

Висновок. Таким чином, можна зробити висновок, що раціональна організація навчально-пізнавальної діяльності сприяє якісному формуванню і розвитку у майбутніх працівників поліції емоційного інтелекту як складника їхньої емоційної, а, отже, й професійної компетентності. Це позитивно впливає на результати практичної професійної роботи правоохоронців з різними категоріями населення, а також на власне самопочуття і здоров'я працівників поліції.

Одним з перспективних напрямків педагогічної роботи з курсантами, на наш погляд, є подальше удосконалення тренінгу емоційного інтелекту та його впровадження у навчальну роботу. Це сприятиме поліпшенню професійної підготовки курсантів як майбутніх офіцерів поліції України.

Список бібліографічних посилань

1. Березюк Г. Емоційний інтелект як детермінанта внутрішньої свободи особистості. *Психологічні студії Львівського університету*. 2003. С. 20–23.
2. Ильин Е.П. Эмоции и чувства. СПб. : Питер, 2002. 752 с.

Одержано 31.10.2019

УДК 316.774-049.5

Олександр Володимирович ТЯГЛО,

доктор філософських наук, професор,
професор кафедри соціально-гуманітарних дисциплін факультету № 6
Харківського національного університету внутрішніх справ;

 <https://orcid.org/0000-0003-0721-1153>;

Тетяна Степанівна ВОРОПАЙ,

доктор філософських наук, професор,
професор кафедри соціально-гуманітарних дисциплін факультету № 6
Харківського національного університету внутрішніх справ;

 <https://orcid.org/0000-0001-6170-5512>

БЕЗПЕЧНЕ СПОЖИВАННЯ ІНФОРМАЦІЇ: КОГО, ХТО І ЯК НАВЧИТЬ?

Поняття інформаційного суспільства чи інформаційного суспільства з паростками суспільств знань виявляється ключовими в осмисленні стану і перспектив розвитку людства зонайменше у першій половині XXI століття. Актуальна інформація цінувалася завжди, але сьогодні у системі людських цінностей вона і різноманітні засоби продукування, оперування нею чи її споживання посідають одне з визначальних місць, перетворившись на превалюючий чинник досягнення успіху як у державній економіці, політиці чи військовій справі, так й у громадському чи приватному житті. Однак не важко зрозуміти, що різноякісне наповнення, скажемо так, інформаційного виміру соціального простору – як фактично і будь-які інші інструментальні цінності – може бути використаним на добро і на зло. А тому виникають загальні проблеми морального і правового унормування цього особливого наповнення, всілякої протидії його непоодиноким негативним виявам.

Україна не стоїть осторонь від зазначених проблем. Так, протягом останніх десятиліть розроблено і уведено в дію низку важливих державних документів, зокрема: закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» (2007) [1], «Стратегія національної безпеки України» (2015), «Стратегія кібербезпеки України» (2016), закон України «Про основні засади забезпечення кібербезпеки України» (2017) [2], «Доктрина інформаційної безпеки України» (2017). Нещодавно під час Другого міжнародного форуму «Кібербезпека. Захисти свій бізнес» актуальність продовження всебічної активності у даному напрямку підтвердив чинний секретар РНБО Олексій Данілов: «Сьогодні питання кібербезпеки є питанням номер один для кожної сучасної країни, а спільне завдання бізнесу й влади – створити реальну дієву систему кіберзахисту, щоб жоден агресор не мав можливості зазіхати на безпеку держави» [3]. Нарешті, не можна не згадати, що 7 жовтня 2019 року заступник секретаря РНБО Сергій Кривонос провів з силовиками закриту координаційну нараду з питань протидії агресії проти України в інформаційній сфері [4]. Таким чином, ефективно вирішення питання кібербезпеки і, ширше, інформаційної безпеки у різних ситуаціях та в різних полях соціального простору мусить бути пріоритетом сучасної наукової й практичної активності. Зрозуміло, що успіху тут не досягти без цілеспрямованої і систематичної активності освітньої.

