Вісник Львівського університету. Серія філос.-політолог. студії. 2023. Випуск 46, с. 187–195
Visnyk of the Lviv University. Series Philos.-Political Studies. Issue 46, p. 187–195

УДК 1:316.4(61)
DOI https://doi.org/10.30970/PPS.2023.46.23

ОСОБИСТІСТЬ ТА ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ: ФІЛОСОФСЬКИЙ КОМПЕНДІУМ СУЧАСНИХ КОНЦЕПТІВ

Олена Уваркіна
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
Інститут спеціального зв'язку та захисту інформації
вул. Верхньоключова, 4, 03056, м. Київ, Україна

Артур Гангал
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
Інститут спеціального зв'язку та захисту інформації
вул. Верхньоключова, 4, 03056, м. Київ, Україна

Наталія Волошина
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
Інститут спеціального зв'язку та захисту інформації
вул. Верхньоключова, 4, 03056, м. Київ, Україна

Стаття присвячена дослідженню сучасних проблем інформаційної безпеки особистості в умовах воєнного стану через філософський компендіум концептуального каркасу безпекового виміру феномену особистості. Зазначено, що дослідження інформаційної безпеки особистості в умовах воєнного стану постає актуальним, практично затребуваним і належить до нагальних питань національної безпеки. Визначено, що рефлексійне нашарування концептів інформаційної безпеки особистості, яке здійснювалось впродовж попередніх років, в наш час, потребує сучасної діагностики відповідно адекватності суспільним реаліям.

Стверджується, що наявність стратегічного наукового вакууму у питаннях запобігання безперервним світовим кіберінцидентам, які пов'язані з безпекою людини у процесі її кібердіяльності, потребує активізації прогресивного нормоутворення щодо кіберконкуренції на основі міжнародного співробітництва для створення універсального європейського стратегічного підходу до протидії ворожим кібернетичним діям. Доведено відсутність кон'юкційних претензій або понятійних демаркацій поняття «інформаційна безпека». З'ясовано, що амплітуда коливань концептуального каркасу інформаційної безпеки особистості конотаційно змінюється від традиційних структурно-функціональних моделей до інтенції сучасних кіберінновацій.

Рефлексія емпіричної інтерпретації темпоральних орієнтацій українців в умовах війни виявила парадоксальний приклад суб'єктності опитуваних особистостей, що виявляється у здатності усвідомлено і виважено приймати рішення навіть у надважких умовах, інколи нехтуючи власною безпекою.

Обґрунтовано, що динамічний континуум психологічних концептів визначається апріорним пієтетом до використання по відношенню до особистості терміну «інформаційно-психологічна безпека» та виявленню деструктивних інформаційних впливів як на особистість, так і на військових.

Ключові слова: особистість, інформаційна безпека, інформаційно-психологічна безпека особистості, воєнний стан.

Актуалізація питання інформаційної безпеки особистості безумовно пов'язано з експоненціальністю світового кіберпростору, проте в умовах воєнного стану амплітуда концептуальних точок зору на проблемний горізонт безпекових вимірів в тріаді «особистість-інформація-безпека» вбагатократ підвищила необхідність філософського компедіуму існуючих наукових парадигм та їх праксису.

В умовах воєнного стану та відсічі збройної агресії уважна рефлексія сучасних концептів інформаційної безпеки особистості доводить, що парадигмальна несумірність підходів визначається багаторівневим комплексом траєкторій дослідження, які завжди спрямовані на забезпечення захисту особистості від інформаційних впливів та інформаційної агресії, але не завжди адекватні суспільним реаліям.

