групової інформованості про значущі елементи навколишнього дійсності.

Середовище діяльності складають сфера домінування і некерована сфера. До сфери домінування відносять кошти, якими володіє суб'єкт діяльності, і елементи навколишньої дійсності, на які вона може впливати.

Некеровану сферу утворює група елементів, на які суб'єкт діяльності не може впливати, але які необхідно враховувати у вигляді обмежень [1].

Актуальні питання в сфері підготовки фахівців

У ході дослідження узагальнено різні підходи науковців щодо моделей підготовки фахівців у галузі інформаційних технологій для оперативних підрозділів Національної поліції. Зокрема запропоновано створити у закладах вищої освіти зі специфічними умовами навчання МВС України:

Відповідні спеціалізації курсантів, у рамках яких разом з юридичними спеціальними дисциплінами поглиблено вивчати спеціальні технічні дисципліни у галузі інформаційних технологій;

Відповідні групи слухачів-правоохоронців, які вже мають вищу технічну або економічну освіту у галузі інформаційних технологій, з метою поглибленого вивчення ними спеціальних юридичних дисциплін.

За результатами опитування 180 практичних працівників оперативних та інформаційно-аналітичних підрозділів Національної поліції визначено пріоритетні моделі підготовки фахівців у галузі інформаційних технологій для оперативних підрозділів.

Всі ці підходи мають право на існування, єдине, що має їх об'єднувати, – це ретельний відбір кандидатів на навчання. Водночас необхідно враховувати особливості відбору та підготовки фахівців для підрозділів Департаменту кіберполіції Національної поліції України [2].

1. Інформаційні технології в діяльності національної поліції України //вебсайт. URL: https://journalnam.com.ua/index.php/journal/article/download/339/325 (дата звернення: 02.03.2023).

2. Модель підготовки фахівців у галузі інформаційних технологій для органів національної поліції України// вебсайт. URL:

3. https://www.researchgate.net/publication/331405709_model_pidgotovki_fahivciv_u_galuzi_informacijnih_tehnologij_dla_organiv_nacionalnoi_policii_ukraini (дата звернення 20.11.2022).

УДК 004
DOI: 10.31733/17-03-2023-586-588

Тарас ПРОКОПЧУК
здобувач магістерського рівня вищої освіти Національного університету водного господарства та природокористування, м. Рівне

ІНФОРМАЦІЙНА БЕЗПЕКА: СУЧАСНІ ВИКЛИКИ ТА ЗАГРОЗИ

В умовах сучасних глобальних та регіональних інформаційних протистоянь, деструктивних комунікативних впливів, зіткнення різновекторних національних інформаційних інтересів, поширення інформаційної експансії та агресії, захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними стратегічними завданнями сучасних держав у системі глобальних інформаційних відносин. Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою і для України, яка часто є об'єктом зовнішньої інформаційної експансії, маніпулятивних пропагандистських технологій та руйнівного інформаційного вторгнення. В умовах збройної агресії рф захист національного інформаційного простору від негативних інформаційно-психологічних впливів, гарантування інформаційної безпеки та інформаційного суверенітету набувають особливого значення і стають чинниками збереження національної ідентичності України та функціонування її як суверенної та незалежної держави.

Метою теми «Інформаційна безпека: сучасні виклики та загрози» є дослідження проблем у сфері інформаційних відносин, формування інформаційних ресурсів і

користування ними в Україні, а також шляхів їх вирішення з метою забезпечення національної безпеки нашої держави.

Значення інформації для людини, суспільства, держави відзначається ще за часів Античності, а перші згадки про інформаційну безпеку сягають корінням сивої данини. Наприклад, ще другий Цар єдиного Ізраїльського царства Давид, який правив приблизно у 1010 – 970 роках до нашої ери, у своїй молитві промовляв: "Ти погубиш тих, хто говорить брехню; кровожерним і підступним гребує Господь". Якщо розмірковувати над цим виразом через призму сучасних інформаційних процесів, під брехнею можна розуміти "дезінформацію" чи "недостовірну інформацію".

Із розвитком інформаційного суспільства, збільшенням обсягу інформації, до якої людина отримує доступ легко та без особливих зусиль, рівень та кількість інформаційних загроз, швидкість їх розповсюдження та масштабність можливих наслідків зростає.

Таким чином, актуальність забезпечення інформаційної безпеки України, особливо в умовах інформаційної агресії, з кожним днем збільшується, а її ефективне нормативно-правове регулювання стає життєво необхідним для забезпечення суверенітету держави.

Інформаційна безпека є одним із найважливіших чинників національної безпеки України. Інформаційна і національна безпека повною мірою узгоджуються і співвідносяться між собою за схемою «частина» і «ціле». Сьогодні інформаційна складова не існує поза межами загальної національної безпеки, так само, як і національна безпека не буде всеохоплюючою без інформаційної безпеки. Загальним підґрунтям цих понять є, безумовно, поняття «безпека», що обумовлює стан захищеності життєвих інтересів людини як особистості, суспільства, держави. Сьогодні їх слід розглядати у геополітичному вимірі як невід'ємну частину державної політики із системою заходів економічного, політичного, організаційного та іншого спрямування, які адекватні загрозам життєво важливим інтересам громадян, суспільства і держави саме в такому контексті.

