людину з зовсім іншими цінностіми та навіть власною ідентичністю. Цьому також сприяє упередження – схильність людини до сприйняття інформації, що підтверджує її власні переконання та ігнорування тієї інформації, що цим переконанням суперечать. Це самоізоляція у певному колі однодумців. Відповідним визначенням для таких груп є – «зона власного комфорту» [4].

Розглядаючи дану тему, обов'язково варто зупинитися на такому інструменті як пропаганда. Хоча, це фактично є певною моделлю побудови інформації та її використання. Варто зауважити, що агресивного використання. Науковці Е. Херман та Н. Хомскі, вказували, що пропаганда є фактично зброєю і за наявності зосередженої в певних руках влади, призводить до вибірковості та фільтрації новин [5, с.102]. ЗМІ фактично втрачають незалежність, оскільки вони «служать і пропагують від імені потужних суспільних інтересів, які контролюють та фінансують їх». А у випадку сучасної доступності медіа ресурсу (фактично в кожного у кишені), маніпуляції теж спрощуються і впливають на кожну сферу життя – від політичних переконань, до побудову родинних стосунків та кулінарії. У психології це пояснюється Фактором сенсаційності та скандальності [4]. Сенсація має умовно пріоритетний попит у споживачів та користується підвищеною увагою останніх. Чим скандальніша новина, тим менше її перевірятимуть, аби ніхто не спростував. Схильність до ілюзорної істини — багаторазове повторення певної інформації сприяє формуванню думки щодо її істинності та правдивості, навіть коли людина напевно знала реальний стан речей, особливо без можливості критично та детально розглянути питання [4].

Наразі, фіксується тенденція до зниження довіри до ЗМІ, однак, є одне «Але»! Мова йде про традиційні засоби масової інформації. Так, дослідники звертають увагу на те, що 68% громадян є активними користувачами соціальних мереж для отримання новин. І цей показник постійно зростає [6].

Таким чином, можемо зробити висновок, що ми фактично перебуваємо у перехідному етапі народження нового типу людини – mediasapiens, для якої характерні не те що інші цінності, а вони взагалі є дуже пластичними і залежними від того, хто сьогодні авторитет у його кишені. І саме з цими викликами сучасності нам варто боротися, хоча, багато в чому вже запізно.

1. Мак-Люен, Маршалл. Галактика Гутенберга: становлення людини друкованої книги / М. Мак-Люен ; пер. з англ. В. І. Постнікова, С. В. Єфремова. — К. : Ніка-Центр, 2001. — 464 с. — С.23.

2. Дослідження про соціальні мережі: [Електронний ресурс] - Режим доступу: www.applied-research.ru

3. Психологічні аспекти пов'язані з пост правдою: [Електронний ресурс] – Режим доступу: wikiwand.com

4. Виробництво згоди. Політична економія мас-медіа: JeffGoodwin. What's Right (And Wrong) about Left Media Criticism? Herman and Chomsky's Propaganda Model // Sociological Forum / Edward S. Herman, Noam Chomsky. — 1994. — Т. 9, вип. 1. — С. 101–111.

5. Данні соціологічного опитування: [Електронний ресурс] – Режим доступу: https://www.ukrinform.ua/rubric-society/2803560-dovira-ukrainciv-do-zmi-za-rik-znizilasa-na-11.html

УДК 004
DOI: 10.31733/17-03-2023-572-574

Даніела ГОЛУБЄВА
курсант ННІ права та підготовки
фахівців для підрозділів Національної поліції
Дніпропетровського державного
університету внутрішніх справ

СТРАТЕГІЇ ЗАХИСТУ: РОЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У сучасному світі, коли інформаційні технології досягають високих рівнів розвитку, національна безпека неможлива без забезпечення інформаційної безпеки. Кібератаки, кібершпигунство, кібертероризм і кіберзлочинність можуть серйозно підривати національну безпеку, тому в кожній країні необхідно розробляти стратегії захисту, які

включають заходи з інформаційної безпеки. У даному науковому дослідженні буде розглянута роль інформаційної безпеки у забезпеченні національної безпеки та розробка стратегій захисту.