Чимало зарубіжних дослідників кіберпростору визнають наявність стратегічного наукового вакууму у питаннях запобігання безперервним світовим кіберінцидентам, які пов'язані з безпекою людини у процесі її кібердіяльності. Розвиваючи ці дискусії, науковці шукають шляхи активізації прогресивного нормоутворення щодо кіберконкуренції на основі міжнародного співробітництва для створення універсального європейського стратегічного підходу до протидії ворожим кібернетичним діям. А під впливом подій у глобальної політиці, цифрових технологіях і стратегічної культурі пропонується розробка на мезорівні національних європейських стратегій, посилення кодифікації норм та правового поля кібербезпеки людини для захисту від зловмисної кумулятивної кібердіяльності та уникнення подальшого отруєння глобальної цифрової свердловини [1, с. 13–15].

Стратегії розвитку української інформаційної галузі також позначені багатьма труднощами і проблемними вузлами методологічного синтезу. Принагідно зауважимо, що тривалий час науковці розробляли концепцію державної інформаційної безпеки, основною метою якої був захист і розвиток національного інформаційного простору та всебічне інформаційне забезпечення українського суспільства. Нажаль, поданий у 2015 році проєкт концепції не набрав чинності, проте вже через рік була затверджена Доктрина інформаційної безпеки України.

Сьогодні, правовою основою сучасних вітчизняних концептів інформаційної безпеки особистості є Конституція України, Стратегія національної безпеки України (2020), Стратегія кібербезпеки України (2021), закони України, міжнародні договори, а також Стратегія інформаційної безпеки (далі – Стратегія), яка введена в дію Указом Президента України від 28 грудня 2021 року № 685/2021 та розрахована на період до 2025 року.

Слід зазначити про втрату чинності, у зв'язку з затвердженням Стратегії, попереднього Указу Президента України від 25 лютого 2017 року № 47 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [2].

На сучасну пору поняття «інформаційна безпека» визначається у Стратегії як «складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [2]».

Філософська рефлексія концептуального каркасу інформаційної безпеки *ad rem* не виявила кон'юкційних претензій або понятійних демаркацій зазначеного у Стратегії поняття «інформаційна безпека». Дослідників більш цікавить обґрунтування концептуальних положень для встановлення взаємозв'язку між об'єктами та суб'єктами інформаційної безпеки, розроблення її деталізованої концептуальної моделі [3], а також основні мейнстрими реалізації політики інформаційної безпеки держави в контексті національної безпеки [4].

У концепті інформаційної безпеки дослідника М. Гаврильціва увага сконцентрована на інформаційної безпекової стратегії у проблемному горизонті удосконалення нормативно-правової бази у сфері інформаційної політики держави та створення системи комплексного моніторингу публічного інформаційного простору для забезпечення «протидії руйнівному інформаційному впливу рф» [5, с. 203].

Достатньо переконливу аргументацію наводить у своїх дослідженнях А.Войцеховський, який розробляючи концепт інформаційної безпеки як складової системи національної безпеки та використавши міжнародний та зарубіжний досвід, визначає факт домінування у фаховому середовищі консенсусу про те, що «забезпечення інформаційної безпеки вже стало пріоритетним стратегічним завданням багатьох держав світу» і що інформаційна безпека у системі національної безпеки може розглядатися як самостійна частина [6, с. 288].

Безумовно, що в умовах воєнного стану безпекові стратегії посилюються теоретичними розробками на зміцнення воєнної безпеки та імплементації міжнародного досвіду для захисту національних інтересів держави у просторовому світі інформаційних загроз [7]. Нажаль, практичні шляхи реалізації цієї теоретичної концепції В. Школяренко не мають відкритого доступу у цілях національної безпеки в умовах воєнного стану.

На нашу думку, не менш важливою для концептуального каркасу інформаційної безпеки особистості в умовах воєнного стану є етична концепція інформаційних процесів (О. Проценко, Т. Чубіна, М.Дмитренко), яка має високий рівень дискутивності та варіативності, але у авторської версії у вигляді послідовності структурних компонентів інфоетики має ознаки респектабельності з позиції існуючих у фаховому середовищі стереотипів і водночас переконливої з міркувань інтерпретації солідності і доведеності.

