національними судами, оскільки вони повинні встановлювати факти на підставі поданих доказів. Але оцінюючи справу Суд не зв'язаний висновками національних судів і може вільно оцінювати їх з огляду на всі представлені матеріали, але потрібні переконливі доводи, щоб Суд відходив від фактичних висновків, зроблених національними судами [27].

Надані до Суду докази свідчать про те, що заявник був поінформований роботодавцем про внутрішні положення, які забороняють використовувати ресурси компанії в особистих цілях. Він підтвердив, що прочитав відповідний документ і підписав копію 20 грудня 2006 року. Крім того, роботодавець надіслав повідомлення від 26 червня 2007 року всім працівникам нагадуючи, що використання ресурсів компанії в особистих цілях заборонено, а одного працівника було звільнено за порушення цієї заборони. Заявник прочитав повідомлення та підписав його копію в невстановлену дату між 3 та 13 липнєм 2007 року. Суд також зазначив, що 13 липня 2007 року роботодавець двічі закликав його роз'яснити питання використання службової пошти в особистих цілях. Спочатку, коли роботодавець показав йому список його кореспонденції, працівник заявив, що використовує обліковий запис Yahoo Messenger лише у зв'язку з роботою. Потім, коли роботодавець показав йому через п'ятнадцять хвилин 45-сторінкову кореспонденцію з братом та нареченою, працівник звинуватив роботодавця у злочині у порушенні конфіденційності кореспонденції [26].

На думку Суду, національні суди правильно визначили зацікавлені сторони у спорі - чітко вказавши право заявника на повагу до приватного життя, а також застосовані правові принципи. Зокрема, апеляційний суд прямо посилався на принципи необхідності, мети, прозорості, пропорційності та безпеки, та наголосив, що моніторинг кореспонденції підпадає під ці принципи. Суди також вивчали, чи проводилось дисциплінарне провадження в змагальних умовах та чи може заявник подавати свої доводи.

Залишається визначити, як національні суди враховували у своїх обґрунтуваннях вищезазначені критерії під час зважування права заявника на повагу його приватного життя та кореспонденції проти права роботодавця здійснювати контроль, включаючи його дисциплінарні права, з метою забезпечення ефективного функціонування компанії.

Що стосується питання про те, чи був заявник попередньо повідомлений роботодавцем, Суд зазначив, що він раніше заявляв, що він, здавалося, не був

попередньо інформований про ступінь і тип моніторингу з боку роботодавця, або що роботодавець міг мати доступ до фактичного змісту його кореспонденції. У зв'язку з можливістю здійснення моніторингу Суд зазначив, що національний суд просто зауважив, що "працівники помітили - незадовго до покарання заявника було звільнено іншого працівника", і постановили, що заявника попередили, що він не повинен використовувати ресурси компанії в особистих цілях. Національні суди не визначили, чи був заявник раніше поінформований про можливість роботодавця запровадити моніторинг, а також про його сферу та характер. Суд вважає, що для того, щоб це було розглянуто як попереднє повідомлення, попередження роботодавця повинно бути зроблене до моніторингу, особливо коли воно охоплювало також доступ до кореспонденції працівників. Міжнародні та європейські стандарти рухаються в цьому напрямку, вимагаючи проінформувати суб'єкта перед застосуванням моніторингу.

У зв'язку з питанням обсягу та ступеня вторгнення в приватне життя заявника Суд зазначив, що це питання не було розглянуто судом, хоча роботодавець, здавалося, реєстрував всю кореспонденцію заявника протягом періоду моніторингу, мав доступ до неї та скопіював її зміст [26].

Також здається, що суди не достатньо оцінили законні причини, що виправдовують моніторинг кореспонденції заявника. Не вказано конкретної мети, яка могла б виправдати такий суворий моніторинг, вказано тільки на необхідність подбати про те, щоб ІТ-системи компанії не були пошкоджені, про її відповідальність у разі незаконної діяльності в кіберпросторі та розкриття комерційної таємниці компанії. Однак, на думку Суду, ці приклади можна розглядати лише як теоретичні, оскільки ніщо не свідчить про те, що заявник фактично піддав компанію такому виду ризику [26].

Крім того, національні суди недостатньо вивчили, чи можна досягти мети, яку переслідує роботодавець, способами, менш обтяжливими, ніж доступ до фактичного змісту кореспонденції заявника. Крім того, жоден із судів не розглядав значення наслідків моніторингу та подальших

дисциплінарних проваджень. Суд зазначив, що заявнику було призначено найсуворіше покарання, а саме звільнення [26].

Суди не встановили, чи роботодавець, коли він закликав заявника пояснити використання ресурсів компанії, насправді мав доступ до вмісту переписки. Суди не визначили, коли в дисциплінарному провадженні роботодавець дійшов до змісту кореспонденції. Прийняття можливості доступу до вмісту кореспонденції на будь-якій стадії дисциплінарного провадження суперечило принципу прозорості. З цих причин висновок національних судів про збереження правильного балансу інтересів був спірним. Таке твердження, здається, є вираженням чисто формального та теоретичного підходу. Національні суди не пояснили, зважаючи на обставини, конкретних причин стосовно заявника та його роботодавця, які привели його до такого висновку.

Отже, видається, що суди не змогли встановити, чи заявник був попередньо повідомлений роботодавцем про можливість контролю за його кореспонденцією Yahoo Messenger; вони також не враховували, що він не був поінформований про ступінь вторгнення в його особисте життя та таємницю кореспонденції. Крім того, вони не встановили конкретних причин, що виправдовували моніторинг; чи міг роботодавець застосувати засоби, які менше обмежують вторгнення в приватне життя та кореспонденцію заявника, та чи можливий був доступ до кореспонденції заявника без його відома.

З усіх цих причин, і незважаючи на свободу оцінювання фактів національними судами, Суд вважав, що заявнику не забезпечено належного захисту його права на повагу до приватного життя та кореспонденції, і, як наслідок, не встановила правильного балансу між інтересами сторін. Тому було порушено ст. 8 Конвенції [27].

Санкції за порушення конфіденційності кореспонденції та права на повагу до приватного життя. Через характер блага, яке може бути порушено, тобто права на приватність та конфіденційність листування, багато польських законів передбачають санкції за порушення.

Санкції за порушення положень про санкціонований моніторинг працівника, процедур моніторингу та інших вимог щодо обробки персональних даних працівника, вказані насамперед в положеннях Закону про захист персональних даних з 2018 року [19].

Крім того, якщо працівник виявить порушення своїх особистих прав або зазнає шкоди в цьому відношенні, він може вимагати захисту на підставі положень Цивільного кодексу Республіки Польща [16].

Загалом, працівник також зможе скористатися правом негайно припинити трудові відносини через серйозне порушення роботодавцем основних зобов'язань перед працівником відповідно до ст. 55 частина 1 Трудового кодексу Республіки Польща [19].

Як уже згадувалося вище, порушення таємниці листування може навіть призвести до кримінальної відповідальності, а також до порушення Конвенції про захист прав людини і основоположних свобод. Однак у випадку порушення підприємством положень Конвенції, стороною яка несе відповідальність перед працівником в справі розглянутій Європейським судом з прав людини, буде не підприємець, а держава.

5.7. Функції Організації з безпеки і співпраці в Європі та місія США

Концепція національної безпеки як філософії досягнення стійкого стану держави, пов'язана з подіями, які називали в історії як Вестфальський мир, в ході яких концепція суверенної держави стала основою нових міжнародних відносин між державами.

Найбільш ранні згадки про концепцію національної безпеки відносяться до 1790 року і були зроблені в Єльському університеті. Історично поняття національна безпека включало в себе політичну, військову та економічну сфери.

В США у 1934 році був створений перший Комітет з економічної безпеки, основною метою функціонування якого була стабілізація соціальної

обстановки в державі. В 1947 році Концепція національної безпеки стала офіційним основоположним принципом міжнародної політики в Сполучених Штатах. В цей час (26 липня 1947 року) президентом Гаррі Труманом був підписаний Акт про Національну безпеку . Білл Клінтон під час знаходження на посту президента Сполучених Штатів, створив Національний економічний комітет для розробки та проведення заходів з підтримки національної економічної безпеки.

Дещо інша ситуація з економічною безпекою склалася в Європейському Союзі. Термін економічна безпека має два значення в європейському союзі. Перше значення відноситься до позиції Європейського союзу в світовій економічній системі. На офіційному сайті Європейського союзу зібрані різні посилання на ресурси, пов'язані з економічними цілями Європейського союзу і їх інтерпретації терміна економічна безпека. Європейський союз наголошує на важливості європейської інтеграції в конкурентному процесі глобалізації світової економіки. Держави Європи історично мають меншу кількість ресурсів і працездатного населення порівняно з іншими розвиненими країнами, такими як, наприклад, Сполучені штати Америки.

Найбільшою офіційною організацією, що займається комплексними питаннями безпеки в Європі є ОБСЄ (Організація з безпеки і співробітництва в Європі). Вона об'єднує 56 країн, розташованих в Північній Америці, Європі та Центральній Азії. «Нараду з безпеки і співробітництва в Європі» було скликано з ініціативи СРСР і соціалістичних держав Європи як постійно діючий міжнародний форум представників 33 європейських держав, а також США і Канади для вироблення заходів зменшення військового протистояння і зміцнення безпеки в Європі. Нарада проводилася в три етапи- з 1973 по 1975 роки і завершилася підписанням Заключного акта Наради з безпеки і співробітництва в Європіб (Гельсінські угоди).

В період з 1977 по 2010 роки проводилося ще ряд зустрічей в результаті яких були підписані основні історичні документи, такі як:

- Паризька хартія для нової Європи (проголосила закінчення холодної війни);
- укладений Договір про звичайні збройні сили в Європі (ДЗЗСЄ);
- прийнята спільна декларація 22 держав (членів НАТО і ОВД);
- Хартія європейської безпеки;
- угоду про адаптацію ДЗЗСЄ;
- підсумкова Політична декларація;
- модернізований Віденський документ по заходам довіри.

Всі держави-учасниці ОБСЄ мають рівні права та положення статусом. Рішення приймаються на основі консенсусу. Рішення не носять юридично обов'язкового характеру, але мають велике політичне значення [28].

Отже, Організація з безпеки і співробітництва в Європі є найбільшою в світі регіональною організацією з безпеки, держави-учасниці якої оперізують планету від Ванкувера до Владивостока. Крім цього організація має додатково 11 держав-партнерів. ОБСЄ є головним форумом для обговорення і прийняття заходів по життєво важливих питань світу, безпеки і прав людини в Європі та Центральній Азії. Дорога до створення колективної безпеки і стабільності вибудовується шляхом пошуку угод, прийнятих після досягнення консенсусу сторін.

Як спадкоємиця історичних Гельсінських угод , ОБСЄ є платформою для політичної та громадської дипломатії, на якому США працюють разом з Європою з глобальних проблем для знаходження шляхів побудови єдиної, вільної і мирної Європи, для вирішення нових завдань, для врегулювання затяжних конфліктів в регіоні дії ОБСЄ, а також для заохочення розвитку демократії та поваги до прав людини. Очікується, що після війни в Грузії в серпні 2008 р і після закликів Росії до нових підходів до питань безпеки в Європі, роль ОБСЄ у формуванні розгортається дискусії щодо європейської безпеки стане ще значніше.

56 держав-учасниць ОБСЄ прийняли принцип про те, що справжня безпека і взаємна довіра між державами-учасниками включає в себе

транспарантність кожної держави щодо дії його політичної системи та поваги норм ОБСЄ з прав людини, нормам права, свободи ЗМІ та демократії. Визнання того, що реальна політична і військова безпека Трансатлантичного / Європейського / Центрально-Азіатського регіону повинна бути побудована на базі зобов'язань відкритого суспільства робить ОБСЄ унікальною організацією щодо її підходів до питань військової і політичний безпеки. [28]

США розцінюють ОБСЄ як засіб для ефективного багатостороннього співробітництва. За допомогою тісної співпраці з 18 польовими місіями ОБСЄ, а також з іншими міжнародними організаціями та інститутами регіональної безпеки США сприяє демократичним перетворенням, розвитку поваги до прав і фундаментальних свобод людини, контролю за озброєннями, регіональної стабільності і постконфліктного примирення, розвитку заходів по зміцненню довіри і безпеки, економічного процвітання і стійкої екологічної політики. Роль ОБСЄ полягає також в наданні допомоги в боротьбі з тероризмом і іншими виникають загрозами безпеці.

Основним органом ОБСЄ для формування рішень є Постійна Рада (ПС). ПС збирається щотижня у Відні для обговорення поточного стану справ в регіоні уваги ОБСЄ і для розробки колективних рішень.

Через свою місію при ОБСЄ США бере участь в роботі трьох багатосторонніх органів спостереження за виконанням міжнародних угод по контролю за озброєннями, який проводиться в рамках ОБСЄ:

1. Беручи участь в Спільній консультативній групі (СКГ) разом з делегаціями з 30 держав - за виконанням Договору про звичайні збройні сили в Європі (ДЗЗСЄ);

2. Беручи участь в Форумі зі співпраці в області безпеки (ФСОБ) спільно з делегаціями з усіх 56 держав - в спостереженні за військово-політичним виміром ОБСЄ і Заходами зміцнення довіри і безпеки в Європі (МДБ). Сюди ж входить Віденський документ 1999 року переговорів щодо заходів зміцнення довіри і безпеки (Віденський документ);

3. Беручи участь в Консультативній комісії за Договором з відкритого неба (ККОН) спільно з делегаціями з 34 держав - за реалізацією Договору з відкритого неба (ДОН), яке дозволяє військові польоти над територією держав-учасниць договору і фотографування їх території.

У той же час, місія США при ОБСЄ використовує Форум зі співробітництва в галузі безпеки, включаючи його щотижневі «Діалоги з безпеки», для залучення союзників і партнерів до справи просування наших більш широких пріоритетних завдань європейської стратегії. Кожне рішення щодо будь-якої угоди з контролю за озброєннями приймається тільки на підставі консенсусу всіх держав-учасників.

Конкретні цілі США в рамках ОБСЄ [29]:

• підвищення політичної і військової безпеки в регіоні дії ОБСЄ, включаючи запобігання поступової ремілітаризації Євро-Атлантичної безпеки;

• реалізація та контроль за дотриманням угод по контролю за озброєннями;

• посилення можливостей ОБСЄ з попередження і врегулювання конфліктів;

•сприяння реалізації угод ОБСЄ в усіх трьох вимірах: військово-політичному, економічному, екологічному та соціальному вимірі;

•підтримка демократії, правових норм і поваги до прав і до фундаментальних свобод людини;

• боротьба з новими загрозами безпеці, такими як тероризм, нетерпимість і торгівля людьми;

• залучення підвищеної уваги і ресурсів до Центральної Азії за допомогою програм сприяння демократичним інститутам і практиці демократії, поліпшення прикордонної безпеки, розширення існуючих програм допомоги поліції і заохочення розвитку економіки і вільного ринку з метою досягнення миру, безпеки, справедливого управління і демократії;

• збереження ефективності ОБСЄ.

Польові місії ОБСЄ грають важливу роль в досягненні цих цілей. Значний внесок в ефективність роботи ОБСЄ вносять також такі інститути ОБСЄ, як Бюро з демократичних інститутів і прав людини (БДІПЛ), Верховний комісар у справах національних меншин (ВКНМ) і Представник з питань свободи ЗМІ (ПССМІ).

ОБСЄ дотримується всебічного підходу, що охоплює три виміри - військово-політичний, економіко-екологічний та суспільний. Права людини і основні свободи є основою стабільних суспільств. ОБСЄ допомагає своїм державам- учасницям у[29] :

- формуванні демократичних інститутів;
- проведенні справедливих і прозорих демократичних виборів;
- забезпеченні поваги до прав людини;
- свободи ЗМІ;
- прав національних меншин і верховенства закону;
- просуванні принципів толерантності і недискримінації.

ОБСЄ також протидіє викликам безпеки, що несуть транснаціональний характер, таким як насильницький екстремізм і радикалізація, що ведуть до тероризму, кіберзлочинність, великі міграційні потоки, незаконний обіг наркотиків та зброї, торгівля людьми. Це ті сфери, де державам при необхідності потрібно працювати спільно. У всіх напрямках своєї діяльності ОБСЄ працює над просуванням гендерної рівності та займається залученням молоді. ОБСЄ тісно працює з іншими міжнародними та регіональними організаціями і співпрацює з країнами-партнерами в Середземномор'ї та Азії. Вона залучає до своєї діяльності громадянське суспільство і збільшує коло інших партнерів, включаючи наукове співтовариство, а також приватний сектор і сектор розвитку. Працюючи разом, різні структури ОБСЄ підтримують держави в зміцненні довіри і побудові вільного, демократичного, загального і єдиного євроатлантичного і євразійського спільнот безпеки. У військовій області ОБСЄ прагне до підвищення відкритості, прозорості та співпраці. З цією метою було створено найсучасніший в світі режим контролю

над озброєннями і заходів зміцнення довіри. Напрямки роботи включають в себе реформування сектора безпеки і безпечного зберігання та утилізації стрілецької зброї та звичайних боєприпасів.