Забезпечення інформаційної безпеки стає все більш важливим завданням для країн у сучасному світі. Розвиток технологій та Інтернету призвів до того, що національні інформаційні ресурси стають дедалі більш уразливими перед злочинними та терористичними організаціями. Це створює небезпеку для національних інтересів та підкреслює необхідність розробки та впровадження ефективних заходів забезпечення інформаційної безпеки. З метою захисту національних інтересів країні необхідно виявляти та аналізувати загрози, розробляти та впроваджувати адекватні заходи відповіді на них, та вважати захист інформації пріоритетним державним завданням [1].

У сучасному світі, інформаційна безпека є ключовою у забезпеченні життєво важливих інтересів країни. Розвиток технологій та Інтернету зробив національні інформаційні ресурси дедалі більш уразливими перед злочинними та терористичними організаціями, що створює небезпеку для національних інтересів. Це вимагає розробки та впровадження ефективних заходів забезпечення інформаційної безпеки, щоб захистити національні інтереси. Розробка та виконання адекватних заходів відповіді на загрози є необхідним для країни пріоритетним державним завданням. Тому, з метою захисту національних інтересів, важливо виявляти та аналізувати загрози інформаційної безпеки та розробляти необхідні заходи для їх протидії. При цьому, необхідно враховувати не тільки загрози з боку іноземних держав, терористичних організацій, кримінальних груп та зловмисників, а й внутрішні загрози, такі як кіберзлочини, хакерські атаки та інші небезпечні дії з боку власних громадян і організацій [2].

Інформаційна безпека визначається як стійкість інформаційних систем та даних від незаконного доступу, втрати, порушення цілісності, зміни та розповсюдження. Для забезпечення цієї безпеки необхідний високий рівень технічних, організаційних та правових заходів. Інформаційна безпека є необхідною для захисту національних інтересів та забезпечення національної безпеки [1, 3].

Забезпечення національної безпеки залежить від багатьох факторів, таких як захист від зовнішньої агресії, економічний розвиток, захист прав людини та свободи слова, політична стабільність, інформаційна безпека тощо. Інформаційна безпека є ключовою для забезпечення національної безпеки, оскільки вона включає в себе захист інформації, яка є важливою для національних інтересів.

Стратегії захисту повинні бути розроблені з метою захисту національних інтересів та забезпечення національної безпеки від кіберзагроз. Ці стратегії мають включати технічні, організаційні та правові заходи, які мають бути прийняті на рівні держави, органів влади, підприємств та громадян [2].

Технічні заходи полягають у забезпеченні безпеки інформаційних систем, мереж та даних. Це включає в себе застосування захисного програмного забезпечення, шифрування даних, встановлення захисних мережевих систем, захисту від DDoS-атак та інших методів захисту від кібератак [2, 3].

Організаційні заходи передбачають розробку політики безпеки інформації, регулярне проведення навчання та тренінгів з питань безпеки інформації, а також забезпечення відповідного контролю за дотриманням правил та стандартів безпеки [3].

Правові заходи включають у себе розробку законів та нормативно-правових актів, що стосуються інформаційної безпеки, визначення відповідальності за порушення правил та стандартів безпеки, а також забезпечення відповідного контролю за дотриманням цих норм [3].

Окрім цього, у стратегії захисту необхідно враховувати глобальний характер кіберзагроз та співпрацювати з іншими державами та міжнародними організаціями в області кібербезпеки. У забезпеченні національної безпеки важливо не тільки реагувати на кіберзагрози, але й активно працювати над їх передбаченням та запобіганням, забезпечуючи стійкість інформаційної інфраструктури та ефективне управління кризовими ситуаціями в цій сфері [4].