Науково-теоретичний аналіз авторів дослідження інформаційної етики показав, що по-перше, етичні стратегії мають «практично-прикладний вимір»; по-друге, впливають «на репрезентацію особистості в мережевому просторі»; по-третє, етичні знання «заважають реалізації потворних інстинктів і схильностей, які мають наочні форми морального зла»; по-четверте, інфоетика «пов'язана з сучасною цифровою культурою та присутністю особистості в ній»; по-п'яте, існує «об'єктивна необхідність у механізмі регулювання мораллю цифрового простору» [8, с. 103]. На нашу думку, в умовах воєнного стану, м'яка примусовість моральних імперативів, об'єктивно замінюється більш жорсткими вимогами до поведінки в цифровому просторі завдяки нормам права, діючим у зв'язку з військовою агресією рф проти України.

Вимога філософської сумлінності потребує визнання, що конотація інформаційної безпеки у колах психологічної спільноти виявила апріорний пієтет до використання по відношенню до особистості терміну «інформаційно-психологічна безпека», який визначається дослідниками як «стан захищеності індивідуальної, групової та суспільної свідомості від впливу інформаційних факторів (загроз), викликаючи дисфункціональні процеси в суспільстві та в життєдіяльності окремої людини, здатні супротив її волі та бажання змінювати психічний стан і психологічні характеристики, модифікувати поведінку та обмежувати свободу вибору» [9, с. 228].

Сьогодні психологи актуалізують проблеми інформаційно-психологічної безпеки особистості в умовах війни для протидії негативному інформаційному впливу, який «має надзвичайно деструктивний характер і може призводити до непередбачуваних наслідків» [10, с. 106]. Тому у дослідженнях акцентується увага як на встановленні ролі психологічних механізмів інформаційного впливу на особистість, так і на вивченні деструктивних інформаційних впливів на військових під час виконання обов'язків служби.

Попри те, що основні напрями протидії негативному інформаційно-психологічному впливу серед військових були розроблені ще до збройній агресії рф, у публікаціях під час війни (В. Алещенко, А. Уманець) цілком природно рефлектуються безпекові патерни для поточної реальності в умовах воєнного стану та актуалізується розробка сучасного комплексу заходів, спрямованих на розвиток особистісних якостей військових, необхідних для якісної нейтралізації дії негативних інформаційних факторів [10, с. 106].

Слід зазначити, що у деяких психологічних дослідженнях, які присвячені інформаційної безпеці, пропонуються структурно-функціональні моделі інформаційно-психологічної безпеки особистості (В. Алещенко, О. Панченко, А. Кабанцева), які показують динаміку роботи системи, починаючи від джерел інформаційних загроз і закінчуючи способами захисту психічних ресурсів особистості.

Наприклад, модель інформаційно-психологічної безпеки особистості дослідників О. Панченко, А. Кабанцева складається: з джерел інформаційних ризиків (офіційних і неофіційних); з особливостей інформації (повнота, доступність, наявність маніпулятивнх елементів); з свідомих та безсвідомих компонентів психіки особистості та з рівня ресурсів особистості (високий, середній, низький) [9, с. 230]. На превеликий жаль, заявлена та опублікована у 2022 році модель інформаційно-психологічної безпеки особистості професора В. Алещенко [11. с. 18]. виявилась повною копією, раніше опублікованої в 2020 році, моделлю О. Панченко, А. Кабанцева [9, с. 230]. Безперечно, що цей факт відчутно пауперизує вірогідно-ймовірнісно-евентуальний когнітивний щабель запропонованих моделей у науковому середовищі та їх змістовне вивчення

