

Гусак О. П.,
канд. наук із соц. комунік., доцент,
Інститут журналістики
Київського університету імені Бориса Грінченка

Husak Olha,
Candidate of Sciences on Social Communications,
Associate Professor, Institute of Journalism
of Borys Grinchenko Kyiv University

УДК 007: 304: 659.4

КОМУНІКАЦІЙНА БЕЗПЕКА ЯК НАПРЯМ ПІДГОТОВКИ ФАХІВЦІВ: СУТНІСТЬ, ЗМІСТ КОМПЕТЕНТНОСТЕЙ, ПЕРСПЕКТИВИ РОЗВИТКУ

COMMUNICATION SECURITY AS THE PROGRAM OF SPECIALISTS TRAINING: SUBSTANCE, CONTENT OF COMPETENCIES, PROSPECTS OF DEVELOPMENT

Анотація. Мета статті полягає у розкритті компетентнісного підходу щодо формування майбутніх фахівців з комунікаційної безпеки, у розробці перспективних напрямів їхньої кваліфікованої підготовки. Основні результати дослідження відображено у переліку професійних компетентностей спеціалістів у галузі комунікаційної безпеки, який включає здатність до виявлення комунікаційних загроз, особливостей цивілізованого, маніпулятивного і варварського впливу на державному, корпоративному і особистісному рівнях, типів маніпуляторів, різновидів маніпулятивних пасток, маніпулятивних технологій; можливість використання ефективних способів нейтралізації і протидії маніпулятивному впливу; навички організації, планування і реалізації своєї діяльності в умовах інформаційних атак; володіння комунікаційними, організаційними, технічними методами захисту інформації в сучасних інформаційних системах та мережах.

Ключові слова: зв'язки з громадськістю, комунікація, компетентність.

Abstract. The article aims at defining the competence-based approach to training the future professionals in communication security and development of the advanced fields of their high-qualitative training. The main results of the study are represented in the list of specialists' professional competencies in the field of communication security, which includes: capability to identify communication threats; peculiarities of civilized, manipulative and barbaric influences at the state, corporate and personal levels; categories of manipulators, types of manipulative traps, existing manipulative techniques; capability for using effective means to neutralize or counteract to manipulative influences; skills required for organization, planning and implementation of one's actions in terms of information attacks; acquisition of communicative, organizational and technical methods of information protection in the existing information systems and networks.

Keywords: PR, communication, competence.

Вступ. Інформаційні війни, які розгортаються у сучасному світі та в Україні, зокрема, стали ключовою загрозою для наявного світового ладу. На початку XXI ст. від уміння «тримати» зовнішні інформаційні удари і реалізовувати на їх тлі послідовну адекватну комунікаційну політику залежить існування держав як незалежних суверенних систем.

У світі, де інформація поступово стає небезпечною зброєю, вказані чинники актуалізують питання підготовки вузькоспеціалізованих фахівців. Фахівців, професійно відповідальних за вибудовування чіткої безпечної системи комунікації і взаємозв'язків як усередині держави, так і за її межами. Їхня загальна місія полягає в тому, щоб

розуміти, як реагувати на інформаційні загрози, й усувати їх.

Факти свідчать, що попит на таких «профі» починає формуватися передусім у державному секторі. Зокрема, йдеться про офіційні заяви зовнішньополітичної служби ЄС про набір фахівців-експертів для інформаційної війни з кремлівською пропагандою [1]. З цією самою метою в Латвії та Естонії планується запуск російськомовних телеканалів, які вибудовуватимуть свою стратегію за допомогою таких фахівців [2]. Також наприкінці квітня цього року Фінляндія виступила з ініціативою сформувати окрему власну робочу групу для боротьби з російською пропагандою [3]. Не кажучи вже про Україну, яка потребує кваліфікованих кадрів для

захисту власного інформаційного простору, особливо після створення Міністерства інформаційної політики [4].

