якість освіти та науки; регуляторне середовище, фінансовий капітал у ІТ-галузі, стан інтернету та комунікаційних технологій; рівень готовності використання цифрової трансформації. На сьогоднішній день наша держава прагне розпочати новий етап формування інформаційного суспільства. Відбувається перехід від впровадження інформаційних технологій до комплексної побудови цифрової системи в масштабі країни.

Ефективність правоохоронної діяльності значною мірою залежить від якості інформаційного забезпечення, тому інформаційні технології широко використовуються в діяльності правоохоронних органів. Найдоступнішим та найпростішим джерелом інформаційних технологій є сучасний смартфон. Фактично кожен поліцейський може лише за допомогою цього девайса бути на зв'язку з колегами, отримати доступ до онлайн-карт, усіх типів баз даних, навіть дізнатись особисті данні злочинця.

В свою чергу такий легкий доступ до мережі, надає можливість злочинцям порушувати закон, не виходячи з дому. Одним з найпопулярніших видів злочину за допомогою мобільних пристроїв є "онлайн-магазини наркотичних речовин". Більшість з яких працюють через анонімний месенджер "telegram". Такий спосіб збуту має певні переваги: продаж відбувається повністю анонімно, продавець та покупець не мають фізичного контакту [2].

Найпростішим способом боротьби з цим "феноменом" є сам месенджер , в якому є можливість поскаржитись на аккаунт чи канал, набираючи певну кількість скарг, вони блокуються. Існує телеграм бот "стоп наркотик" розроблений працівниками органів внутрішніх справ, який збирає такі канали та дає можливість кожному охочому поскаржитись маючи з собою лише мобільний пристрій, що значно спрощує цю процедуру. Завдяки цьому боту кожен день блокуються сотні аккаунтів.

Ще одним видом використання злочинцями мобільних пристроїв є телефонне шахрайство. Злочинець телефонує жертві представившись працівником банку чи інших установ, та починає запитувати персональні данні. Для запобігання подобних випадків слід дотримуватись наступних рекомендацій: встановити додаток для ідентифікації невідомих номерів, не залишати особисті данні на невідомих сайтах, надавати інформацію про шахраїв відповідним органам.

Висновки. Суспільство широко використовує новітні технології в повсякденному житті, найчастіше, мобільні пристрої. Це стало появою відповідного шахрайства. Органи внутрішніх справ в свою чергу активно використовують мобільні пристрої для протидії відповідній злочинності. Сучасні проблеми потребують сучасного рішення з допомогою засобів захисту інформації та обмеження доступу до персональних даних громадян.

1. World Digital Competitiveness Rankings - IMD. IMD business school. URL: https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/ (дата звернення: 03.03.2023).

2. Пядишев В. Г., Монастирський М. В. Смартфони в руках населення як засіб удосконалення діяльності поліції: порівняння українського та зарубіжного досвіду. Південноукраїнський правничий часопис. 2022, 1-2'. С. 152 158.

УДК 342.95
DOI: 10.31733/17-03-2023-575-578

Олександр ДУНЯШЕНКО
курсант ННІ права та підготовки
фахівців для підрозділів Національної поліції

Науковий керівник:
д.філос.наук, проф. **Елеонора СКИБА**

(Дніпропетровський державний університет внутрішніх справ)

ІНФОРМАЦІЙНА БЕЗПЕКА – ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Варто зазначити, що проблема національної безпеки України є особливо актуальною як сьогодні, так і в контексті подальшого загально цивілізаційного розвитку країни. Бурхливий розвиток інформаційної сфери супроводжується появою принципово

нових загроз інтересам особистості, суспільства, держави та її національній безпеці [1, с.68]. Інформація у сучасних умовах створює поле єдності та впливу на формування цілісності духовного та має прояв на різні аспекти соціально-культурного дискурсу. Інформаційна безпека у числі різних завдань безпосередньо та опосередковано сприяє вихованню соціальної індивідуальної та колективної ідентичності, національної у тому числі. Інформація як один із найпотужніших інструментів розбудови духовної національної єдності задовольняє суспільну потребу в урегулюванні соціального життя.

Інформаційна політика України формується як складова частина її соціально-економічної політики, виходячи з пріоритетності національних інтересів та загроз національній безпеці країни. Із правової точки зору вона ґрунтується на засадах правової демократичної держави і впроваджується шляхом розробки та реалізації відповідних національних доктрин, стратегій, концепцій та програм згідно із чинним законодавством. В Україні назріла об'єктивна потреба у державно-правовому регулюванні науково-технологічної та інформаційної діяльності, що відповідала б реаліям сучасного світу та рівню розвитку інформаційних технологій, нормам міжнародного права, але водночас ефективно захищала б власні українські національні інтереси [1, с.68].

Об'єктами інформаційної безпеки є людина, суспільство та держава, забезпечення їхніх інтересів є завданням інформаційної безпеки.

Питання пов'язані з інформаційною безпекою, проблемами інформаційного суспільства та інформаційних війн досліджували такі науковці, як Г.М. Сащук, В. А. Ліпкан, М. В. Гуцалюк, О. Г. Данільян, О. П. Дзьобань, М. І. Пановта ін. Дослідники відзначають існуючі та потенційні ризики у вітчизняній інформаційній сфері: незбалансованість політико-правової бази, відсутність необхідної інформаційної інфраструктури, проблеми входження української держави у світовий інформаційний простір тощо [4, с.2].

Інформаційна безпека, як складова національної безпеки – стан захищеності життєво важливих інтересів людини, суспільства і держави, коли запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [4, с.3].

Регулювання інформаційної безпеки в нашій країні здійснюється за допомогою таких нормативно-правових актів: Конституція України, Закон України «Про інформацію», Закон України «Про Національну програму інформатизації», Указ Президента України «Про Доктрину інформаційної безпеки України», Концепція національної безпеки України [4, с.3].

У ст. 17. Конституції України зазначено: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу». Інформаційну безпеку слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека має включати ефективну протидію сукупності інформаційних загроз. Необхідність гарантування інформаційної безпеки зумовлюється, по-перше, потребою забезпечення національної безпеки України в цілому, по-друге, існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам, по-третє, врахуванням того, що за допомогою інформації можна впливати на зміну свідомості і поведінку людей. Завдання інформаційної безпеки – створення системи протидії інформаційним загрозам та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави. При виникненні криз, загостренні конфліктів інформаційна боротьба може перерости в інформаційну війну, яка здійснюється за допомогою інформаційної зброї. Показниками, виступають цілеспрямованість, масштабність та комплексність дій тощо [1, с.69].

Відповідно до Закону України «Про основи національної безпеки» стосовно загроз національній безпеці зазначає: на сучасному етапі найбільш важливими потенційними та реальними ризиками стабільності в суспільстві та національній безпеці України в інформаційній сфері є:

1) розголошення конфіденційної інформації, що є власністю держави та спрямована на забезпечення національних інтересів та потреб держави та суспільства;

2) прояви обмеження доступу громадян до інформації та свободи слова;

3) поширення через засоби масової інформації культу та ідеології насильства, жорстокості тощо;

4) комп'ютерна злочинність та комп'ютерний тероризм;

5) розголошення інформації, що становить як державну, так і іншу таємницю, що передбачена Законом;

6) намагання маніпулювання суспільною свідомістю, зокрема, шляхом поширення упередженої, неповної чи недостовірної інформації [4, с.5].

Загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку - головна інформаційна загроза національної безпеки. Це і є, власне, загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізовується на інформаційному рівні. Стратегічне інформаційне протистояння є самостійним і принципово новим видом протистояння, здатним вирішувати конфлікт без застосування збройних сил у традиційному розумінні [1, с.69].

Національну безпеку України в інформаційній сфері слід розглядати як інтегральну цілісність чотирьох складових – персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки [1, с.71].

В умовах воєнного стану країни особливо актуальним постало питання необхідності єдиної інформаційної політики. У зв'язку із цим Президент України підписав Указ № 152/2022, яким увів в дію Рішення Ради національної безпеки і оборони України «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» [3, с.21].

Підвищення медіакультури та медіаграмотності суспільства особливо гостро виявилася в умовах війни. Так, наприклад, несвідомі громадяни публікують у соціальних мережах фото та відео ворожих обстрілів, пересування української військової техніки чи позиції військових, не усвідомлюючи те, що цим полегшують завдання ворогові, створюють загрозу для військових та цивільних людей. Тому органи влади та структури громадянського суспільства мають через засоби масової інформації проводити постійну роз'яснювальну роботу серед населення, а правоохоронні органи – жорстко припиняти такі дії [3, с.22]. Розбудова інформаційного суспільства є завданням не тільки Ради національної безпеки і оборони України, але й сфери наукового знання. Філософія права – є науково-теоретичним знанням, яке однією із своїх функцій має інформаційно-освітню. Якщо суспільство ставить на меті створити державу сталого розвитку, то мета всього виховання як завдання суспільних наук, зокрема філософії права, – формування суб'єкта права, людини, що має критичне мислення, свідомо прямує певним правовим орієнтирам, вважає за справу своєїгідності дотримуватися певних правових ідеалів [8].