На нашу думку, безпековий вимір концепції інформагенезу особистості відомого науковця, лікаря П. Назара, заслуговує на особливу компліментарність, завдяки оперуванню проблемними аспектами та теоретико-праксеологічними неузгодженостями в сучасному інформаційному просторі. Дослідник стверджує, що нівелюючи старі загрози для розвитку особистості, інформаційне суспільство породжує нові, набагато небезпечні для прав і свобод особистості та тотальні в сенсі контролю над діяльністю людини. Науковець зазначає, що інформагенез «зачіпає ще один важливий аспект, як розуміння і реальне співвідношення рівності і нерівності». Йдеться про постійне розширення горизонтів доступності для особистості в інформагенезе та створення інформаційно-безпекових можливостей у віртуальної реальності [12, с. 68]. Рефлектуючи з приводу цього аспекту, слід зазначити, що однією з особливостей сучасної особистості є її здатність швидко адаптуватися до змін безпекового середовища й створювати безпечні умови власної життєдіяльності, використовуючи соціальні, інтелектуальні, особистісні та фізичні ресурси.

З цих міркувань, розглядаючи концепт особистості з позицій криптографії, для дешифрування розлогого проблемного горизонту інформаційної безпеки особистості, доводитися констатувати наявність тісного зв'язку криптограми особистості та інформації. Видається, що під впливом експоненціальної інформатизації суспільства особистість елімінує старі знаки і символи, оновлює свій інформаційний тезаурус, виявляє складні символи логічних якісних змін, котрі поступово стають новим потенціалом для її розвитку та зміцнення. Так склалося, що об'єктивно порівнюючи зовнішні на внутрішні фактори

впливу на зміни у структурі особистості, ми визнаємо, що є небезпека негативного впливу інформації на ціннісний підмурівок людини [13, с. 131]. Зокрема, чимало науковців визнають, що без впровадження безпекових інформаційних заходів зі збільшенням потоків інформації «існує реальна небезпека поглинання або розмивання традиційної системи цінностей суспільства», «небезпека нечесних стосунків, взаємного використання, експлуатації [14, с. 29, 31]».

Однак, небезпека змін у змістовних характеристиках особистості не обмежується ціннісними аспектами проблеми. Діюча Стратегія інформаційної безпеки приділяє особливу увагу забезпеченню прав та свобод людини в інформаційній сфері. Наприклад, коли в умовах «збільшення кількості соціальних мереж, їх інтегрованість з іншими соціальними сервісами повсякденного користування, а також специфіка організації всесвітньої мережі Інтернет ставлять під загрозу гарантії права особи на приватність», виявляється «недостатній рівень медіаграмотності (медіакультури)», що «супроводжується зменшенням критичності сприйняття інформації та створенням «підґрунтя для можливих маніпуляцій громадською думкою». Тому для підвищення рівня медіакультури та медіаграмотності у Стратегії пропонується «проведення просвітницької кампанії з медіаграмотності, що включатиме такі компоненти, як розвиток критичного мислення, навички перевірки фактів і визначення маніпуляційних технік, ознайомлення з найпоширенішими порушеннями прав людини із застосуванням інтернет-технологій тощо [2]». Така повага до інформаційної безпеки особистості та захисту її прав є апостеріорним свідченням того, що відбувається активна взаємодія людей і суспільства у конгломераті номократичного (керованого правом) та теократичного (керованого метою) соціального порядку для досягнення суспільного оптимуму у питаннях безпеки.

Хочеться нагадати, що прикладом виконання зазначеного у Стратегії завдання є започатковані Інститутом спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського (Далі – Інститут) відкриті уроки на тему «Вступ до кібергігієни» в школах України. Ця соціальна ініціатива, яка була запланована на час проведення у жовтні щорічного Місяцю кібербезпеки, була продовжена і в умовах воєнного стану. Науково-педагогічні працівники Інституту спільно з курсантами проводять онлайн-уроки з кібергігієни та ознайомлюють учнів з основними принципами зменшення ризиків у інформаційному просторі та основам протидії негативному інформаційному впливу. Звернемо увагу, що в опублікованих Інститутом матеріалах конференції «Кібербезпека державних інституцій та подолання кризових станів» (2022) зазначається, що «за час проведення занять «Вступ до кібергігієни» було охоплено понад 15000 учнів» та уроки з кібергігієни виявили значний інтерес з боку педагогів та батьків учнів. [15, с. 242]. Це, безперечно, один з шляхів досягнення третьої стратегічної цілі Стратегії інформаційної безпеки про підвищення рівня медіакультури та медіаграмотності суспільства та його захисту від деструктивного впливу дезінформації й маніпулятивної інформації перед широким спектром загроз, зокрема в інформаційній сфері.