У цьому контексті актуалізуються питання підготовки фахівців для ефективного протистояння інформаційній агресії на державному, корпоративному та особистісному рівнях. Підготовки, яка б здійснювалась із врахуванням чітко сформульованих компетентностей для професіоналів у галузі комунікаційної безпеки, що, на думку науковців, якнайкраще сприяє адаптації майбутніх фахівців до мінливих умов сучасного ринку праці й бурхливого розвитку науки й техніки [5, с. 233].

Проблему впровадження компетентнісного підходу у професійну підготовку фахівців порушували у своїх наукових розвідках А. Капська, В. Євдокимов, В. Бондар, С. Козак. Теоретико-методологічним засадам компетентнісного підходу присвячені дослідження таких науковців, як О. Савченко, Н. Бібік, А. Маркова, О. Овчарук, В. Байденко, А. Хуторський, В. Петрук, М. Розов. Окремо особливості та специфіку інформаційно-комунікаційної безпеки звизчали теоретики В. Дубов, Н. Брусицін, Т. Мишова, С. Охрименко, С. Тутунару, К. Склифос, Ю. Данюшина. Водночас у теорії соціокомунікації, зокрема в галузі зв'язків з громадськістю, найважливіші питання сутності та змісту компетентностей фахівців із комунікаційної безпеки не було досліджено вичерпно.

У практичній площині можна констатувати той факт, що в Україні в переліку галузей знань і спеціальностей, за якими здійснюється підготовка бакалаврів (станом на 29 квітня 2015 р.), напрям «Комунікаційна безпека» із розробленими компетентностями відсутній [6]. Більше того, з переліку освітніх спеціальностей зникли окремі галузі знань, які стосувалися безпосередньо інформаційної безпеки. Як відомо, за ними відбувалася підготовка фахівців у сфері технічного захисту інформації. Ідеться про шифр 1701 – «інформаційна безпека», що включав такі спеціальності, як безпека інформаційних і комунікаційних систем, безпека державних інформаційних ресурсів, системи технічного захисту інформації, автоматизація її обробки, управління інформаційною безпекою, а також адміністративний менеджмент у сфері захисту інформації. Замість цього з'явилася лише одна спеціальність «кібербезпека» (код 125) у рамках галузі знань «Інформаційні технології», яка, за нашою оцінкою, становить незначну частину сфери інформаційно-комунікаційної безпеки, підготовки за якою недостатньо для вирішення проблем і нейтралізації загроз у світі, де інформація стала небезпечною зброєю, а не просто товаром.

Отже, враховуючи все викладене вище, доходить висновку, що тема дослідження є актуальною як

в теоретичному, так і в практичному аспектах.

Мета дослідження полягає у визначенні переліку професійних компетентностей для фахівців з комунікаційної безпеки, у розробці перспективних напрямів їхньої кваліфікованої підготовки.

Для досягнення поставленої мети необхідно виконати такі завдання:

- проаналізувати теоретичні підходи до сутності комунікаційної безпеки, уточнити поняття «комунікаційна безпека» у межах теорії соціальних комунікацій;

- сформулювати перелік компетентностей для спеціалістів у галузі комунікаційної безпеки;

- окреслити напрями професійної підготовки фахівців з комунікаційної безпеки.

Методи дослідження. Під час дослідження застосовано комплекс загальнонаукових методів: аналіз, синтез, індукцію, дедукцію, узагальнення (під час дослідження теоретичних засад комунікаційної безпеки); термінологічний (для характеристики розробки наукової проблеми та основних понять дослідження), емпіричні методи (вивчення наукової літератури, статистичних даних, інших документів тощо).

Результати й обговорення. Для з'ясування сутності поняття «комунікаційна безпека» звернімося до енциклопедичної літератури та відповідних словників і спершу розтлумачимо слово «безпека». У тлумачних словниках сучасної української мови представлено такі його значення (від праслов'янськ. *vezrešьpъ* (jь), утвореного від прийменника *bez* – «при відсутності; крім» та іменника *reša* – «турбота, клопоти» [7, с. 163]): а) стан, який не викликає занепокоєння [8, с. 53]; б) стан, коли кому-, чому-небудь ніщо не загрожує [9, с. 70]. Згідно з ними, можна припустити, що провідним компонентом значення «безпека» виступає захищеність від загроз та шкідливих дій.

Термін «комунікація» (від лат. *communicatio* – повідомлення, передача) у науковій літературі з'явився, за твердженнями дослідників [10, с. 12], на початку ХХ ст. і в різних науках трактується по-різному. Теоретики виокремлюють кілька основних підходів до розуміння комунікації в сучасній науці та розглядають її як:

- засіб зв'язку будь-яких об'єктів матеріального чи духовного світу;

- спілкування, передачу інформації між людьми або від одного соціального суб'єкта до іншого (соціальна інформація);

- передачу інформації від однієї системи до іншої з використанням спеціальних матеріальних носіїв [11, с. 7].

Доволі змістовним, на нашу думку, є визначення, запропоноване українським теоретиком

В. Мойсеевим, за яким під комунікацією розуміють «двосторонній потік інформації з використанням мовних та паралінгвальних (жести, міміка, рухи тіла, організація простору між учасниками тощо) засобів і зворотного зв'язку, коли одна сторона одержує чи отримує інформацію з одночасною реакцією на неї» [12, с. 218].

Отже, на основі викладеного вище комунікаційна безпека може розглядатись як стан захищеності потреб та інтересів держави/організації/особистості вербальними та невербальними засобами. Інакше кажучи, це комплекс дій, спрямованих на попередження і подолання інформаційно-комунікаційних загроз на державному, корпоративному, особистісному рівнях. А фахівці з комунікаційної безпеки – це професіонали, здатні планувати і реалізовувати систему заходів комунікаційного управління із захисту держави, організації або особистості від нецивілізованих і маніпулятивних форм впливу.

Основні завдання, які стоять перед такими фахівцями сьогодні:

- формування сучасного підходу до комунікаційної безпеки як системної науково-практичної діяльності;
- виявлення комунікаційних ризиків і чинників, що загрожують комунікаційній безпеці суб'єктів;
- оперативна діагностика маніпулятивних технологій;
- нейтралізація маніпулятивної дії і переведення її на рівень конструктивної взаємодії;
- розвиток ресурсів для антиманіпулятивної компетентної поведінки;
- профілактика і підготовка суб'єкта до потенційних комунікаційних ризиків у майбутньому.

Систематизація теоретичних розробок щодо сутності комунікаційної безпеки [9; 10], кризового менеджменту та кризової комунікації в системі PR дає змогу зробити певні висновки. На нашу думку, фахівець з комунікаційної безпеки повинен володіти такими компетентностями:

1. Він повинен знати:

- особливості цивілізованого, маніпулятивного і варварського впливу на державному, корпоративному й особистісному рівнях;
- типи маніпуляторів, різновиди маніпулятивних пасток, маніпулятивні технології;
- цивілізовані способи нейтралізації і протидії маніпулятивному впливу;
- етичні основи комунікації;
- перспективи розвитку методів і засобів інформаційної й комунікаційної безпеки.

2. Він повинен уміти:

- виявляти комунікаційні загрози;

- застосовувати на практиці отримані знання про методи і засоби комунікаційної безпеки, проводити їх порівняльний аналіз та оптимізувати;

- застосовувати комунікаційну техніку цивілізованого протистояння інформаційній агресії.

3. Він повинен володіти:

- навичкою організації, планування і реалізації своєї діяльності в умовах інформаційних атак;

- навичкою розпізнавання ознак маніпулятивного впливу;

- комунікаційними, організаційними, технічними методами захисту інформації в сучасних інформаційних системах і мережах.