Економіко-екологічні питання є одним з ключових факторів забезпечення безпеки. ОБСЄ сприяє шляхом просування таких тем, як належне врядування, боротьба з корупцією, обізнаність про екологічні проблеми, використання природних ресурсів та раціональне управління екологічними відходами.

5.8. Правове регулювання забезпечення економічної безпеки в США

Особливу увагу та інтерес для ефективного забезпечення економічної безпеки будь-якої держави представляє аналіз особливостей забезпечення економічної безпеки Сполучених Штатів Америки. Проблема економічної безпеки була вперше поставлена в США в 30-і роки. Актуальність цього питання була обумовлена світовою економічною кризою і необхідністю розробки заходів швидкого реагування на негативні фактори впливу світової економіки на національну. Тому рішенням президента Ф. Рузвельта 29 червня 1934 був утворений федеральний комітет з економічної безпеки

Діюча американська доктрина в галузі забезпечення економічної безпеки відрізняється від вітчизняної своїми принципами, цілями, завданнями, формами і методами її реалізації. Американський вчений У. Ліппман концептуальну ідею національної безпеки держави сформулював наступним чином: «Нація забезпечує свою безпеку, коли вона не жертвує своїми законними інтересами для уникнення війни і здатна, в разі якщо ці інтереси наражаються на небезпеку, відстоювати їх за допомогою війни» [29].

Нормативно-правовим актом, на основі якого будується забезпечення економічної безпеки США, є Стратегія національної безпеки. До нормативно-правових актів, які регулюють суспільні відносини у сфері забезпечення безпеки США, також відноситься Акт національну безпеку . У ньому наводиться логічна формула безпеки. Національна безпека - це умова

функціонування держави, що є результатом оборонних (захисних) заходів, які підвищують невразливість держави від загроз ззовні або зсередини у відкритій і підривної формі.

Основними ознаками безпеки за американським законодавством є:

- безпека - умова функціонування держави;

- безпека - є результатом оборонних (захисних) заходів;

- оборонні (захисні) заходи спрямовані на підвищення невразливості держави;

- загрози класифікуються як внутрішні і зовнішні;

- формою прояву загроз може бути відкрита (явна) і підривна (прихована, замаскована).

Сказане дозволяє зробити висновок про мету безпеки, яка полягає в збільшенні потенціалу держави та його ресурсів. Стосовно до категорій «оборона» і «наступ» зауважимо, що подібна мета досягається виключно за рахунок настання необхідності в таких діях. Тож можна зробити висновок, що безпека США є результатом захисних заходів. У нормативних правових актах США закріплено, що безпека досягається шляхом «проведення заходів». Законодавство США вказує на необхідність протидії загрозам, які не виражені в явній формі. Ймовірно, йдеться про широке застосування заходів превентивного характеру щодо загроз і можливості залучення державних органів, що забезпечують безпеку, для протидії проявам зовнішнього середовища, які підпадають під визначення «підривну» (приховане, неявне).

З огляду на те що США мають виражені в законодавстві економічні інтереси, будь-який вплив світової економіки, політичний захід окремої держави можна визначити як «протидія» інтересам США. Безпека в американському визначенні є активною наступальною системою заходів щодо недопущення реалізації факторів негативного впливу та можливих протидій національним інтересам.

У законодавстві США немає окремого нормативно-правового акта, що регулює забезпечення національної економічної безпеки. Але Стратегія

національної безпеки США, будучи концептуальним документом, що визначає цілі, завдання та напрямки діяльності американських державних органів, приділяє особливу увагу економічному аспекту проблеми. Стратегія складається із [29]:

- вступу;
- розділу, присвяченого забезпеченню інтересів США в світі;
- розділу, присвяченого комплексним регіональним проблемам.

Одним з ключових положень Стратегії, що визначають важливий напрям регулювання суспільних відносин, є наступна норма: «Ми виходили з того, що грань між внутрішньою і зовнішньою політикою зникає. Ми повинні підвищити економіку, щоб підтримувати збройні сили, положення за кордоном і глобальний вплив. Ми повинні брати активну участь в міжнародних справах, щоб відкрити іноземні ринки і створити робочі місця для американців». У даній нормі визначені національні інтереси США і зазначений рядметодів, спрямованих на їх досягнення. Цілями економічної сторони національної безпеки США є підвищенння рівня економіки. Забезпечення безпеки США має сприяти зростанню економіки. Збільшення ресурсного потенціалу досягається за рахунок використання ресурсного потенціалу світової економіки. Засобом досягнення цих цілей є завоювання іноземних ринків для американських товарів і послуг. Збільшення присутності на іноземних ринках може досягатися зміною кількісних і якісних показників. В обох випадках засобами досягнення зазначених цілей можуть бути збільшення кількості американських товарів і послуг. У цьому випадку мета досягається в результаті того, що американські товари займають утворені ними ж ринки або витісняють з наявних ринків товари інших держав. Подібний результат може досягатися за рахунок високої конкурентоспроможності американських товарів, закріплення наявних або потенційно можливих ринків збуту за американськими компаніями. Такий розвиток подій можливий у випадку появи нових товарів і послуг.

Забезпечення безпеки держави в даний історичний відрізок часу, згідно зі Стратегією, полягає в здійсненні заходів за трьома напрямками. Стратегія вказує на необхідність:

- надійно підтримувати власну безпеку, спираючись на збройні сили;

- сприяти пожвавленню американської економіки;

- сприяти зміцненню демократії за кордоном .

Зазначені напрями діяльності взаємно доповнюють один одного. Демократичні держави не будуть загрожувати американським інтересам і будуть співпрацювати з США, протидіючи загрозам у галузі безпеки, підтримуючи вільну торгівлю і сталий розвиток. Сильна економіка не менш важлива для забезпечення положення у світі, ніж боєготові збройні сили .

Стратегія національної безпеки США вказує на необхідність підтримки лідируючого положення США у світі. До цілей національної безпеки Стратегія відносить:

- забезпечення військових і оборонних переваг над будь-якою іноземною державою або групою держав;

- забезпечення сприятливих політичних позицій на міжнародній арені;

- досягнення військового потенціалу, здатного успішно протистояти ворожим і руйнівним силам ззовні або зсередини.

Американський дослідник Д. Нойхтерлайн визначає національні інтереси в такий спосіб: «Національний інтерес - збереження добробуту американських громадян і американського підприємництва, пов'язаних з міжнародними відносинами і перебувають під впливом політичних сил поза адміністративного контролю уряду США».

Безпека США досягається не в результаті нейтралізації факторів впливу на національні інтереси, а в результаті заходів, спрямованих на збереження лідируючого становища держави в світі. Американський досвід показує, що навіть в сталій ринковій економіці проблеми економічної безпеки зберігають свою актуальність і вимагають постійного вдосконалення механізму її забезпечення. Необхідно мати на увазі, що американська стратегія безпеки

покликана не тільки захищати власні економічні інтереси від зовнішніх загроз. У не меншому ступені на меті вона закріпила пристосування світової економіки, економіки будь-якої країни в світі, включаючи економіки своїх союзників, до економічних інтересів США. Більшість з відомих в світі транснаціональних корпорацій зосереджена в США. Тому американська стратегія забезпечення економічної безпеки передбачає реалізацію економічних інтересів на всьому просторі комерційної діяльності своїх підприємств, фактично по всьому світу. Оскільки США є найбільшим експортером і імпортером товарів і послуг, мають активний торговельний баланс, стратегія економічної безпеки США більшу частину відводить питань забезпечення безпеки так званої другої економіки (зарубіжної). Американське законодавство передбачає наявність чітко вираженої економічної мети. Як території, на яку поширюються національні економічні інтереси, нормативна база США вказує територію всього світу. Для успішної реалізації економічних інтересів і досягнення економічних цілей США активно беруть участь у створенні міжнародних спілок, асоціацій та договорів. При цьому США прагнуть забезпечити собі провідну роль у підготовці та прийнятті рішень даними союзами. Законодавчо закріплені не тільки поняття, принципи, умови забезпечення економічної безпеки, а й пріоритети, засоби, методи, цілі даної діяльності. У законодавстві США приділяється достатня увага механізмам державного регулювання економіки. Науково обгрунтовані і нормативно врегульовані такі аспекти забезпечення економічної безпеки, як антимонопольна діяльність, охорона власності. Разом з цим державний сектор економіки малий у порівнянні з приватним, існує відносна свобода переміщення капіталу, відсутні системи ліцензування, квотування виробництва, регулювання діяльності підприємств відбувається в основному нормативним методом. Тому економіка США може бути віднесена до категорії змішаної, з переважанням ліберальної моделі, що накладає відбиток на правову модель забезпечення економічної безпеки.