Зрозуміло, що сучасний вектор забезпечення інформаційної безпеки особистості визначається особливостями запровадженого воєнного стану, які характеризуються високим ступенем невизначеності і непередбачуваності та створюють дефіцитарність ознак безпеки. Крім того, іманентна персоніфікація дефініції інформаційної безпеки особистості передбачає об'єктивну та суб'єктивну оцінку можливих загроз.

За даними опитування, яке було проведене на третьому місяці війни, у період активний бойових дій на території України, незалежно від наявних загроз життю, з якими 83% учасників анкетування вже зіткнулися (проживання в фронтових, прифронтових,

окупованих місцях), 55,6% респондентів відповіли, що попри все мають довгострокові плани на 2–5 років з відповідною корекцією на терміни закінчення військових дій. Авторка емпіричних інтерпретацій темпоральних орієнтацій українців в умовах війни О.Гончарова стверджує, що позиція «мої плани попри все» є невротичною і доволі небезпечною для психічного здоров'я респондентів. Дослідниця впевнена, що «це один з симптомів того, що людина насправді не адаптувалася до ситуації війни, не включила війну в свою реальність як явище, з яким треба миритися» [16, с. 12]. Проте, на нашу думку, це є прикладом суб'єктності опитуваних особистостей, які і під час війни намагаються дотримуватися свідомого вибору та зберігають здатність усвідомлено і виважено приймати рішення навіть у надважких умовах. Безумовно, така темпоральна орієнтація була б неможливою без впевненості у перемогу та віри у міцність збройних сил України.

Така впевненість також об'єктивно підсилює прагнення 73,9% респондентів «бачити нові перспективи для України, новий політичний курс та велике будівництво» після закінчення війни та залишає у меншості (7,8%) «потенційно ризиковану когорту людей», які не будують довгострокових планів на майбутнє і «можуть потерпати від глибокої екзистенційної кризи» та фрустрації [16, с. 12]. Розуміючи застереження О.Гончарової від «застрягання» «пересічних опитуваних» на поточному моменті трьох місяців війни, сьогодні, у річницю військової агресії рф проти України, дозволимо гіпотетично припустити, що рівень готовності дати відсіч інформаційним загрозам та забезпечити безпеку особистості має експоненціальний ефект можливостей до телеологічності та праксису.

Сьогодні інформаційний фронт виступає одним з напрямків національного опору збройній агресії проти України. Концепція п'ятивимірної війни на суходолі, в морі в повітрі, в космосі та в кіберпросторі визнається НАТО вже у праксиологічному вимірі на прикладі України. Тому, як справедливо зазначає міністр закордонних справ України, український дипломат і комунікатор Дмитро Кулеба, «треба визнати: комунікативний простір є такою ж частиною держави, як земля, повітря і вода». У цьому контексті він впевнений, що «інформація завжди була складовою війни», а «привнесена технологіями новизна полягала лише в тому, що можливості комунікативного впливу на ворога зрівнялися й перевищили можливості збройного впливу». У своєї праці автор наводить вислів, про те що «під час війни найвищим пріоритетом буде не доступ до технологій, а управління інформацією» та передбачає координування інформаційних потоків через спеціальні центри керування для вирішення проблем забезпечення інформаційної безпеки особистості під час воєнного стану. У своїх висновках Д.Кулеба впевнений, що «безпека країни закінчиться там, де Україні перестануть вірити її ж громадини та міжнародні партнери» [17, с. 328–347]. Така авторська субстанційність щодо інформаційної парадигми в умовах війни, на нашу думку, конвенційно має стати аксіоматикою реалій сьогодення та суспільної еволюції.