Хоча поняття інформаційної безпеки і деякі дотичні дотепер дискутуються, у нашій розвідці використовуватимемо закріплене у законодавстві наступне визначення: «Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому 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» [1, ч. III, ст. 13] (порівн., напр., [5]). Вже з цього стає зрозумілим, по-перше, що інформаційна безпека без безпеки споживання інформації людиною, суспільством і державою не має сенсу; по-друге, інформаційної безпеки не можна досягнути без огляду, серед іншого, на зміст – *раціональний чи емоційний, явний або прихований – інформації*, а також без системної протидії продукуванню, поширенню чи рецепції шкідливих за змістом «інформаційних впливів». Ми вважаємо за доречне наголосити на цих фундаментальних

обставинах, оскільки досить часто вони губляться на тлі потреб кіберзахисту, тобто захисту, так би мовити, матеріального наповнення інформаційного виміру соціального простору – носіїв інформації і обладнання, програмного забезпечення, ліній комунікації тощо. Справді, «кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямований на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» [2, ст. 1. п. 7].

Проте чи не, щонайменше, сумірною зі шкодою від хакерських атак на світовий бізнес, яка на рік сягає трильйонів доларів, виявляється шкода від змісту «інформаційних впливів» потужних ботоферм, котрі, уникаючи будь-яких кіберінцидентів і кібератак, намагаються маніпулювати свідомістю багатомільйонних мас та можновладців, розпалювати збройні конфлікти, сприяти розвалу крупних міжнародних союзів або спотворювати вибори керівників провідних держав світу?! І свою частку відповідальності за цю шкоду несуть не тільки ботоферми і замовники їх послуг, а й покликані протидіяти їм державні інституції та, не в останню чергу, непідготовлені споживачі зловмисної інформації.

Розуміння гостроти питання інформаційної безпеки, включаючи безпеку споживання інформації, насамперед веде до думки про освіту здатних розв'язувати це питання фахівців. Звертаючись до чинного переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, знаходимо, що освіта у галузі знань «Інформаційні технології» здійснюється за спеціальністю «125 Кібербезпека», однак спеціальності на кшталт «Інформаційна безпека» тут не зазначено. Звертаючись далі до стандарту вищої освіти на першому (бакалаврському) рівні за спеціальності «Кібербезпека», бачимо, зокрема, що за цілі навчання тут приймається «підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки» [6]. Тож хоча поняття кібербезпеки й інформаційної безпеки розводяться, проте навчання інформаційній безпеці фактично поглинається освітою з кібербезпеки. Наявний дисонанс поглинання ширшого вужчим тут підсилюється ґрунтовною підозрою, що спрямована у такий спосіб освіта втрачає суттєву частину навчання інформаційній безпеці, у тому числі пов'язаної з убезпеченням споживання інформації, виявленням шкідливого змісту і протидією зловмисним «інформаційним впливам». Дійсно, у зазначеному стандарті згадка про протидію якщо і зустрічається, то лише в зв'язку з протидією «отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах», тобто суто у плані кібербезпеки. Збіг вже зазначених обставин веде до висновку: у межах галузі знань «Інформаційні технології» доцільно виділити окрему спеціальність, умовно кажучи «Інформаційна безпека» у роз'ясненому вище розумінні.

Пропонована освітня інновація за своїм наповненням і методами має відрізнятися від інших спеціальностей, що сьогодні асоціюються з галуззю знань «Інформаційні технології». Не випереджаючи зараз ще потрібних для її повного обґрунтування наукових і методичних студій, відмітимо лише дві доволі очевидні обставини. По-перше, пріоритетом тут мусить бути поглиблена підготовка з гуманітарних і соціальних дисциплін, узгоджена з загальнолюдськими цінностями та цінностями української політичної нації. По-друге, з огляду на загальні вимоги до успішного працівника XXI століття особливу увагу слід приділити навчанню критичному мисленню (докладніше див., напр., [7]).