Особливу увагу в стратегії захисту необхідно приділяти критичним інфраструктурам, таким як електропередача, транспортна мережа, банківська система, медична допомога та інші. Захист цих інфраструктур від кібератак є важливим завданням національної безпеки [3].

Окрім того, важливо забезпечити захист інформаційної безпеки на рівні громадян, зокрема у сфері електронних фінансів, онлайн-платежів та інтернет-банкінгу. Для цього необхідно забезпечити належний рівень безпеки інтернет-сервісів та навчати громадян

правилам безпеки в мережі Інтернет [3].

Сьогодні, в оборонній сфері, інформаційні ресурси та інформаційна структура оборонного потенціалу країни, яка включає в себе збройні сили та військово-промисловий комплекс, є одними з найважливіших об'єктів безпеки. Сучасні засоби озброєння, військова техніка, системи управління військами та зброєю, є системами критичних додатків з високим рівнем комп'ютеризації, що робить їх дуже вразливими до впливу інформаційної зброї, як у військовий, так і у мирний час.

Ці системи можуть стати предметом атак з використанням програмних закладок, що може призвести до повного або часткового блокування зброї стримування країни до моменту загрозливої ситуації. Така загроза стає дедалі більш актуальною з кожним роком, як свідчить досвід локальних воєн останніх років. Тому, забезпечення безпеки інформаційних ресурсів та структури оборонного потенціалу стає надзвичайно важливим завданням в оборонній сфері [4, 5].

Отже, стратегії захисту є важливим інструментом у забезпеченні національної безпеки від кіберзагроз. Вони мають включати технічні, організаційні та правові заходи, спрямовані на захист інформаційних систем та даних, розробку політики безпеки інформації, підвищення рівня свідомості та навичок громадян з питань безпеки в Інтернеті, співпрацю з іншими державами та міжнародними організаціями в області кібербезпеки, а також захист критичних інфраструктур від кібератак. Забезпечення інформаційної безпеки є невід'ємною складовою національної безпеки, і від цього залежить не тільки ефективне функціонування держави, а й безпека громадян та їхніх прав і свобод.

1. Бєлай С. В., Корнієнко Д. М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою держави. Київ: Національна академія Служби безпеки України, 2018. С. 408.

2. Войціховський А. В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. Журнал східноєвропейського права. 2018. № 53. С. 26-37.

3. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 2. С. 16-22.

4. Дмитренко М.А. Проблемні питання інформаційної безпеки України. Міжнародні відносини. Серія Політичні науки. 2017. № 17. С. 236-243.

5. Залєвська І. І., Удренас Г. І. Інформаційна безпека в Україні в умовах російської військової агресії. Південноукраїнський правничий часопис. № 1. 2022. С. 20-26.

УДК 351.74
DOI: 10.31733/17-03-2023-574-575

Олексій ДІДЕНКО
курсант факультету № 4
Харківського національного
університету внутрішніх справ

ЗАСОБИ ВДОСКОНАЛЕННЯ ДІЯЛЬНОСТІ ПОЛІЦІЇ ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Інформаційне суспільство мета більшості сучасних країн світ. В першу чергу, це обумовлено стратегічною перевагою. Такі країни як США, Канада, Японія, члени європейського союзу, вже давно впроваджують інформаційні технології в повсякденні сфери життя.

В основному пов'язаний подальший розвиток інформаційних технологій, з появою нових технічних засобів обробки інформації, які визначають рівень розвитку інформаційних технологій. Покращення управління є найважливішим чинником підвищення ефективності. На основі досягнень ведеться робота з удосконаленням форм і методів управління науково-технічного прогресу, вивчення законів, способів накопичення, обробка та передача інформації.

Згідно з рейтингом міжнародного конкурсу World Digital Competitiveness Ranking [1], Україна у 2021 році посіла 54 місце. Порівняно з 2020 роком показник покращився на чотири позиції. Підсумкова рейтингова система розраховується на основі трьох показників: