

http://www.libussr.ru/doc_ussr/usr_15404.htm(Дата звернення : 08.10.2016). – Назва з екрана.

9. ДАСО. – Р.-102. – Оп. 1. – Спр. 13. – Арк. 14
10. ДАСО. – Р.-1635. – Оп. 1. – Спр. 194. – Арк. 5
11. ДАСО. – Р.-1635. – Оп. 1. – Спр. 200. – Арк. 104
12. ДАХО. – Р.-102. – Оп. 1. – Спр. 13. – Арк. 12

REFERENCES

1. Hrytsak, Ya. (1996). *Narys istoriyi Ukrainy: formuvannya modernoyi ukrayins'koyi natsiyi KhKh – KhKh stolittya*. [Essay on the history of Ukraine: formation of modern Ukrainian nation XIX – XX century]. Kyiv.
2. Zakharchuk, A. (2002). *Derzhavotvorchi poshuky na Slobozhanshchyni v konteksti Ukrayins'koyi revolyutsiyi: Polityko-pravovyy aspekt*. [Creative searches in Slobozhanshchyna in the context of the Ukrainian revolution: Political and legal aspect]. Sumy: «Kozats'kyu val».
3. Mykytyuk, I. (1990). *Zolote dytynstvo*. [Golden childhood]. Symy.
4. Popiv, O. I. (2003). *Deklaratsiya Narkomosvity USRR pro sotsial'ne vykhovannya ditey*. [Declaration of the people's Commissariat of the USSR about the social upbringing of children]. Kyiv.
5. Popil'nyukh, M. (1995). *Po shlyakhu kaydaniv do voli*. [The path of the shackles for freedom]. Kyiv.
6. *Pro orhanizatsiyu vidkrytykh dytyachykh budynkiv: zbirnyk dekretiv, postanov, nakaziv ta rozporyadzen' po Narodnomu Komisariatu osvity URSR. (1920)*. [The organisation of public children's homes: a collection of decrees, regulations, orders and instructions of people's Commissariat of education of the Ukrainian SSR.]. Kharkiv.

7. Halkin, O. (2017). «Holos Okhtyrshchynu» ta yoho tvortsi – [Elektronnyy resurs]. – Rezhym dostupu:

<http://www.okhtyrka.net/content/view/3763/106/>

(Data zvernennya: 02.02. 2017). – Nazva z ekrana.

8. Pro dodatkovi zakhody shchodo vstanovlennya spravedlyvosti po vidnoshennyu do zhertv represiy, yaki mali mistse v period 30-40-kh ta pochatku 50-kh rokiv (iz zm. i dod., vnesenymy z'hidno iz Zakonom SRSR vid 31.07.1989 – Vidomosti SNR i ZS SRSR, 1989, N 9, st. 202) [Elektronnyy resurs]. – Rezhym dostupu : http://www.libussr.ru/doc_ussr/usr_15404.htm (Data zvernennya : 08.10.2016). – Nazva z ekrana.

9. DASO. – R.-102. – Оп. 1. – Спр. 13. – Арк. 14
10. DASO. – R.-1635. – Оп. 1. – Спр. 194. – Арк. 5
11. DASO. – R.-1635. – Оп. 1. – Спр. 200. – Арк. 104
12. DAKhO. – R.-102. – Оп. 1. – Спр. 13. – Арк. 12

ВІДОМОСТІ ПРО АВТОРА

ШТАНЬ Ольга Олексіївна – аспіранта Сумського педагогічного університету імені А. С. Макаренка.

Наукові інтереси: загальна педагогіка та історія педагогіки; менеджмент в освіті.

INFORMATION ABOUT THE AUTHOR

SHTAN Olha Oleksiivna – postgraduate student of Sumy State A. S. Makarenko Pedagogical University

Circle of scientific interests: general pedagogy and the history of pedagogy; educational management.

