Список використаних джерел:

1. Бутиліна В.О. Управлінське консультування [Електронний ресурс] //Харківський національний університет внутрішніх справ. Х.: Видавництво «Форт». 2014. 165 с. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/1054/upravlins_ke_konsul_tuvannya_navch_metod.pdf?sequence=2&isAllowed=y (дата звернення 03.11.2021).
2. Інформаційний консалтинг [Електронний ресурс]. URL: https://sites.google.com/site/informacijniproduktiiposlugi/informacijnij-konsalting (дата звернення 03.11.2021).
3. Інформаційний консалтинг: поняття, функції, принципи [Електронний ресурс]. URL: https://opu-konf.at.ua/2011/l.s-prokopenko.pdf (дата звернення 03.11.2021).
4. Послуги з консалтингу [Електронний ресурс]. URL: https://fin.biem.sumdu.edu.ua/images/My_files/Fin_Services/Part23.pdf (дата звернення 03.11.2021).
5. Ринок консалтингових послуг в Україні [Електронний ресурс]. URL: https://leschishin.org/review/r003.php (дата звернення 03.11.2021).
6. Тарасенко С. І. Управлінське консультування [Електронний ресурс]// Дніпровський державний технічний університет. Кам'янське. 2017. 149 с. URL: http://www.dstu.dp.ua/Portal/Data/7/33/7-33-mzs77.pdf (дата звернення 03.11.2021).

Мохова К.С.,
студентка IV курсу факультету менеджменту і бізнесу ВП «Миколаївська філія Київського національного університету культури імистецтв»;
Науковий керівник: Шуляк С.О., кандидат педагогічних наук, доцент, декан факультету менеджменту і бізнесу ВП ««Миколаївська філія Київського національного університету культури і мистецтв», м. Миколаїв

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЇЇ МІСЦЕ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Захищаючи свої інформаційні інтереси, кожна держава має дбати про свою інформаційну безпеку. Необхідною умовою для нормального існування та розвитку кожного суспільства є захищеність від зовнішніх і внутрішніх загроз, стійкість до спроб зовнішнього тиску та здатність протистояти таким спробам і нейтралізувати загрози.

З огляду нашого дослідження, важливим постає розуміння понять «інформаційна безпека» та «національна безпека України».

Інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [4].

Відповідно до Закону України «Про національну безпеку України», *національна безпека України* – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [3].

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

Загрозами національній безпеці України в інформаційній сфері є:

1. Загрози комунікативного характеру в сфері реалізації потреб людини і громадянина, суспільства та держави щодо продукування, споживання, розповсюдження та розвитку національного стратегічного контенту та інформації, що включають:

а) зовнішні негативні інформаційні впливи на свідомість людини та спільноти через засоби масової інформації, а також мережу Інтернет, що здійснюються на шкоду державі.

б) поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації для дискредитації органів державної влади, дестабілізації суспільно-політичної ситуації, що значно ускладнює прийняття політичних рішень, завдає шкоди національним інтересам України чи створює негативний імідж України.

в) загрози свободі слова, що виражається у відсутності правової бази для посилення ролі творчих (трудових) колективів і редакцій у процесі здійснення редакційної політики засобами масової інформації усіх форм власності.

г) створення, розповсюдження, передача та зберігання інформації з метою підтримки, супроводження чи активізації злочинної та терористичної діяльності [5].

2. Загрози технологічного характеру в сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору, що включають:

а) прояви кіберзлочинності, кібертероризму чи кібернетичної військової агресії, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем з метою: здійснення з їх допомогою деструктивного інформаційного впливу.

б) недостатній рівень розвитку національної інформаційної інфраструктури, зокрема: використання неліцензованого і несертифікованого програмного забезпечення, засобів і комплексів обробки інформації.

в) порушення порядку доступу, поводження та встановлених регламентів збору, обробки, зберігання, поширення чи передачі інформації, яка захищається державою, або роботи з інформаційними ресурсами, що її містять.

г) відсутність громадського контролю за діяльністю суб'єктів забезпечення інформаційної безпеки, захищеністю національної інформаційної інфраструктури та інформаційного простору України [5].

Для формування збалансованої державної політики та ефективного проведення комплексу узгоджених заходів щодо захисту національних інтересів в інформаційній сфері є створення сприятливих умов для їх реалізації, які в сукупності становлять об'єкт управління органами державного управління, систему забезпечення інформаційної безпеки, тобто основні напрямки політики національної безпеки в інформаційній сфері, а також внутрішнє та зовнішнє середовище. Інформаційна безпека забезпечується комплексом заходів системи забезпечення національної безпеки України, що включає сукупність державних органів, громадських організацій, посадових осіб та окремих громадян [6].

Таким чином, можна констатувати, що пріоритетами державної політики в інформаційній сфері мають бути:

1) щодо забезпечення інформаційної безпеки:

– створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

– визначення механізмів регулювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій, закладів культури та засобів масової інформації;

– розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України;

– боротьба з дезінформацією та деструктивною пропагандою.

2) щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію:

– стимулювання розвитку національного виробництва текстового і аудіовізуального контенту, зокрема шляхом створення системи квотування та проведення цільових конкурсів на надання грантів;

– забезпечення функціонування суспільного телебачення і радіомовлення України, у тому числі його належного фінансування;

– підтримка вітчизняної книговидавничої справи, зокрема перекладів іноземних творів;

– розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист.