Список використаних джерел до розділу 5

1. Деренуца А.С. АНАЛИЗ ОПЫТА СТРАН ЕВРОПЕЙСКОГО СОЮЗА В СФЕРЕ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ. Таврический Национальный Университет им. В.И. Вернадского. УДК 351.863/339.923:061.1ЕС+001.8. URL: http://gisap.eu/ru/node/172

2. Ocepek A. Economic Security and the European Dream . Anthony Louis Ocepek. – Marquette University.
URL: http://www.anselm.edu/Documents/NHIOP/Global%20Topics/2010/Ocepekpaper.pdf.

3. A Strong Britain in an Age of Uncertainty: The National Security Strategy. Официальный сайт Министерства Обороны Великобритании. – УДК : http://www.official-documents.gov.uk.

2. Г.А. Гончаров. Пути внедрения зарубежного опыта развития индустрии безопасности в Украине. Економіка: реалії часу. Науковий журнал. – 2015. – № 1 (17). – С. 173-179. URL: : http://economics.opu.ua/files/archive/2015/n1.html

3. Амитан В. Н. Экономическая безопасность: концепция и основные модели. Экономическая кибернетика. – 2009. – №3. – С. 13 – 20.

4. Зарубежное военное обозрение. 2015, №1, С.27-31 URL: http://www.library.ugatu.ac.ru/pdf/magazins/zavo15_no1.pdf

5. Додаток до Першого Загального Розпорядження Європейської комісії № 800/2008 від 6 серпня 2008 року.

6. Рішення Суду Європейського Союзу у справі С-222/04.

7. Рішення Суду Європейського Союзу від 12 грудня 1974 року № 36,74 в справі Walrave.

8. Закон про безпеку масових заходів від 20 березня 2009 року.

9. М.Друждж, Закон про безпеку масових заходів. Коментар, Варшава 2015.

10. Положення щодо безпеки під час футбольних матчів, організованих Польською футбольною асоціацією та Ekstraklasa S.A.

11. Перший додаток до Положень щодо безпеки під час футбольних матчів, організованих Польською футбольною асоціацією та Ekstraklasa S.A - план УЄФА щодо расизму.

12. Ewelina Rutkowska. Kluby sportowe zapłacą milionowe kary za korupcję swoich zawodników. URL: https: //prawo.gazetaprawna.pl/artykuly/28969,za-yszneenstwo-kibicow-odpowiedza-kluby-sportowe.html.

13. URL: https://www.rpo.gov.pl/pl/content/trybunał-konstytucyjny-zaskarżone-przez-rpo-przepis-o-tzw-zakazie-klubowym-zgodne-z-konstytucist

14. URL: https://osce.usmission.gov/ru/our-relationship-ru/why-osce-matters-ru/

15. URL: https://www.mfa.am/ru/international-organisations/4

16. Трудовий кодекс Республіки Польща від 26 червня 1974 р. – URL: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU19740240141/U/D19740141Lj.pdf

17. Яськовський К. Трудовий кодекс Республіки Польща. Коментар. Wolters Kluwer Польща. URL: https://sip.lex.pl/#/commentary/587787380/584820

18. Конституція Республіки Польща від 2 квітня 1997 року. URL: https://www.sejm.gov.pl/prawo/konst/polski/kon1.htm

19. Куба М. Трудовий кодекс Республіки Польща: Коментар. Том I. Видання V. Wolters Kluwer Польща URL: https://sip.lex.pl/#/commentary/587769455/614263

20. Бояньчик А. Кримінально-правові аспекти захисту права працівника на таємне спілкування. Палестра, 2003, 1-2, стор. 51.

21. Кримінальний кодекс Республіки Польща від 6 червня 1997 року. URL: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU19970880553/U/D19970553Lj.pdf

22. Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000 (2000 No. 2699), стаття 3.

23. Act on the Protection of Privacy in Working Life (759/2004).

24. Куба М. Моніторинг електронної пошти працівника - роздуми на тлі нових правових норм. URL: https://sip.lex.pl/#/publication/151359061

25. Рішення Європейського Суду з прав людини від 25 червня 1997 року, Заява № 20605/92, в справі Гелфорд проти Сполученого Королівства. URL: http://kryminologia.ipsir.uw.edu.pl/images/stronka/ETPCz/A.%20Rzeplinski_Wyrok%20ETPCz_Sprawa%20Halford%20przeciwko%20Zjednoczonemu%20Krolestwu.pdf

26. Омбудсмен. Моніторинг електронної кореспонденції працівника був порушенням його права на повагу до приватного життя та кореспонденції. URL: https://www.rpo.gov.pl/pl/content/monitorowanie-korespoencji-elektronycznej-pracownik-stanowi%C5%82o-naruszenie-jego-prawa-do

27. Рішення Європейського суду з прав людини від 5 вересня 2017 року, Велика палата, заява № 61496/08, у справі Барбулеску проти Румунії. URL: https://www.hfhr.pl/wp-content/uploads/2017/09/Omowienie_orzeczenia_Barbulescu_przyżko_Rumanii_WI.pdf

28. Гаджієв К. С. Введення в політичну науку. М .: Інститут «Відкрите суспільство». 1997. С. 292.

29. Стрельников К.А. Правовое регулирование обеспечения экономической безопасности в США. Военно-юридический журнал». 2009. N 4

РОЗДІЛ 6. СТАН ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

6.1. Захист інформації

Принцип сучасного захисту інформації можна виразити так – пошук оптимального співвідношення між доступністю й безпекою.

Актуальність вивчення різних аспектів інформаційної безпеки (ІБ) пов'язана із входженням України в глобалізаційні процеси, в яких постійно зростає значення інформації. По суті, йдеться про становлення інформаційного постіндустріального суспільства, однією з найголовніших ознак якого є перетворення інформації на найцінніший товар і продукт. В інформаційному суспільстві інформаційний вплив на державу, суспільство, громадянина є ефективнішим, ніж політичний, економічний, військовий. Значення інформації зростає в міру зникнення національних кордонів між державами, подолання наслідків інформаційної ізоляції пострадянського суспільства (хоча ці наслідки в багатьох сферах, зокрема науковій, не подолані дотепер). Водночас суспільство не може не турбувати інша проблема − інформаційне перенасичення, надмір недостовірної та шкідливої інформації, не зникає і загроза національній безпеці держави через інформаційне шпигунство, інформаційну агресію іноземних держав тощо.

У таких умовах Конституція України проголошує ІБ «справою всього українського народу». Звісно, це декларація, оскільки захист ІБ держави не може бути загальнонародною справою, для цього існують спеціальні державні органи. Однак прогалини та недоліки чинної системи ІБ можуть негативно позначитися на матеріальному та духовному становищі народу. 1997 року Верховна Рада України ухвалила «Концепцію національної безпеки України», яка до загроз у національній безпеці відносить «інформаційну експансію з боку інших держав, витік інформації, що становить державну таємницю, а також конфіденційної інформації, що є власністю держави». ІБ заявлена як

одна з головних цілей «Національної програми інформатизації» (1998 р.) Цим питанням опікується комісія з питань ІБ при Президенті України.

Що ж таке ІБ? На жаль, жодні нормативні акти не дають визначення ІБ, поняття не має законодавчого оформлення. Є кілька неофіційних визначень, які не завжди узгоджені між собою. Одне з них можна знайти в проєкті Закону «Про інформаційний суверенітет та інформаційну безпеку України». У ньому ІБ розглядається як «захищеність життєво важливих інтересів суспільства, держави і особи, якою виключається заподіяння шкоди через неповноту, несвоєчасність, недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок розповсюдження інформації, забороненої для розповсюдження законами України». На думку фахівців, це визначення демонструє надмірний патерналізм держави, яка бере на себе готовність визначати, яка саме інформація є «недостовірною», «зіпсованою», «достовірною» і яку треба заборонити. Демократична держава не повинна мати монополії на інформацію та її тлумачення, а сприяти інформаційному плюралізму.

Існують інші визначення ІБ. За «Концепцією інформаційної безпеки України», ІБ − це «стан захищеності національних інтересів України в інформаційній сфері, за якою не допускається завдання шкоди особі, суспільству, державі», або 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». У цих визначеннях ми можемо спостерігати зміну акцентів та пріоритетів: якщо проєкт Закону «Про інформаційний суверенітет та ІБ» на перший план ставить інтереси суспільства та держави, то в останніх визначеннях на першому плані – інтереси особи. Тобто інформаційна безпека – це комплекс заходів захисту інформації від несанкціонованого доступу; стан забезпечення захисту таких складових інформації, як конфіденційність, доступність, цілісність.