Отже, підводячи результуючу риску під філософським компендіумом концептуальних проблем інформаційної безпеки особистості, до очевидних переваг і здобутків наукової спільноти можна віднести, завперш, наявність сучасного правового поля вітчизняних концептів інформаційної безпеки особистості, яке запобігає термінологічним неузгодженостям та парадоксальним синтезам, відкривая надзвичайно широкий горизонт для повноцінного наукового дискурсу. Щоправда, треба зазначити, що зоднобіч превалює апріорний пієтет до змістовного визначення терміну «інформаційна безпека», а здругобіч, відчувається потреба у кон'юкції основних та нових понятійних конструктів в категорії «інформаційно-психологічна безпека особистості». Варто зауважити, що варіативність концепту інформаційної безпеки особистості продовжує перебувати в епіцентрі соціально-філософського дискурсу і в наш час поповнився концепціями криптограми

та інформагенезу особистості. а також дослідженнями інформаційної етики. Аналіз емпіричних інтерпретацій об'єктивних та суб'єктивних орієнтацій українців в умовах воєнного стану показав, що сучасна особистість свідомо сприймає темпоральні зміни, які спричинила війна, але неуклінно зосереджена на майбутньому, інколи, нехтуючи власною безпекою, сподіваючись на захист своїх прав і свобод військовими, які щодобово знаходяться на бойових позиціях, дають відсіч ворогу і дають можливість, в такий складний час для країни, представляти наші когнітивні коди безпеки сучасності у інформаційному науковому просторі.

Список використаної літератури

1. Liebetrau Tobias. Cyber conflict short of war: a European strategic vacuum, *European Security*, 2022. p. 1–20. https://doi.org/10.1080/09662839.2022.2031991
2. Рішення Ради національної безпеки і оборони України «Про Стратегію інформаційної безпеки України» від 15 жовтня 2021 року. Указ Президента України від 28 грудня 2021 року №685/2021. URL: https://www.president.gov.ua/documents/6852021-41069#:~:text
3. Дзюба Т.М. Обґрунтування концептуальних положень інформаційної безпеки України. *Наука і оборона*. 2021. №3. https://doi.org/10.33099/2618-1614-2021-16-3-41-46
4. Князєв С.О. Іінформаційна безпека України в контексті національної безпеки. *Інформаційна безпека людини, суспільства, держави.* 2021. № 1-3 (31–33). С. 81–88. URL: http://journals.uran.ua/ispss/article/view/260247/256605
5. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал*. 2020. №2. с. 200–203. https://doi.org/10.32782/2524-0374/2020-2/52
6. Войціховський А.В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «ПРАВО».* 2020. Випуск 29. с. 281–288. https://doi.org/10.26565/2075-1834-2020-29-38
7. Школяренко В.В. Шляхи зміцнення воєнної безпеки України в умовах повномасштабного вторгнення Росії в Україну. *Наука і оборона*. 2022. №2. https://doi.org/10.33099/2618-1614-2022-19-2-3-9
8. Проценко О., Чубіна Т., Дмитренко М. Етика та інформаційна етика у комунікативному просторі сучасного суспільства. *Вісник Львівського університету. Серія філос.-політолог. студії.* 2022. Випуск 44, с. 98–104. https://doi.org/10.30970/PPS.2022.44.11
9. Панченко О.А., Кабанцева А.В. Людська психіка в інформаційній небезпеці. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління.* 2020. Том 31(70) № 3. С. 226–233. https://doi.org/10.32838/TNU-2663-6468/2020.3/39
10. Уманець А.О. Інформаційно-психологічні впливи: поняття, особливості реалізації та способи протидії. Вчені записки ТНУ імені В.І.Вернадського. Серія: Психологія. 2022. Том 33(72) № 3. С. 106–112. https://doi.org/10.32838/2709-3093/2022.3/18
11. Алещенко В. Інформаційно-психологічна безпека особистості в умовах гібридної війни. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки.* 2022. Випуск 1 (49). С. 13–21.
12. Назар П.С.Філософія людини та особистості. Київ : Сталь, 2018. 578 с.
13. Уваркіна О. Криптограма особистості: знаки та символи сучасних змін. *Вісник Львівського університету. Серія філос.-політолог. студії.* 2021. Випуск 35, с. 129–134. https://doi.org/10.30970/PPS.2021.35.15
14. Білоус В. Зміни потреб особистості під впливом сучасних технологій у нестабільному суспільстві. *Вісник Львівського університету. Серія філос.-політолог. студії.* 2020. Випуск 29, С. 27–32. DOI https://doi.org/10/30970/PPS.2020.29.3