Інформаційна політика держави повинна відбивати нагальні питання, що склалися у міжнародній сфері та сфері інформаційної безпеки тощо. Необхідним є забезпечення законодавчого захисту прав та інтересів всіх суб'єктів інформаційних відносин. Найскладнішими тут є такі завдання, що передбачають гармонійне забезпечення інформаційної безпеки держави, особи і суспільства з одночасним виокремленням нагальних пріоритетів, до яких слід віднести створення/відновлення основних точок захисту системи національної безпеки в інформаційній сфері, практичну реалізацію наведеної вище схеми створення ефективної системи інформаційної безпеки держави, перегляд списку нових інформаційних загроз, усунення наявних із визначенням ступеня можливих наслідків та рівнів їх інтенсивності. Основні акценти державної інформаційної політики повинні базуватись на забезпеченні права на достовірну, повну та своєчасну інформацію, свободу слова та інформаційну діяльність, недопущення втручання в зміст та внутрішню організацію інформаційних процесів, крім випадків, визначених законодавством відповідно до Конституції України; забезпеченні інформаційної та національно-культурної ідентифікації України у світовому інформаційному просторі; гарантуванні державної підтримки та розвитку ресурсів науково-технічної продукції та інформаційних технологій [1, с.73].

Таким чином, інформаційне забезпечення національної безпеки виконує важливу багатопланову роль у визначенні національних інтересів і пріоритетів національної безпеки. Для забезпечення інформаційної безпеки держави необхідно всебічне задоволення потреб громадян, підприємств, установ і організацій всіх форм власності в доступі до достовірної та об'єктивної інформації; збереження і примноження духовних, культурних і моральних

цінностей Українського народу; розвиток медіа-культури суспільства і соціально відповідальної медіа-середовища; формування ефективної правової системи захисту особистості, суспільства і держави від деструктивних пропагандистських впливів; створення на базі норм міжнародного права системи і механізмів захисту від негативних зовнішніх впливів, перш за все, пропаганди; розвиток інформаційного суспільства [4, с.9].

1. Боднар І.Р. Інформаційна безпека як основа національної безпеки [Електронний ресурс].– Режим доступу: https://core.ac.uk/download/pdf/141443493.pdf

2. Закон України. Про інформацію / [Електронний ресурс].– Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12.

3. Залєвська І. І., Удренас Г. І. Інформаційна безпека України в умовах російської військової агресії [Електронний ресурс].– Режим доступу: http://www.sulj.oduvs.od.ua/archive/2022/1-2/6.pdf

4. Панченко О. Інформаційна складова національної безпеки [Електронний ресурс]. – Режим доступу: https://www.rdc.org.ua/download/stati/Informational-warehouse.pdf

5. Почепцов, Г. Інформаційна політика: навч. посібник [Текст] / Г. Г. Почепцов. – К.: Знання, 2006. – 663 с.

6. Супрун, В. М. Інформаційний суверенітет як один з елементів інформаційної безпеки держави: І. Р. Боднар. Інформаційна безпека як основа національної безпеки Механізм регулювання економіки, 2014, № 1 теоретико-правовий аспект [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/portal/natural/vkhnu/Pravo/2009 .

7. Ярочкін, В. Система безпеки фірми [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua.

8. Скиба, Е. Роль філософії права в формуванні свідомості суспільства сучасної формації. Науково-теоретичний альманах Грані, 2020. *23*(5), 64-76. https://doi.org/10.15421/172054

УДК 004+351
DOI: 10.31733/17-03-2023-578-579

Ілля ЖЕЛНОВАЧ
курсант факультету №4
Харківського національного
університету внутрішніх справ

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Інформація, а також процеси, системи та мережі, які її обробляють, є важливими активами кожної організації, як у державному, так і в приватному секторі. Інформаційна безпека має гарантувати конфіденційність, цілісність і доступність інформації та систем, які її обробляють.

Система управління інформаційною безпекою включає в себе необхідну організаційну структуру (ролі та комітети) та процедурну організацію (процеси безпеки), а також необхідні інструкції (процедури та правила). постійно визначати, управляти, контролювати, підтримувати та покращувати інформаційну безпеку в організації на основі підходу до управління ризиками.

Управління інформаційною безпекою - це безперервний процес, стратегії та концепції якого повинні постійно переглядатися на предмет їх ефективності та результативності, а також оновлюватися за необхідності [1].

Хоча СУІБ призначена для створення цілісної системи управління інформаційною безпекою, цифрова трансформація вимагає від організацій постійного вдосконалення та розвитку їхніх політик безпеки та засобів контролю. Структура та межі, визначені СУІБ, можуть застосовуватися лише протягом обмеженого періоду часу, і на початкових етапах співробітникам може бути складно прийняти їх. Завдання організацій полягає в тому, щоб розвивати ці механізми контролю безпеки в міру того, як змінюються їхні ризики, культура та ресурси.

Стратегія управління інформаційною безпекою організації може бути зумовлена багатьма різними факторами. Програма може бути натхненна внутрішньою політикою або вимагатися зовнішніми силами. Обидва ці потенційні чинники мають відповідні стандарти та вимоги до дотримання.

У деяких випадках внутрішні політики безпеки та бізнес-цілі організації можуть