Дослідники пропонують такі характеристики ІБ:

- ІБ балансує на стику національної безпеки та інформаційної функції держави;
- питання ІБ має екстериторіальний характер, не замикається на національних кордонах;
- протистояння між бажанням держави «засекретити» якомога більший масив інформації і невід'ємним правом людини та громадянина мати вільний доступ до інформації;
- державне регулювання інформаційної сфери відбувається лише на правовій основі.

Зважаючи на це, об'єктом ІБ є інформація, важлива для функціонування держави, демократичного розвитку суспільства, інформаційні стосунки між особою, державою та суспільством, інформаційні права людини як невід'ємна складова загальнолюдських прав.

6.2. Державна політика та система технічного захисту інформації в Україні

Якою ж є політика держави у сфері ІБ? Україна − посттоталітарна країна, відтак, чимало проблем, що виникають є наявні у сфері ІБ, вкорінюються у так званий «синдром тоталітаризму», який полягає у намаганні держави, попри демократичні декларації, побудувати таку модель стосунків між державою та суспільством, за якої суспільство матиме мінімальні відомості про державу, і відповідно мінімальний вплив на прийняття політичних рішень. І при цьому держава знатиме про суспільство практично все. Якщо конкретніше, йдеться про дві небезпечні тенденції. З одного боку, ми маємо дуже низький рівень законодавчого забезпечення інформаційної сфери. Зокрема, Закон України «Про інформацію» 1992 р., навіть з доповненнями до 2005 р., застарів і не відповідає низці демократичних

засад. Єдиним законом, який регулює сферу інформації з обмеженим доступом (ІЗОД), є чинний Закон «Про державну таємницю» в редакції 1999 р. Та з іншого боку, існують величезні масиви інформації, які під дію цього Закону не підпадають, а власної законодавчої бази або не мають, або вона вкрай незадовільна. Йдеться про службову таємницю («конфіденційна інформація, що є власністю держави»), комерційну таємницю, охорону персональних даних та інше. Коли доступ до інформації обмежується не законом, а особистим рішенням посадової особи, це відкриває шляхи для чиновницького свавілля, порушення інформаційних прав громадян, необґрунтованих засекречень тощо.

Щодо державної таємниці (ДТ) держава здійснює політику поступового збільшення обсягу засекреченої інформації, хоча, на думку фахівців, це навряд чи є доцільним. Наслідком такої політики можуть бути зниження якості прийняття політичних рішень через недоступність потрібної інформації, криза влади, інформаційна ізоляція, застій в економічному, політичному та науковому житті. Наприклад, абсолютно недоречним кроком учені вважають віднесення до сфери ДТ інформації «*про наукові, науково-дослідні, конструкторські, проектні роботи, на базі яких можуть бути створені прогресивні технології, нові види виробництва продукції, технологічних процесів, які мають важливе оборонне чи економічне значення чи суттєво впливають на зовнішньоекономічну діяльність і національну безпеку України*», оскільки держава не повинна безпідставно засекречувати інформацію «про всяк випадок», бо те, чи матиме така наукова інформація оборонне чи економічне значення, ще невідомо. Але це істотно обмежує науково-інформаційні контакти наших учених з їхніми колегами з-за кордону, не сприяє вільному обігу наукової інформації. А без свободи, поза сферою інформаційного різноманіття, інформація існувати не може.

Інформаційне право − це відносно молода галузь права, предметом якої є інформаційні відносини, що виникають у процесі обігу інформації в інформаційній сфері. За останні роки сформувався великий обсяг

законодавчих актів, що регулюють інформаційну сферу, зокрема сферу ІБ та захисту інформації. Отже, до предмета вивчення інформаційного права потрапляє ІБ та нормативно-правова база, яка її гарантує. Якими ж є недоліки українського законодавства у сфері ІБ та захисту інформації? Це:

1. Невідповідність більшості законів та нормативно-правових актів, ухвалених до 1996 року, Конституції України та міжнародним нормативно-правовим актам.
2. Надмірна декларативність українських законів, певні положення декларуються без вказівок на механізми їх реалізації.
3. Нерідко трапляються посилання на посилання, або посилання на такі норми, які неможливо застосувати.
4. Відсутність чіткої ієрархічної структури у нормативно-правовій базі (Конституція − закони − підзаконні акти та відомчі інструкції).
5. Велика кількість підзаконних актів ускладнює можливості їх застосування.
6. Випадки суперечностей між законами та відомчими інструкціями, міжнародними правовими актами та українськими законами, колізії між різними законами тощо.
7. Неузгодженість нових законів з попередніми, що спричиняє правовий хаос.
8. Наявність великого обсягу засекреченої інформації поза законодавчим полем.
9. Широкі можливості для посадових осіб безкарно і безпідставно засекречувати інформацію.
10. Незадовільна правова основа доступу громадян до інформації, що перебуває в руках державних органів.
11. Термінологічна неузгодженість (наприклад, у законодавстві відсутнє однозначне тлумачення таких термінів, як «документ», «інформація», «державні секрети», «таємна інформація», «таємниця», «інформаційна безпека», «інформаційний суверенітет», «документована інформація», є

5 різних визначень «конфіденційної інформації», 3 визначення «захисту інформації», 2 – «таємної інформації» тощо).

12. Невизначеність механізмів забезпечення відповідальності за порушення інформаційного законодавства.

13. Не розробленість, точніше відсутність законодавчої бази для таких сфер як захист персональних даних, доступ до конфіденційної інформації, що є власністю держави, комерційна таємниця та інше.

14. Відсутність інституцій, які б спеціалізувалися на питанні захисту інформації, форм запиту на отримання інформації, невизначеність механізму надання державних документів.

За подібних умов інформація про діяльність державних органів може фактично перетворитися на «державну таємницю», що суперечить принципам України як демократичної, правової, соціальної держави, та міжнародним демократичним нормам стосунків влади і громадян.

6.3. Нормативно-правова база України у сфері технічного захисту інформації

Права людини в інформаційному суспільстві: міжнародні правові акти, що стосуються інформаційних прав особи. Принцип верховенства права в інформаційній політиці держави. Важливим аспектом інформаційної діяльності демократичної держави є ієрархія пріоритетів, серед яких на першому місці стоїть міжнародне право, на другому – національне законодавство разом з Основним Законом, і вже далі − підзаконні акти, які не повинні суперечити міжнародному та національному законодавству. Як відомо, в українському законодавстві з дотриманням цієї ієрархічності не все гаразд. Часто підзаконні акти та відомчі інструкції стоять на першому місці в діяльності окремих державних органів та посадових осіб.

Які міжнародні правові акти гарантують інформаційні права та свободи людини і громадянина, зокрема право на конфіденційність та право на вільне

отримання інформації? Передусім, це «Загальна Декларація прав людини» (1948 р.). Відповідно до статті 12, «ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя“. Згідно з статтею 19 «кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів».

Важливим документом є «Європейська конвенція про захист прав людини та основних свобод» (1950 р.), яка про інформаційні права людини говорить таке: стаття 10 «Кожен має право на вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів». У цій же конвенції міститься перелік винятків, коли права громадян можуть бути обмежені на законних підставах: «Здійснення цих свобод може бути обмежене в інтересах громадської безпеки, запобігання злочинам, охорони здоров’я, моралі, запобігання розголошенню конфіденційної інформації».

Розвиток комп’ютерних технологій призвів до масової практики автоматизованої обробки інформації в комп’ютерних мережах, в тому числі інформації персонального характеру. Виникла потреба додаткового захисту інформаційних прав людини. Цій меті має служити «Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру» (Страсбург, 28 січня 1981 р.). У Преамбулі Конвенції зазначено, що її головною метою є гарантування свободи інформації незалежно від кордонів, безперешкодного обігу інформації між народами. Зміст Конвенції можна проілюструвати через окремі статті.

Стаття 1 гарантує право людини на недоторканність особистого життя, яке підлягає ризику під час автоматизованої обробки персональних даних. Стаття 5 визначає якість обробки даних про особу: «Дані особистого характеру, що підлягають автоматизованій обробці: а) отримуються та

обробляються сумлінно та законно; б) зберігаються для визначених та законних цілей; в) мають бути адекватними, відповідними і ненадмірними з точки зору цілей, заради яких вони зберігаються; г) мають бути точними і поновлюватися (на вимогу особи); д) зберігатися не довше, ніж це потрібно цілям збереження». Стаття 6 виокремлює особливу категорію персональних даних, які одержали назву «вразливі» або «делікатні». Це «дані особистого характеру, що свідчать про расову належність, політичні або релігійні та інші переконання, а також дані особистого характеру, що стосуються здоров'я, статевого життя, не можуть піддаватися автоматизованій обробці. Це правило стосується також особистих даних, що стосуються кримінального засудження». Стаття 8 встановлює додаткові гарантії для суб'єкта даних: а*)* «особі надається можливість встановлювати існування файлу особистих даних для автоматизованої обробки, особу і місцезнаходження контролера файлу; б) отримувати без затримки чи витрат підтвердження чи спростування інформації про зберігання даних особистого характеру; в) вимагати виправлення і знищення незаконно одержаних даних; г) гарантується правовий захист персональних даних». Звісно, європейське право передбачає чітке окреслення сфери винятків, їх обґрунтованість і зрозумілість. Обмежити інформаційні права громадян можна в кількох випадках: в інтересах захисту державної та громадської безпеки, валютно-кредитних інтересів держави, боротьби з кримінальними структурами, а також в інтересах захисту прав і свобод інших громадян (стаття 9). Крім того, особисті дані можна використовувати в статистичних підрахунках та наукових дослідженнях (як правило, в знеособленому вигляді).

Важливим міжнародним документом є також «Директива Європарламенту та Ради Європи стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» від 15 грудня 1997 року, метою якої є «забезпечення невтручання в особисте життя при обробці персональних даних в телекомунікаційному просторі та для забезпечення вільного переміщення таких даних». Сфера

винятків будується за аналогією з попередніми європейськими актами: це громадський порядок, оборона, державна безпека (включаючи економічний добробут держави), кримінальне право.

Імплементація положень європейського права щодо захисту інформаційних прав людини та громадянина вважається необхідною умовою демократизації політико-правової системи України, її наближення до стандартів ЄС та формування громадянського суспільства.

Конституція України про інформаційні права громадян та інформаційну безпеку. Конституція (1996 р.) у статті 17 проголошує, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу». Йдеться про те, що від інформаційної безпеки держави залежить доля народу, його матеріальний добробут та духовне благополуччя. Стаття 19 однозначно стверджує пріоритет Закону та Конституції перед іншими нормативними актами: «Органи державної влади та органи місцевого самоврядування, їхні посадові особи зобов'язані діяти лише в межах повноважень та у спосіб, що передбачені Конституцією та законами України». Проте громадяни мають право апелювати до Конституції як закону прямої дії, якщо посадова особа відмовляє у задоволені запиту громадянина, керуючись підзаконними актами чи внутрішніми інструкціями.

32-га стаття гарантує, що «ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати

вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації».

34-та стаття говорить про право «вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір», а також встановлює перелік винятків, коли право громадян може бути обмежено: «Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя».

Як бачимо, поряд із винятками, визначеними європейськими документами, згадується кілька специфічно українських, а саме: запобігання розголошенню конфіденційної інформації та «підтримання авторитету правосуддя». При цьому найменш зрозумілим є останній виняток.

Так чи інакше, Конституція є найважливішим юридичним актом, що забезпечує інформаційні права громадян України, право на недоторканність приватного життя, та закладає основи для розробки спеціального законодавства з охорони інформаційної безпеки держави.

Основні положення Закону України «Про інформацію». «Концепція національної безпеки України» про загрози в інформаційній сфері. Базовим чинним законом, що регулює інформаційну сферу, є Закон України «Про інформацію», прийнятий 2 жовтня 1992 р. Доцільно викласти основні положення закону. Під терміном «інформація» закон розуміє «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві» (стаття 1). Основними принципами інформаційних відносин вважаються: гарантованість права на інформацію; відкритість та доступність інформації; свобода інформаційного обміну; об’єктивність та вірогідність

інформації; законність її одержання, використання, поширення та збереження (стаття 5).

Статті 17 та 18 визначають галузі та види інформації: основними галузями інформації є: політична, економічна, духовна, науково-технічна, соціальна, екологічна, міжнародна. До видів належить: статистична інформація; адміністративна інформація (дані); масова інформація; інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування; правова інформація; інформація про особу; інформація довідково-енциклопедичного характеру; соціологічна інформація.

Стаття 27 надає законодавче визначення терміну «документ»: «Документ – це передбачена законом матеріальна форма одержання, зберігання, використання і поширення інформації шляхом фіксації її на папері, магнітній, кіно-, відео-, фотоплівці або на іншому носієві. Первинний документ – це документ, що містить в собі вихідну інформацію. Вторинний документ – це документ, що являє собою результат аналітико-синтетичної та іншої переробки одного або кількох документів».

Стаття 28 поділяє інформацію на відкриту та інформацію з обмеженим доступом (ІЗОД), а стаття 30 роз'яснює, що таке ІЗОД, встановлює режими доступу до інформації. Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну.

«*Конфіденційна інформація* – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ – надано статус конфіденційної. Порядок обліку, зберігання і використання документів та інших носіїв інформації, що містять зазначену інформацію, визначається Кабінетом Міністрів України. До конфіденційної інформації, що

є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, не можуть бути віднесені відомості:

про стан довкілля, якість харчових продуктів і предметів побуту;

про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;

про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

стосовно стану справ із правами і свободами людини і громадянина, а також фактів їх порушень;

про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

інша інформація, доступ до якої відповідно до законів України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути обмеженим.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до закону про цю інформацію.

Порядок обігу таємної інформації та її захисту визначається відповідними державними органами за умови додержання вимог, встановлених цим Законом.

Порядок і терміни обнародування таємної інформації визначаються відповідним законом.

Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист».

Ця стаття є засадничою для роботи державних службовців з документами, що належать до категорії ІЗОД, громадян, які зацікавлені в отриманні «суспільно важливої» інформації та захисті своїх інформаційних прав, в тому числі права на конфіденційність. У наступній статті 31 якраз йдеться про право громадян на доступ до інформації, а саме: громадяни мають право «*знати у період збирання інформації, які відомості про них і з якою метою збираються, як, ким і з якою метою вони використовуються; доступу до інформації про них, заперечувати її правильність, повноту, доречність тощо.*

Державні органи та організації, органи місцевого і регіонального самоврядування, інформаційні системи яких вміщують інформацію про громадян, зобов'язані надавати її безперешкодно і безкоштовно на вимогу осіб, яких вона стосується, крім випадків, передбачених законом, а також вживати заходів щодо запобігання несанкціонованому доступу до неї. У разі

порушень цих вимог Закон гарантує захист громадян від завданої їм шкоди використанням такої інформації.

Забороняється доступ сторонніх осіб до відомостей про іншу особу, зібраних відповідно до чинного законодавства державними органами, організаціями і посадовими особами.

Зберігання інформації про громадян не повинно тривати довше, ніж це необхідно для законно встановленої мети.

Всі організації, які збирають інформацію про громадян, повинні до початку роботи з нею здійснити у встановленому Кабінетом Міністрів України порядку державну реєстрацію відповідних баз даних.

Необхідна кількість даних про громадян, яку можна одержати законним шляхом, має бути максимально обмеженою і може використовуватися лише для законно встановленої мети.

Відмова в доступі до такої інформації, або приховування її, або незаконні збирання, використання, зберігання чи поширення можуть бути оскаржені до суду».

Усі ці положення відповідають європейським правовим нормам. Держава не має права безпідставно відмовляти громадянину у задоволенні його інформаційного запиту, а термін вивчення запиту не повинен перевищувати 10 днів. Задоволення ж запиту повинно відбутися упродовж 30 днів. Громадянин має право оскаржувати в суді відмову державного органу задовольнити інформаційний запит, при цьому саме держава повинна доводити в суді законність такої відмови. Якщо суд встановив, що запитувачу відмовили незаконно, винні посадові особи притягуються до дисциплінарної та іншої, передбаченої законодавством, відповідальності.

37-ма стаття роз'яснює обмеження на доступ до тієї чи іншої інформації. Не всі інформаційні запити громадян можуть бути задоволені. До інформації, що не надається та не оприлюднюється, належать: інформація, визнана державною таємницею; конфіденційна інформація; інформація про оперативну і слідчу роботу органів прокуратури, Міністерства внутрішніх

справ, Служби безпеки України, роботу органів дізнання та суду, якщо її розголошення може зашкодити оперативним заходам, розслідуванню чи дізнанню, порушити право людини на справедливий та об'єктивний судовий розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи; інформація, що стосується особистого життя громадян; документи, що становлять внутрішньовідомчу службову кореспонденцію (доповідні записки, переписка між підрозділами та інше), якщо вони пов'язані з розробкою напряму діяльності установи, процесом прийняття рішень і передують їх прийняттю; інформацію, що не підлягає розголошенню згідно з іншими законодавчими або нормативними актами. Установа, до якої надано запит, може не надавати для ознайомлення документ, якщо він містить інформацію, яка не підлягає розголошенню на підставі нормативного акта іншої державної установи, а та державна установа, яка розглядає запит, не має права вирішувати питання щодо її розсекречення; інформація фінансових установ, підготовлена для контрольно-фінансових відомств.

Закон забороняє державну цензуру: «*забороняються створення будь-яких органів державної влади, установ, введення посад, на які покладаються повноваження щодо здійснення контролю за змістом інформації, що поширюється засобами масової інформації*» (стаття 45-1). Водночас інформацією та інформаційною свободою не можна зловживати: «*інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання расової, національної, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини*» (стаття 46).

Закон гарантує рівність усіх учасників інформаційних відносин (громадяни, юридичні особи та держава), розглядає інформацію з погляду права власності. Крім того, закон визначає низку термінів, важливих у процесі інформаційних відносин: це поняття «інформація як товар», «інформаційна продукція», «інформаційна послуга».

Важливим моментом є встановлення відповідальності за розголошення інформації, яка розголошенню не підлягає (стаття 47). Однак у цій статті є важливий елемент, пов'язаний з формуванням громадянського суспільства: громадянин звільняється від відповідальності за розголошення ІЗОД, якщо він у суді зміг довести «суспільну важливість» такої інформації, тобто потреба суспільства знати цю конкретну інформацію визнана важливішою за можливі негативні наслідки її розголошення. На цьому пункті, до речі, ґрунтується легітимність роботи журналістів.

Закон «Про інформацію» 1992 р. (з доповненнями до 2005 р.) безумовно є прогресивним у плані забезпечення демократичних прав та свобод громадян, вільного обігу інформації, але до деяких його положень фахівці висловлюють зауваження. Наприклад, акцентують на відсутності у Законі концепції офіційної інформації, неконкретність положень про секретність, розмитість сфери прав та обов'язків громадян і обов'язків державних органів. До осіб, що мають право доступу до інформації, пропонують включити також жителів держави, які ще не отримали громадянства. Концепція «авторського контролю» за доступом до конфіденційної інформації вважається застарілою, принаймні, вона зникає з європейського права (йдеться про те, що власник конфіденційної інформації самостійно визначає режим доступу до неї, спосіб отримання, коло осіб, що мають доступ, захист і так далі). Також звертається увага на брак критеріїв гіпотетичної шкоди від розголошення інформації та суспільного інтересу до цієї інформації. Дослідники пропонують створити доступний реєстр усіх документів, на які поширюються положення Закону для того, щоб допомогти громадянам у пошуку потрібної їм інформації. Нарешті, найбільшій критиці підлягає положення 29-ї статті про переважне право доступу до інформації службовців під час виконання службових обов'язків. На думку фахівців, це положення суперечить принципові рівності усіх осіб у доступі до інформації. Отже, Закон «Про інформацію» потребує істотних змін та доповнень, враховуючи демократичний поступ нашої держави та вимоги часу.

Україна − суверенна держава. Тому на порядку денному – проблема захисту її інформаційного простору від негативних впливів. Це не означає запровадження цензури, мова йде лише про те, що держава, яка існує на кошти платників податків, повинна забезпечити для них належні умови для інтелектуального, фізичного, духовного розвитку. Про захист інформаційного простору держави йдеться у документі під назвою «Концепція національної безпеки України» (1997 р.). У 3-му розділі концепції визначено загрози національній безпеці України в інформаційній сфері:

- відсутність необхідної інфраструктури в інформаційній сфері;
- повільне входження України у світовий інформаційний простір, брак у міжнародного співтовариства об'єктивного уявлення про Україну;
- інформаційна експансія з боку інших держав;
- витік інформації, що становить державну та іншу таємницю, а також конфіденційної інформації, що є власністю держави;
- запровадження цензури.

«Концепція» формулює основні напрями державної політики у сфері національної безпеки України:

- вжиття комплексних заходів щодо захисту інформаційного простору та входження України у світовий інформаційний простір;
- усунення причин інформаційної дискримінації України, інформаційної експансії інших держав;
- розробка засобів і режимів отримання, зберігання суспільної цінності інформації, створення розвиненої інфраструктури в інформаційній сфері.

«Концепція» є, по суті, декларацією про наміри, а здійснення цих заходів, їх конкретизація покладається на органи державної влади, зокрема силові структури. Але найголовніше: суспільство має усвідомити важливість інформаційної політики, яка поки що недооцінюється.

Державні стандарти та нормативні документи, що стосуються технічного захисту інформації (ТЗІ). До них належать такі документи:

«Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення» (ДСТУ 3396.0-96); «Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт» (ДСТУ 3396.1-96); «Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення» (ДСТУ 3396.2-96).

Ці стандарти установлюють об'єкт, мету, основні організаційно-технічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ. Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності і підпорядкування, громадян – суб'єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють та користуються інформацією, що підлягає технічному захисту.

Об'єктом технічного захисту є інформація, що становить державну або іншу передбачену законодавством України таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження. Об'єкт, мету і завдання ТЗІ визначають і встановлюють особи, які володіють, користуються, розпоряджаються ІЗОД у межах прав і повноважень, наданих законами України, підзаконними актами та нормативними документами системи ТЗІ. Цими стандартами визначаються носії ІЗОД, середовище поширення, мета ТЗІ (див. далі), джерела загроз.

До джерел загроз належать діяльність іноземних розвідок, а також навмисні або ненавмисні дії юридичних і фізичних осіб. Далі йдеться про канали поширення загроз, розроблення і реалізацію системи захисту інформації, контроль за ТЗІ та функції нормативних документів у сфері ТЗІ. Такими функціями, зокрема, є: проведення єдиної технічної політики; створення і розвиток єдиної термінологічної системи; функціонування багаторівневих систем захисту інформації на основі взаємоузгоджених

положень, правил, методик, вимог та норм; функціонування систем сертифікації, ліцензування й атестації згідно з вимогами безпеки інформації; розвиток сфери послуг у галузі ТЗІ; установлення порядку розроблення, виготовлення, експлуатації засобів забезпечення ТЗІ та спеціальної контрольно-вимірювальної апаратури; організація проектування будівельних робіт у частині забезпечення ТЗІ; підготовка та перепідготовка кадрів у системі ТЗІ. Нормативні документи системи ТЗІ поділяють на: нормативні документи із стандартизації у галузі ТЗІ; державні стандарти та прирівняні до них нормативні документи; нормативні акти міжвідомчого значення, що реєструються у Міністерстві юстиції України; нормативні документи міжвідомчого значення технічного характеру, що реєструються уповноваженим Кабінетом Міністрів України органом; нормативні документи відомчого значення органів державної влади та органів місцевого самоврядування.

6.4. Структура системи захисту інформації

Комплексна система захисту інформації (КСЗІ) наведена на рис. 6.1. Основне завдання КСЗІ полягає в блокуванні технічних каналів витоку інформації та ліквідації наслідків реалізації загроз інформації. Загрози інформації складаються з багатьох факторів, тому завдання захисту потребує комплексного підходу з використанням новітніх технічних засобів і наукових розробок. Вирішення завдань включають в себе аналіз об’єкта захисту, розробку системи виявлення каналів витоку інформації та економічне обґрунтування необхідності використання системи захисту інформації. КСЗІ являє собою діючі у єдиній сукупності законодавчі, організаційні, технічні, криптографічні та інші заходи і засоби, які забезпечують захист інформації від усіх визначених загроз і можливих каналів її витоку, і особливо каналів електромагнітного випромінювання.

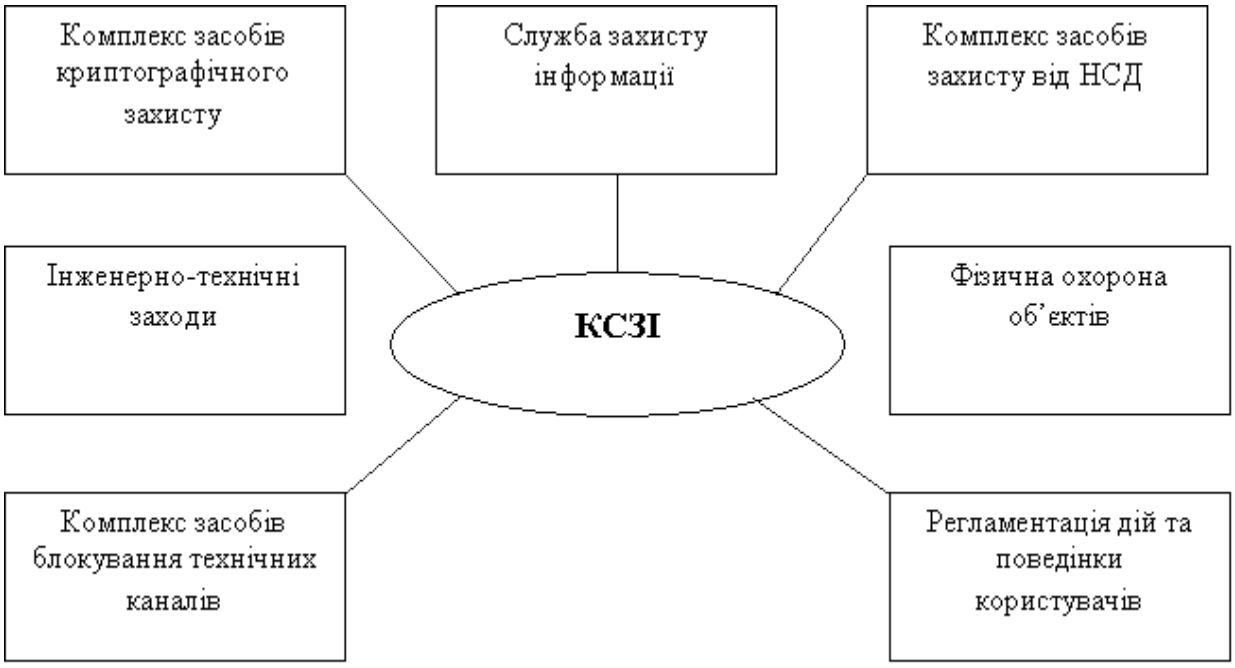

Рис. 6.1. Комплексна система захисту інформації

КСЗІ створюється поєднанням застосування технічних, фізичних та організаційних заходів. Проектування КСЗІ відбувалось на принципах побудови раціональної та ефективної системи захисту. Структура засобів КСЗІ зображена на рис. 6.2. Організаційно-правовими заходами реалізується комплекс відповідній нормативно-правовій базі держави адміністративних і обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту шляхом аналізу загроз, регламентації діяльності персоналу і визначення порядку функціонування засобів забезпечення інформаційної діяльності і засобів ТЗІ, а також шляхом створення служб, відповідальних за їх реалізацію. Основним завданням технічних заходів є забезпечення фізичної інформаційної безпеки.

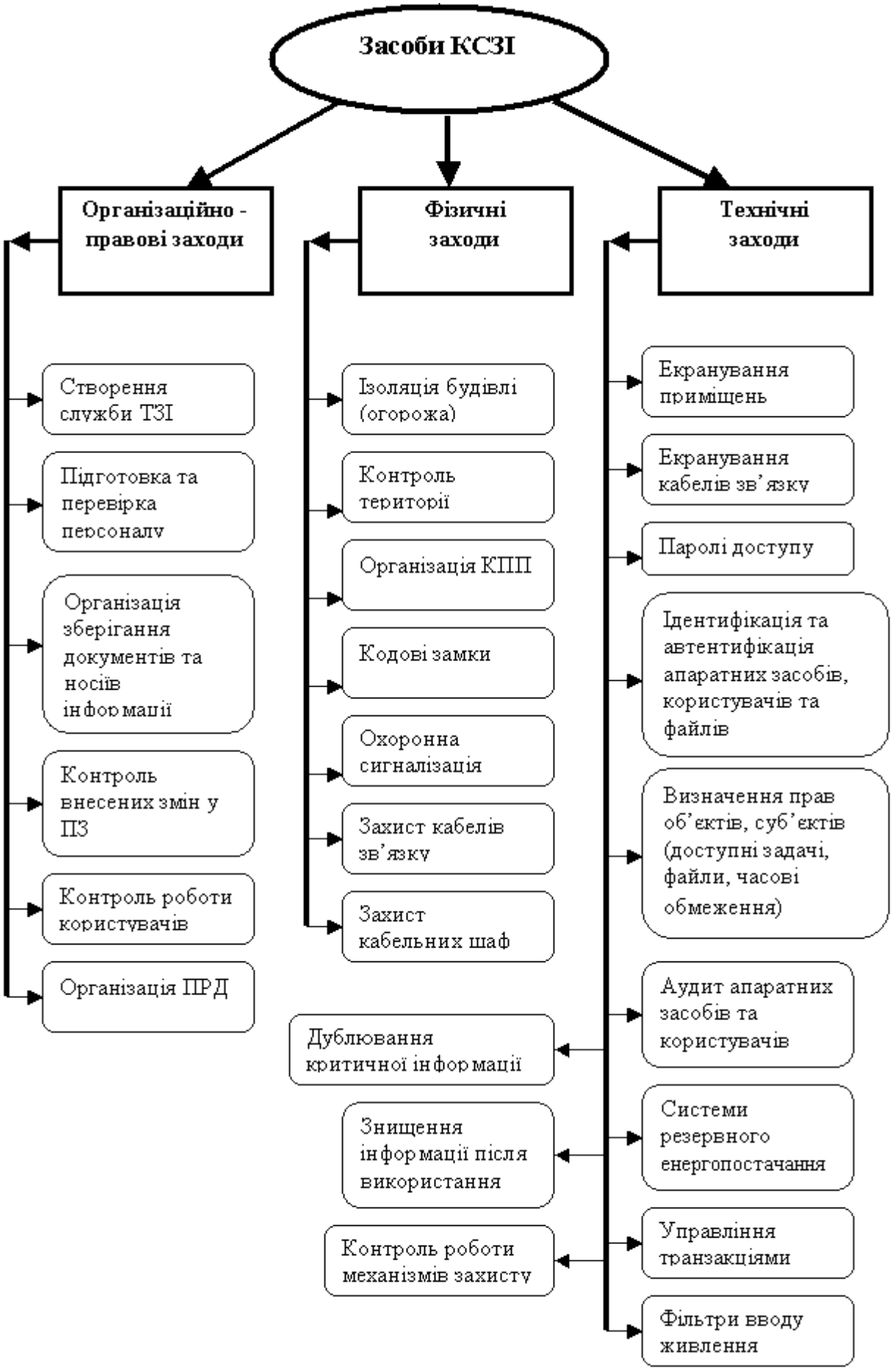

Рис.6.2. Структура засобів КСЗІ

Фізичні заходи захисту інформації створюють пристрої та споруди, проводять заходи, що утруднюють або унеможливлюють проникнення потенційних порушників у місця, де можна мати доступ до системи управління та інформації, що захищається. Пропонується застосувати фізичну ізоляцію споруди, де встановлена апаратура, від інших будівель зокрема – огородження й систематичний контроль території, організація контрольно-пропускних пунктів, обладнання вхідних дверей спеціальними замками, організація системи охоронної сигналізації.

Застосовані ізоляція будинку, контроль території, кодові замки, контрольно-пропускний пункт (КПП), охоронна сигналізація. Від витоку інформації по каналах побічних електромагнітних випромінювань та наводок (ПЕОМ) пропонується екранування приміщень та кабелів зв'язку, по кабелях електроживлення передбачається установка фільтрів.

Список використаних джерел до розділу 6

1. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

2. Сучасні інформаційні війни в соціальних онлайн-мережах / О. В. Курбан // Інформаційне суспільство. - 2016. - Вип. 23. - С. 85-90. - Режим доступу: http://nbuv.gov.ua/UJRN/is 2016-23-15

Наукове видання

Рибальченко *Людмила Володимирівна*
Рижков *Едуард Володимирович*
Тютченко *Світлана Миколаївна*
Гавриш *Олег Степанович*
Варяниченко *Аліна Олегівна*

БЕЗПЕКА ПІДПРИЄМНИЦТВА

Монографія

Видання друкується в авторській редакції

Відповідальний редактор *Біла К. О.*
Технічний редактор *Олексенко Н. С.*
Дизайн обкладинки *Дем'янчук М. О.*

Здано до друку 17.07.20. Підп. до друку 24.07.20.
Формат 60х84 $^{1}/_{16}$. Гарнітура – Times. Папір офсетний.
Спосіб друку – плоский. Ум. друк. арк. 7,6. Тираж 50 пр. Зам. № 0720-03/2.
.

Видавець та виготовлювач СПД Біла К. О.
Свідоцтво про внесення до Державного реєстру
суб'єктів видавничої справи ДК № 3618 від 06.11.09

Надруковано на поліграфічній базі видавця Білої К. О.
Україна, 49000, м. Дніпро, пр. Д. Яворницького, 111, оф. 2
+38 (099) 7805049; +38 (067) 2100256
www.impact.dp.ua e-mail: impact.dnepr@gmail.com