Враховуючи це, програма підготовки фахівців такого профілю, на наш погляд, може включати вказані нижче основні розділи:

- 1) організація системи комунікаційної безпеки;
- 2) дослідницька, прогнозо-аналітична діяльність у цій сфері;
- 3) планування і реалізація комунікаційної політики в державному та комерційному секторах в умовах інформаційної агресії;
- 4) створення інформаційних продуктів під час інформаційної війни;
- 5) основи технічного захисту інформації;
- 6) міжнародні стандарти в галузі інформаційно-комунікаційної безпеки.

За нашим переконанням, у світі, що постійно змінюється і стає дедалі крихкішим і уразливішим, рівень теоретичних знань за таким напрямом підготовки повинен максимально відповідати запитам і викликам сьогодення, а також наближатися до потреб ринку. На нашу думку, важливо випереджати реальність, пропонуючи ефективні форми, інструменти комунікації, спрямовані на зміцнення миру, злагоди і взаєморозуміння усередині держави і за її межами. Натомість ігнорування важливості цих питань та кроків істотно стримуватиме розвиток та реалізацію адекватної інформаційно-комунікаційної стратегії України, що безпосередньо впливатиме на національну безпеку держави.

У цьому контексті ключовими для вітчизняних учених можуть стати такі тематичні наукові напрями:

- організація комунікаційної безпеки;
- управління комунікаційними ризиками;
- теорія і практика кризової комунікації;
- аудит комунікаційної безпеки на державному, корпоративному і особистісному рівнях;
- антиманіпуляція;
- аналіз комунікаційних загроз і засобів протидії;
- управління віртуальною безпекою;
- розвиток ефективних форм інформаційної протидії;
- ефективність комунікаційної безпеки;
- етичні основи комунікаційної безпеки.

Висновки. Таким чином, узагальнюючи сучасні теоретичні погляди щодо специфіки комунікаційної безпеки, ми уточнили це поняття і розглянули його як стан захищеності потреб та інтересів держави/організації/особистості вербальними та невербальними засобами.

Перелік професійних компетентностей фахівців у галузі комунікаційної безпеки, на нашу думку, має включати: здатність до виявлення комунікаційних загроз, особливостей цивілізованого, маніпулятивного і варварського впливу на державному, корпоративному і особистісному рівнях, типів маніпуляторів, різновидів маніпулятивних пасток, маніпулятивних технологій; можливість використання цивілізованих способів нейтралізації і протидії маніпулятивному впливу; навички організації, планування і реалізації своєї діяльності в умовах інформаційних атак; володіння комунікаційними, організаційними, технічними методами захисту інформації в сучасних інформаційних системах та мережах.

Підсумовуючи викладений матеріал, варто підкреслити, що представлена точка зору є лише теоретично обґрунтованою спробою наблизитися до розуміння конкретних кроків для системного поетапного вирішення проблеми підготовки кадрів у галузі комунікаційної безпеки. У цьому контексті глобальні перспективи подальших розвідок вбачаються у:

- всебічному аналізі й прогнозуванні інформаційно-комунікаційних загроз для національної безпеки в усіх сферах їх прояву;
- виробленні комплексу заходів і механізмів гарантування комунікаційної безпеки в корпоративній сфері;
- підготовці освітніх стандартів з підготовки фахівців у галузі інформаційно-комунікаційної безпеки;
- розробці безпечних інформаційних технологій, що використовуватимуться в процесі реалізації життєво важливих функцій суспільства і держави;
- розвитку міжнародної співпраці, розробці і реалізації комплексу заходів із забезпечення міжнародної інформаційно-комунікаційної безпеки.

Список літератури

1. В ЄС вже набрали фахівців для протидії російській пропаганді [Електронний ресурс] // TELEKRITIKA.UA. – 05.06.2015. – Режим доступу: <http://www.telekritika.ua/kontekst/2015-06-05/107864>. – Дата доступу: 16.08.2015.
2. Світ проти кремлівської пропаганди: Mythbusters, бойкот RT та «антиколорадські» наклейки [Електронний ресурс] // TYZH DEN.UA. – 27.04.2015. – Режим доступу: <http://tyzhden.ua/News/135174>. – Дата доступу: 18.08.2015.

3. Стець: Латвія та Естонія розпочали боротьбу з російською пропагандою [Електронний ресурс] // DEPO.UA. – 09.06.2015. – Режим доступу: <http://www.depo.ua/ukr/svit/stets-latviya-ta-estoniya-rozpochali-borotbu-z-rosiyskoyu-09062015182500>. – Дата доступу: 18.08.2015.

4. Для боротьби з путінською пропагандою створюється Міністерство інформполітики – Геращенко [Електронний ресурс] // NEWSRU.UA. – 30.11.2014. – Режим доступу: <http://www.newsru.ua/ukraine/30nov2014/ge5.html>. – Дата доступу: 15.08.2015.

5. Ходань О. Л. Компетентнісний підхід до підготовки майбутніх фахівців у ВНЗ / О. Л. Ходань // Науковий вісник Ужгородського національного університету. – Вип. 29. – С. 232–235.

6. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти № 266 – редакція від 29. 04. 2015 [Електронний ресурс] // KMU.GOV.UA. – 29.04.2015. – Режим доступу: <http://www.kmu.gov.ua/control/uk/cardnpd?docid=248149695>. – Дата доступу: 15.08.2015.

7. Етимологічний словник української мови : в 7 т. / [гол. ред. О. С. Мельничук]. – Т. 1. – Київ : Наук. думка, 1982. – 634 с.

8. Сучасний тлумачний словник української мови: 65000 слів / [за заг. ред. В. В. Дубічинського]. – Харків : ВД «ШКОЛА», 2006. – 1008 с.

9. Великий тлумачний словник сучасної української мови (з дод. і допов.) / [уклад. і голов. ред. В. Т. Бусел]. – Київ ; Ірпінь : ВТО «Перун», 2005. – 1728 с.

10. Бебик В. М. Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технологія, техніка публік рилейшнз : монографія / В. М. Бебик. – Київ : МАУП, 2005. – 440 с.

11. Тихомирова Є. Б. Зв'язки з громадськістю : навч. посіб. / Є. Б. Тихомирова. – Київ : НМЦВО, 2001. – 560 с.

12. Мойсеев В. А. Публік рилейшнз / В. А. Мойсеев. – Київ : Академвидав, 2007. – 224 с.

13. Данюшина Ю. В. Коммуникативная безопасность в государственном и деловом управлении / Ю. В. Данюшина // Актуальные проблемы языкознания. Язык. Словесность. Культура. – Вип. 1. – 2011. – С. 71–86.

Reference list

1. V YeS vzhe nabraly fakhivtsiv dlia protydii rosiiskii propahandi [Electronic resource] // TELEKRITIKA.UA. – 05.06.2015. – Reference: <http://www.telekritika.ua/kontekst/2015-06-05/107864>. – Accessed: 16.08.2015.
2. Svit proty kremlivskoi propahandy: Mythbusters, boikot RT ta «antykoloradski» nakleiky [Electronic resource] // TYZH DEN.UA. – 27.04.2015. – Reference: <http://tyzhden.ua/News/135174>. – Accessed: 18.08.2015.
3. Stets: Latviia ta Estoniia rozpochaly borotbu z rosiiskoiu propahandoiu [Electronic resource] // DEPO.UA. – 09.06.2015. – Reference: <http://www.depo.ua/ukr/svit/stets-latviya-ta-estoniya-rozpochali-borotbu-z-rosiyskoyu-09062015182500>. – Accessed: 18.08.2015.
4. Dlia borotby z putinskoiu propahandoiu stvoruietsia Ministerstvo informpolityky – Herashchenko

[Electronic resource] // NEWSRU.UA. – 30.11.2014. – Reference: <http://www.newsru.ua/ukraine/30nov2014/ge5.html>. – Accessed: 15.08.2015.