УДК 378.14: 355.12

ШКАТУЛА Олександр Павлович – старший викладач кафедри суспільних наук Житомирського військового інституту імені С. П. Корольова
e-mail:shkatula_a_p@ukr.net

КІБЕРЗАГРОЗИ НАВЧАЛЬНО-ПІЗНАВАЛЬНИЙ ДІЯЛЬНОСТІ КУРСАНТІВ

Постановка та обґрунтування актуальності проблеми: Характерною ознакою сучасного соціуму є швидкий розвиток інформаційних технологій та їх проникнення в усі сфери суспільного життя. Найбільш яскравим феноменом інформаційних технологій є виникнення віртуального середовища – Інтернету, спроможного вмістити безмежну кількість різної інформації. Існуючі засоби, які забезпечують доступ до його інформаційного

контенту: текстів, зображень, баз даних, аудіо та відео пропонують сучасному викладачеві активно залучати увесь цей потенціал до навчальної роботи. Можливість копіювати, відтворювати, передавати, корегувати та зберігати інформацію, помножена ресурсами всевітньої мережі Інтернет: веб-сайтами, електронною поштою, електронними енциклопедіями, блогами, підкастами, вікі, відеоконференціями та вебінарами, сприймається як нова можливість організації

навчального процесу. Сприяє цьому і активне використання Інтернету молоддю. Так, за даними Інтернет Асоціації України 97% осіб у віці від 15 до 29 років вважають себе регулярними користувачами мережі [1]. У цій віковій ніші перебувають, фактично, сто відсотків курсантів військових вишів. Сприймаючи можливість безперешкодного доступу до ресурсів Інтернету як до знань, накопичених людством, загалом, більшість з них не до кінця усвідомлюють усі небезпеки та ризики всесвітньої павутини. Саме така ситуація актуалізує питання вивчення кіберзагроз, з якими можуть стикнутися курсанти під час використання ресурсів Інтернету.

Аналіз останніх досліджень і публікацій. Аналіз досліджень проблем загроз, які можуть підстерігати особу при використанні Інтернет-мережі зазначає, що ними займається досить велика група фахівців з різних сфер. Це програмісти, спеціалісти із захисту інформації, правозахисники, кіберполіція, медики, психологи та педагоги. Однак питаннями впливу кіберпростору на особистість опікуються здебільшого останні. Зокрема, розглядом питань, пов'язаних із забезпеченням безпеки дітей в Інтернеті, займаються С. Болтівець, І. Литовченко, С. Максименко, М.-Л. Чеп, Н.Бугайова. Вивчають проблематику агресивних дій у мережі, які негативно впливають на людину, Н. Дайнека, Є. Кулик, Л. Найдьонова. Міжнародний досвід у протидії загрозам в інформаційному середовищі вивчають Д. Дубов, О. Запорожець, А. Смірнов, Є. Садовська. Питаннями розроблення актуальних напрямів боротьби з протиправними діями в Інтернеті опікуються В. Гавловський, О. Йона, Н. Казакова, О. Орлов, Ю. Онищенко. Способами виховання культури та правил поведінки користувача всесвітньої мережі Інтернет цікавляться В. Дмитрієва, Н. Гущина, О. Кущенко; А. Кочарян, С. Коноплицький. Досить велика кількість вітчизняних та іноземних науковців вивчають питання вияву, профілактики та запобігання проявам Інтернет-залежності в процесі навчання: Н. Бугайова, В. Бурова, Т. Вакуліч, А. Войскунский, І. Голдберг, Т. Ісакова, Ц. Короленко, В. Лоскутова, О. Мартинова, Н. Сергеева, В. Цап, А. Церковний, К. Янг.

Проте, не дивлячись на активне розроблення проблем негативного впливу Інтернету на особу, реалії, у яких перебуває нині українське суспільство, зокрема, ведення Росією проти України гібридної агресії, активізують кіберзагрози іншого виду, що

спонукає подальше вивчення цього питання.

Метою статті є дослідження теперішнього стану загроз та ризиків, з якими можуть стикнутися курсанти вищих військових навчальних закладів при використанні мережі Інтернет у ході своєї навчально-пізнавальної діяльності.