Тобто, інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

Інформаційна безпека є складним, системним і багаторівневим феноменом, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні і внутрішні чинники, найважливішими з яких є: політична обстановка у світі; наявність потенційних зовнішніх і внутрішніх загроз; стан і рівень інформаційно-комунікаційного розвитку країни; внутрішньополітична обстановка в державі тощо.

Суть інформаційної безпеки полягає у захисті інформаційного простору України від небажаного інформаційного впливу, захисті національних інформаційних ресурсів, забезпеченні безпечного функціонування інформаційних та телекомунікаційних систем, а також у захисті інформації, що циркулює в них. Тому основними системоутворюючими складовими інформаційної безпеки є: захист інформаційного простору; захист інформації з обмеженим доступом; захист інформаційних ресурсів.

До об'єктів інформаційної безпеки відносять свідомість, психіку людей або різноманітні інформаційні системи, які складають інформаційну інфраструктуру держави, а у соціальній сфері – особистість, колектив, суспільство та держава (її конституційний лад).

До суб'єктів інформаційної безпеки відносяться: держава, що здійснює свої функції через відповідні органи державної влади шляхом створення системи забезпечення інформаційної безпеки; громадяни, суспільні або інші організації і об'єднання, що володіють повноваженнями із забезпечення інформаційної безпеки відповідно до законодавства.

Основні цілі забезпечення інформаційної безпеки визначаються пріоритетами національної безпеки, що відповідають інтересам суспільного розвитку, а саме:

- забезпечення інформаційного суверенітету України в умовах глобалізації інформаційних відносин і прагнення інших країн до інформаційного домінування;
- формування інформаційного середовища, орієнтованого на духовний та інтелектуальний розвиток особи і суспільства в цілому;
- підтримка необхідної достатності інформаційних ресурсів України, які забезпечують розвиток особи та стійке функціонування суспільства і держави;
- забезпечення захисту інформації фізичних, юридичних осіб та держави від зовнішніх і внутрішніх інформаційних загроз, у тому числі боротьба з комп'ютерними

злочинами;

- забезпечення законності і реалізація прав суб'єктів інформаційних відносин у галузі створення і використання національних інформаційних ресурсів, інформаційних технологій та інформаційної інфраструктури.

Саме тому, з урахуванням зазначених вище факторів, державна політика у сфері інформаційної безпеки повинна реалізовуватись шляхом створення відповідної нормативно-правової бази, яка регулює відносини в сфері інформаційної безпеки, встановлює вимоги і правила провадження діяльності у цій сфері.

Життєва практика переконує, що на сьогодні жодна держава не в змозі захистити себе, використовуючи лише військово-технічні засоби. Забезпечення безпеки стає комплексним завданням, до якого входять політичні, економічні, інформаційні та інші заходи. Успішно вирішувати це завдання вдається завдяки оптимальному застосуванню усіх форм та засобів протиборства, включаючи й інформаційне. У багатьох економічно розвинутих державах відбувається об'єднання в одне ціле сил та засобів інформаційно-психологічного впливу, призначених для досягнення воєнних, ідеологічних і політичних цілей.

Проти України широко використовують сучасні технології негативних інформаційно-психологічних впливів, які стають загрозою українському національному інформаційному простору та суверенітету держави. Гарантування інформаційної безпеки України в умовах дестабілізувальних негативних інформаційно-психологічних впливів та експансіоністської агресивної інформаційної політики рф, потребує консолідації зусиль на усіх рівнях державної влади та громадянського суспільства.

Як протидія масштабним негативним інформаційно-психологічним впливам, операціям та війнам, пріоритетними напрямами державної інформаційної політики та важливими кроками з боку владних органів України мають бути: 1) інтеграція України до світового та регіонального європейського інформаційного просторів; 2) інтеграція у міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації; 3) створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства; 4) модернізації усієї системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики; 5) удосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів; 6) розвиток національної інформаційної інфраструктури; 7) підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг; 8) впровадження сучасних інформаційно-комунікативних технологій у процеси державного управління; 9) ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригуванні державної політики в інформаційній сфері.

Отже, в умовах сучасних інформаційних протистоянь, експансіоністської політики рф, національний інформаційний простір України є недостатньо захищеним від зовнішніх негативних пропагандистських інформаційно-психологічних впливів, загроз. Тому захист інформаційного суверенітету, створення потужної та ефективної системи інформаційної безпеки України, розроблення дієвих стратегій і тактик протидії медіа-загрозам повинні стати пріоритетними завданнями органів державної влади та недержавних інститутів.

---

1. Гріщенко А.О. Підходи до розуміння категорії "інформаційна безпека" та правові засади її забезпечення. Інформація і право. № 4(35)/2020. С. 119-133.

2. Корнейко О., Корнейко С. Застосування та визначення терміну «інформаційна безпека» в національному законодавстві. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2(19) вип., 2009 р. С. 9-13.

3.Інформаційна безпека (соціально-правові аспекти): Підручник/Остроухой Б.В., Петрик Б.М., Присяжнюк М. М. та ін. ; за заг- ред. Є.Д. Скулиша. - К- : КНТ, 2010.

4. Ільницька У. Інформаційна безпека україни: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Політичні науки, Vol. 2, No. 1, 2016 С. 27-32.

5. Інформаційна безпека. Підручник/В.В. Остроухов, М.М. Присяжнюк, О.І. Фармагей, М.М. Чеховська та ін.; під ред. В.В.Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.