3) щодо відкритості та прозорості держави перед громадянами:

– розвиток механізмів електронного урядування;

– сприяння розвитку можливостей доступу та використання публічної інформації у формі відкритих даних;

– розвиток сервісів, спрямованих на більш масштабне та ефективне залучення громадськості до прийняття рішень органами державної влади та органами місцевого самоврядування.

4) щодо формування позитивного міжнародного іміджу України:

– ґрунтовне реформування системи представлення інформації про Україну на міжнародній арені;

– розвиток публічної дипломатії, у тому числі культурної та цифрової;

– участь у міжнародних культурних заходах з метою представлення національної культури та ідентичності;

– запровадження міжнародних культурних фестивалів в Україні з метою популяризації української культури та розвитку комунікацій «від людини до людини» [2].

Отже, на підставі низки законодавчих та підзаконних актів, Конституції України тощо, однозначно інформаційна безпека визнається одним із напрямів державної політики у сфері національної безпеки і оборони, невід'ємною частиною політичного, економічного, оборонного та інших складників національної безпеки [7].

Список використаних джерел:

1. Бондар І. Р. Інформаційна безпека як основа національної безпеки [Електронний ресурс] / І. Р. Бондар // Механізм регулювання економіки. 2014. №1. С. 68-75. URL:https://core.ac.uk/download/pdf/141443493.pdf (дата звернення: 02.11.2021).

2. Гур'єв В. І. Інформаційна безпека держави [Електронний ресурс] / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова// Чернігівський національний технологічний університет. Ніжин. 2018. 166 с. URL:http://ir.stu.cn.ua/bitstream/handle/123456789/19246/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC.%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B4%D0%B5%D1%80%D0%B6.%20New%20booklet%201.pdf?sequence=1&isAllowed=y (дата звернення: 02.11.2021).

3. Закон України «Про Національну безпеку України»(офіц. текст: за станом на 21 червня 2018 р.) [Електронний ресурс] // Верховна Рада України. 2018. № 2469-VIII. URL:https: // zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 02.11.2021).

4. Інформаційна безпека now: яких елементів не вистачає? [Електронний ресурс]. URL:https://www.prostir.ua/?library=informatsijna-bezpeka-now-yakyh-elementiv-ne-vystachaje (дата звернення: 02.11.2021).

5. Концепція інформаційної безпеки України [Електронний ресурс]. URL: https://www.osce.org/files/f/documents/0/2/175056.pdf (дата звернення: 02.11.2021).

6. Малик Я. Інформаційна безпека України: стан та перспективи розвитку[Електронний ресурс] / Я. Малик // Ефективність державного управління. 2015. №44. С. 13-20. URL:

http://lvivacademy.com/vidavnitstvo_1/edu_44/fail/ch_1/3.pdf (дата звернення: 02.11.2021).

7. Шемчук В. В. Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктрини й законодавчої основи [Електронний ресурс] / В.В. Шемчук // Вчені записки ТНУ імені В.І. Вернадського. 2019. №4. С. 31-37. URL:http://www.juris.vernadskyjournals.in.ua/journals/2019/4_2019/8.pdf (дата звернення: 02.11.2021).

Яковлєва Н.Д.,
студентка IV курсу факультету менеджменту і бізнесу ВП «Миколаївська філія Київського національного університету культури і мистецтв»;
Науковий керівник: Шуляк С.О., кандидат педагогічних наук, доцент, декан факультету менеджменту і бізнесу ВП ««Миколаївська філія Київського національного університету культури і мистецтв», м. Миколаїв

ТАРГЕТИНГ ЯК ІНСТРУМЕНТ DIGITAL-МАРКЕТИНГУ

На сьогоднішній день в інтернет-маркетингу широко застосовується таргетинг. *Таргетинг* - це спосіб відбору аудиторії за заданими критеріями до цільової. Термін походить від слова target - ціль або мета. Його ціль – персоналізація та виділення цільової аудиторії для реклами в інтернеті. Цей інструмент необхідний для реклами інформаційнорозважальних роботів для дітей, який допоможе оптимізувати витрати на просування товару, досягти максимального рівня впізнання та збільшить продаж. Результатом націлювання є цільові покази реклами - користувачам, на яких орієнтований продукт або послуга [1].

Таргетинг в інтернет-середовищі надає можливість виокремити з усієї аудиторії користувачів інтернету тільки тих, що відповідають заданим певним критеріям конверсії (цілі маркетингових дій), що дозволяє зменшити витрати на залучення цільової аудиторії до об’єкту маркетингу, котрим може бути товар, сайт, реклама. Таргетинг в інтернет-комунікаціях показує рекламу користувачам відповідно до їх інтересів [2].

Основні види таргетингу при активному використанні сучасних методів показу реклами можна класифікувати наступним чином:

1) *тематичний таргетинг* являє собою показ рекламно-інформаційних повідомлень на інформаційних майданчиках, що відповідають певній тематиці;

2) *націлювання за контекстом* (таргетинг за інтересами) передбачає демонстрацію повідомлення відповідно до інтересів відвідувачів рекламного майданчика;