Виклад основного матеріалу дослідження. Серед загроз, з якими стикається людина у своїй діяльності, останнім часом найчастіше зустрічаються ті, що пов'язані з віртуальним середовищем. Засоби масової інформації насичені термінами «кіберпростір», «кіберзагроза», «кібербезпека», «кібератака», «кібервійна» тощо. Загалом, ці та подібні їм терміни, ототожнюючись, певною мірою, з творами наукової фантастики (оскільки їх поява спричинена романом Уільяма Фон Гібсона «Нейромант»), перебувають поза увагою пересічної особи. Це підтверджується дослідженнями, проведеними Лабораторією Касперського. Аналіз проведеного нею моніторингу користувачів дозволив ввести в обіг поняття «індекс кібернетичної безпеки», який певним чином відображає ступінь вразливості осіб у віртуальному просторі. Значення індексу в Україні виглядає наступним чином: байдуже відносяться до наявності кіберзагроз 86% респондентів, вважають себе вразливими до них – 37%, відчули на собі негативний вплив – 37%. Тобто переважна більшість українських громадян не вірять у те, що вони можуть стати жертвами кіберзлочинців. Для порівняння, загальносвітовий індекс кібербезпеки, за даними лабораторії, виглядає наступним чином: 74%–39%–29% [2].

Розглядаючи поняття кіберпростору, слід зауважити, що його нерідко прирівнюють до поняття Інтернет, оскільки процеси, які відбуваються в них, схожі за змістом, характером та напрямками впливу. Цим прийомом скористаємося і ми у нашому дослідженні.

Під кіберпростором розуміють середовище, створене організованою сукупністю інформаційних процесів на підставі об'єднаних загальними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем незалежно від форми власності [3]. У межах цього середовища інформація зберігається, обробляється, накопичується, забезпечується її вивід, передача, здійснюється комунікація. Аналогічні процеси відбуваються і в Інтернет-мережі.

Сучасний кібернетичний простір є певним віддзеркаленням світу реального.

Процеси, що відбуваються у світі реальному, трансформуються, переносяться у світ кібернетичний. Виникають нові виклики для безпеки і Української держави, і для її громадян. Цьому підтвердженням є прийняття Україною низки правових актів, спрямованих забезпечити безпеку у кіберпросторі:

– Закони України: «Про основи національної безпеки України» від 19.06.2003 № 964-IV; «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 № 2824-IV;

– Укази Президента України: «Про стратегію кібербезпеки України» від 15.03.2016 № 96/2016; «Про стратегію національної безпеки України» від 26.05.2015 № 287/2015; «Про Національний координаційний центр кібербезпеки» від 07.06.2016 № 242/2016; «Про Доктрину інформаційної безпеки України» від 29.12.2016 № 47/2017;

– розпорядження Кабінету Міністрів України «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України» від 10.03.2017 № 155-р.

Аналізуючи зазначені правові акти, можна зробити висновок, що на нинішньому етапі боротьби з кіберзагрозами більшої уваги надається наступним заходам: захисту державних інформаційних ресурсів, інформації; критичної інформаційної інфраструктури ЗСУ, СБУ, банківської системи, запобіганню, виявленню та реагуванню на кіберінциденти, аудиту захищеності інформаційних об'єктів та інше.

Одним з пріоритетних напрямів забезпечення кібербезпеки України визначено: «підвищення цифрової грамотності громадян та культури безпекового поведіння в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадження державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту» [4, ч. 4, ст. 4.1, п. 6].

У межах цього напрямку знаходиться і наше дослідження.

Стрімкий розвиток інформаційних технологій, ускладнення військової техніки, зміна характеру та темпу військово-професійної діяльності призвели до швидкого збільшення обсягу знань, який необхідно засвоїти майбутньому військовому фахівцю. Проте, в умовах військової організації будь-який вид діяльності, в тому числі і навчальної, чітко регламентований у часовому просторі. Саме тому курсанти у процесі підготовки до навчальних занять звертаються до інформаційних ресурсів Інтернету для пошуку необхідної інформації.