5. Khodan O. L. Kompetentnisnyi pidkhdid do pidhotovky maibutnikh fakhivtsiv u VNZ / O. L. Khodan // Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. – Vyp. 29. – S. 232–235.

6. Pro zatverdzhennia pereliku haluzei znan i spetsialnostei, za yakymy zdiisniuietsia pidhotovka zdobuvachiv vyshchoi osvity № 266 – redaktsiia vid 29.04.2015 [Electronic resource] // KМУ. GOV.UA. – 29.04.2015. – Reference: <http://www.kmu.gov.ua/control/uk/cardnpd?docid=248149695>. – Accessed: 15.08.2015.

7. Etymolohichnyi slovnyk ukrainskoi movy : v 7 t. / [hol. red. O. S. Melnychuk]. – T. 1. – Kyiv : Nauk. dumka, 1982. – 634 s.

8. Suchasnyi tlumachnyi slovnyk ukrainskoi movy: 65000 sliv / [za zah. red. V. V. Dubichynskoho]. – Kharkiv : VD «ShKOLA», 2006. – 1008 s.

9. Velykyi tlumachnyi slovnyk suchasnoi ukrainskoi movy (z dod. i dopov.) / [uklad. i holov. red. V. T. Busel]. – Kyiv ; Irpin : VTO «Perun», 2005. – 1728 s.

10. Bebyk V. M. Informatsiino-komunikatsiinyi menedzhment u hlobalnomu suspilstvi: psykholohiia, tekhnolohiia, tekhnika publik ryleishnz : monohrafiia / V. M. Bebyk. – Kyiv : MAUP, 2005. – 440 s.

11. Tykhomyrova Ie. B. Zv'iazky z hromadskistiu : navch. posib. / Ie. B. Tykhomyrova. – Kyiv : NMTsVO, 2001. – 560 s.

12. Moiseiev V. A. Publikrileishnz / V. A. Moiseiev. – Kyiv : Akademvydav, 2007. – 224 s.

13. Danjushina Ju. V. Kommunikativnaja bezopasnost' v gosudarstvennom i delovom upravlenii / Ju. V. Danjushina // Aktual'nye problemy jazykoznanija. Jazyk. Slovesnost'. Kul'tura. – Vip. 1. – 2011. – S. 71–86.

Подано до редакції 26. 08. 2016 р.

Гусак О. П., канд. наук из соц. коммуник., доцент,
Институт журналистики
Киевского университета имени Бориса Гринченко

**КОММУНИКАЦИОННАЯ БЕЗОПАСНОСТЬ
КАК НАПРАВЛЕНИЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ:
СУЩНОСТЬ, СОДЕРЖАНИЕ КОМПЕТЕНТНОСТЕЙ, ПЕРСПЕКТИВИ РАЗВИТИЯ**

Аннотация. Цель статьи заключается в раскрытии компетентностного подхода к формированию будущих специалистов по коммуникационной безопасности, в разработке перспективных направлений их квалифицированной подготовки. Основные результаты исследования отображены в перечне профессиональных компетентностей специалистов в отрасли коммуникационной безопасности, который включает: способность к выявлению коммуникационных угроз, особенностей цивилизованного, манипулятивного и варварского влияния на государственном, корпоративном и личном уровнях, типов манипуляторов, разновидностей манипулятивных ловушек, существующих манипулятивных технологий; возможность использования цивилизованных способов нейтрализации и противодействия манипулятивному влиянию; навыки организации, планирования и реализации своей деятельности в условиях информационных атак; владение коммуникационными, организационными, техническими методами защиты информации в современных информационных системах и сетях.

Ключевые слова: связи с общественностью, коммуникация, компетентность.