15. Пучков О.О., Конюшок С.М. Роль обізнаності громадян у сфері кібербезпеки в умовах кризи: досвід ІСЗЗІ КПІ ім. Ігоря Сікорського. Матеріали І Міжнародної науково-практичної конференції «Кібербезпека державних інституцій та подолання кризових станів» Київ : ІСЗІІ КПІ ім. Ігоря Сікорського, 2022. С. 241–242.
16. Гончарова О. Темпоральні орієнтації українців в умовах війни: минуле, теперішнє та майбутнє крізь призму військової агресії РФ. *Вісник Львівського університету. Серія філос.-політолог. студії.* 2022. Випуск 43, С. 9–17. https://doi.org/10.30970/PPS.2022.43.1
17. Кулеба Д. Війна за реальність: як перемагати у світі фейків, правд і спільнот. Київ : Книголав, 2022. 384 с.

PRIVACY AND INFORMATION SECURITY IN THE CONDITIONS OF WAR: A PHILOSOPHICAL COMPENDIUM OF MODERN CONCEPTS

Olena Uvarkina
National Technical Unversity of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute»,
Institute of Specialized Communication and Information Security
Verkhneklyuchova str., 4, 03056, Kyiv, Ukraine

Artur Hanhal
National Technical Unversity of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute»,
Institute of Specialized Communication and Information Security
Verkhneklyuchova str., 4, 03056, Kyiv, Ukraine

Natalya Voloshyna
National Technical Unversity of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute»,
Institute of Specialized Communication and Information Security
Verkhneklyuchova str., 4, 03056, Kyiv, Ukraine

The article is devoted to the study of modern problems of information security of the individual in the conditions of martial law through the philosophical compendium of the conceptual framework of the security dimension of the phenomenon of the individual. It is noted that the study of the information security of the individual in the conditions of martial law becomes relevant, practically in demand and belongs to the urgent issues of national security. It was determined that the reflexive layering of the concepts of information security of the individual, which was carried out during the previous years, in our time, needs modern diagnostics according to the adequacy to social realities.

It is argued that the existence of a strategic scientific vacuum in the issues of preventing continuous global cyber incidents, which are related to the safety of a person in the process of his cyber activities, requires the activation of progressive norm-making regarding cyber competition on the basis of international cooperation to create a universal European strategic approach to countering hostile cyber actions. The absence of conjunctive claims or conceptual demarcations of the concept of "information security" has been proven. It was found that the amplitude of fluctuations of the conceptual framework of the information security of the individual changes from traditional structural and functional models to the intention of modern cyber innovations.

It is substantiated that the dynamic continuum of psychological concepts is determined by the a priori piety to the use of the term "informational and psychological security" in relation to the individual and the detection of destructive informational influences on both the individual and the military.

The reflection of the empirical interpretation of the temporal orientations of Ukrainians in the conditions of war revealed a paradoxical example of the subjectivity of the interviewed personalities, which is manifested in the ability to consciously and carefully make decisions even in extremely difficult conditions, sometimes neglecting one's own safety.

Key words: personality, information security, informational and psychological security of the individual, martial law.