Харківський національний університет внутрішніх справ, традиційно посідаючи провідне місце серед вищих навчальних закладів МВС у підготовці фахівців з кібербезпеки і зберігаючи потужний корпус висококваліфікованих викладачів гуманітарних та соціальних дисциплін, має реальну перспективу впровадження зазначеної освітньої інновації.

Підготовка корпусу кваліфікованих фахівців з інформаційної безпеки є необхідною, але не достатньою умовою убезпечення споживання інформації. Успіх цієї справи не в останню чергу визначається належною підготовкою споживача, плеканням його мотивації активно-критично ставитися до прямих фейків чи прихованих маніпуляцій. Спрямування потрібної підготовки в основному визначається зазначеними вище пріоритетами освіти фахівців з інформаційної безпеки. А здійснюватися вона може як повноважними державними інституціями, так і громадськими організаціями. Так, останнім часом достатньо широко і ефективно виглядає активність Академії Української преси з підвищення медіаграмотності молоді (див., напр., [8]).

Висновки. По-перше, в загальному випадку інформаційна безпека без безпеки споживання інформації не має сенсу. По-друге, інформаційної безпеки не можна досягнути без огляду, серед іншого, на зміст – раціональний чи емоційний, явний або прихований – інформації, а також без системної протидії продукуванню, поширенню чи рецепції шкідливих за змістом «інформаційних впливів». По-третє, успіх у вирішенні питання інформаційної безпеки, включаючи безпеку споживання інформації, потребує підготовки фахівців з вищою освітою за окремою спеціальністю, умовно кажучи, «Інформаційна безпека». Харківський національний університет внутрішніх справ має реальну перспективу впровадження зазначеної освітньої інновації. По-четверте, підготовка корпусу кваліфікованих фахівців з інформаційної безпеки є необхідною, але не достатньою умовою убезпечення споживання інформації. Успіх тут не в останню чергу визначається державно-громадською підготовкою споживача, плеканням його мотивації на основі узгодженої сукупності загальнолюдських цінностей та цінностей української політичної нації активно-критично ставитися до фейків чи маніпуляцій.

Список бібліографічних посилань

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: закон України від 09.01.2007 № 537-V: станом на 28.10.2019 // База даних «Законодавство України» / Верховна Рада України. <https://zakon.rada.gov.ua/laws/show/537-16> (дата звернення: 26.10.2019).

2. Про основні засади забезпечення кібербезпеки України : закон України від 08.07.2018 № 2163-VIII : станом на 28.10.2019 // База даних «Законодавство України» / Верховна Рада України. <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 26.10.2019).
3. Світовий бізнес за рік може зазнати збитків на \$ 6 трильйонів – експерти // Укрінформ. Мультимедійна платформа іномовлення України. 2019. 25 жовтня. URL: <https://www.ukrinform.ua/rubric-economy/2800152-svitovij-biznes-za-rik-moze-zaznati-zbitkiv-vid-kiberatak-na-6-triljoniv-eksperti.html> (дата звернення: 26.10.2019).
4. Силовики за закритими дверима радились, як протидіяти агресії в інформсфері. *Українська правда*. 2019. 8 жовт. URL: <https://www.pravda.com.ua/news/2019/10/8/7228431> (дата звернення: 26.10.2019).
5. Про внесення змін до законів України щодо інформаційної безпеки : проект закону України від 26.11.2018 № 9340 / ініціатори: Котвицький І. О., Тетерук А. А. // Ліга: Закон. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JH77G00A.html (дата звернення: 26.10.2019).
6. Стандарт вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека : затв. і введено в дію наказом М-ва освіти і науки України від 04.10.2018 № 1074 // Міністерство освіти і науки України: офіц сайт. URL: <https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/125-kierbezpeka-bakalavr.pdf> (дата звернення: 26.10.2019).
7. Тягло О. В., Воропай Т. С. Чого навчати у XXI столітті? // Підготовка охоронців правопорядку в Харкові (1917–2017 рр.) : зб. наук. статей і тез доп. на наук.-практ. конф. до 100-річчя підготовки охоронців правопорядку в Харкові. Харків : Харків. нац. ун-т внутр. справ, 2017 С. 285–287. URL: http://www.univd.edu.ua/general/publishing/konf/25_11_2017/pdf/157.pdf (дата звернення: 26.10.2019).
8. Сидоряченко Я. На Полтавщині проходить тренінговий марафон з медіаграмотності для молоді. *Media Literacy*. 2019. 20 лип. URL: <http://medialiteracy.org.ua/na-poltavshyni-prohodyt-treningovyj-marafon-z-mediagramotnosti-dlya-molodi> (дата звернення: 26.10.2019).

Одержано 28.10.2019

УДК 371.132:371.125

Олена Іванівна ФЕДОРЕНКО,

доктор педагогічних наук, професор,

завідувач кафедри педагогіки та психології факультету № 3

Харківського національного університету внутрішніх справ;

 <https://orcid.org/0000-0003-4948-9524>

СКЛАДОВІ СУЧАСНОЇ ПІДГОТОВКИ МАЙБУТНІХ ОФІЦЕРІВ ПОЛІЦІЇ ДО ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ

Підготовка майбутніх правоохоронців до професійної діяльності під час навчання у закладі вищої освіти – цілеспрямований, організований, динамічний процес, інноваційний за своїм характером, адаптований до умов майбутньої професійної діяльності. Результатом підготовки є підвищення рівня готовності курсантів до її самостійного виконання (засвоєння ними відповідних знань; оволодіння вміннями та навичками, необхідними у професійній діяльності; набуття досвіду їх реалізації та творчого застосування; сформованість пізнавальної і професійної мотивації, усвідомлення соціальної необхідності і цінності професії).

Процес навчання у закладі вищої освіти дозволяє сформувати у майбутніх поліцейських необхідні у професійній діяльності знання, уміння, навички (правові, юридичні, соціальні, педагогічні, психологічні та ін.), виховати та розвинути професійно важливі якості особистості. Освітній процес має бути побудований таким чином, щоб забезпечити взаємодію викладача і курсанта, розвиток пізнавальної мотивації та інтересу майбутніх фахівців як до навчання, так і до майбутньої професії; стимулювати курсантів до активного засвоєння і творчого застосування знань та вмінь; виховання професійно важливих якостей особистості, що досягається шляхом відбору відповідного змісту та варіативного застосування викладачем комплексу традиційних та інноваційних методів, прийомів та організаційних форм навчання.

Підготовка майбутніх правоохоронців до професійної діяльності здійснюється через засвоєння курсантами таких елементів змісту підготовки: 1) знання, що складають основу професійної діяльності; 2) досвід здійснення способів діяльності, на основі якого формуються уміння і навички професійної діяльності; 3) досвід творчої діяльності; 4) досвід емоційно-ціннісного ставлення до об'єктів професійної діяльності.

На основі знань у курсантів формується система понять, уявлень, закономірностей з різних галузей наук, що складають наукову основу майбутньої професійної діяльності. Досвід здійснення способів діяльності забезпечує формування у курсантів умінь та навичок професійної діяльності через застосування набутих знань, сприяє формуванню готовності до виконання конкретних дій та оволодіння різними способами їх виконання. Досвід творчої діяльності забезпечує перетворення, зміну якості виконання умінь та навичок майбутньої професійної діяльності. Цей елемент змісту підготовки сприяє творчому ставленню, пошуку нестандартних підходів та рішень при виконанні навчальних та професійних завдань. Досвід емоційно-ціннісного ставлення виконує функцію оцінки людиною значення