За даними нашого опитування, проведеного серед курсантів, кожен з них хоча б раз на добу використовує можливості Інтернету. Основними напрямками використання Інтернет-ресурсів опитувані вказали: спілкування, пошук цікавої інформації, навчання, розваги. При цьому більшість респондентів визнали, що розуміють ризики та небезпеки, пов'язані з використанням Інтернет-ресурсів, стикалися з ними у ході пошукової роботи в мережі, проте не вважають їх досить суттєвими, оскільки, на їхню думку, курсант не являє якоїсь інформаційної чи фінансової цінності. Така ситуація викликає занепокоєння, оскільки нехтування ризиками у кіберпросторі може призвести до різного виду уражень, проте, це свідчить про деяку «кібервтому», наявну у курсантів. Наявність кіберстомленості у певного числа користувачів Інтернету, яка призводить до нівелювання дій із захисту себе у мережі підтверджується дослідженнями Національного Інституту Стандартів та технології США [5].

Серед основних Інтернет-загроз при опитуванні курсантами були названі: заволодіння логінами та пароллями до акаунтів соціальних мереж, загрози фінансового характеру, віруси. Загалом, ці дані корелюються з дослідженням Інтернет-загроз, які проводять консалтингові компанії на замовлення державних агенцій та установ, Інтернет-провайдерів та виробників антивірусного програмного забезпечення. Так, за даними досліджень Української антивірусної лабораторії Zillua серед основних кіберзагроз, що чекають користувача у кіберпросторі, є віруси, які перешкоджають пошуку в Інтернеті, пошкоджують файли з документами, крадуть банківську та особисту інформацію користувачів [6]. Європейське Агентство з мережевої та інформаційної безпеки опублікувало дані п'ятнадцяти основних найбільших кіберзагроз у 2015 році: шкідливий код, мережеві атаки, атаки на веб-додатки, бот-мережі, відмова в обслуговуванні, електронна крадіжка, внутрішня загроза, фішинг, спам, експлойт – комп'ютерний злам, вразливість даних, крадіжка персональних даних, витік інформації, програми-вимагачі, кібершпигунство [7].

Аналіз досліджень кіберзагроз дає можливість зробити висновок про те, що більшість з них мають за основу функціонування певного програмного продукту чи коду, за допомогою яких реалізується негативний вплив інтересам держави, компанії, споживача. Серед них

найбільш небезпечними сприймаються дії, які спрямовані на збій чи відмову у роботі мережевого чи персонального обладнання, тобто загрози технічного характеру і менше хвилюють небезпеки, пов'язані з втратою персональних даних, розміщенням неправдивої інформації чи повідомлень.

Проте, на наш погляд, загрози кіберпростору здатні негативно впливати не тільки на апаратну частину комп'ютера, планшета, смартфона, їхнє програмне забезпечення, стійкість баз даних, а й на психіку їх власників – курсантів, та за рахунок цього змінювати у потрібному напрямку уявлення про сутність та значення подій, спотворювати орієнтири, цінності та мету діяльності.

Поняття «пізнавальна діяльність» має багато визначень, тлумачення яких залежать від запропонованого підходу до розгляду сутності цього процесу. На думку Л. Виготського, пізнавальна діяльність – це «свідома діяльність, спрямована на пізнання навколишньої дійсності за допомогою таких психічних процесів, як сприйняття, мислення, пам'ять, увага, мова» [8]. А. Назаров вбачає у пізнавальній діяльності процеси набуття, інкорпорації та оперування знаннями та вміннями [9]. За Т. Тернавською, пізнавальна діяльність є процесом виявлення активності, спрямованої на об'єкт пізнання [10]. Та усі дослідники згодні в тому, що це активна, свідомо дія. Вона має на меті виявлення сутності явищ та зв'язків навколишньої реальності та реалізується особою впродовж життя у видах діяльності і у суспільних відносинах.

Пізнавальній діяльності курсантів військових вишів України притаманні особливості, спричинені надважливим соціальним призначенням – бути захисником Вітчизни. Пізнавальна діяльність, яка здійснюється курсантами під час навчання у вищих військово-навчальних закладах є основним видом їхньої діяльності та спрямована, перш за все, на успішне освоєння професії офіцера Збройних Сил України. Фактично, це процес відображення у психіці військовослужбовців, які навчаються у середньому або вищому військово-навчальному закладі, предметів та явищ навколишнього середовища, на ґрунті якого формуються знання, виникають цілі та мотиви військово-професійної діяльності. Структурними компонентами цієї діяльності є її зміст, мета, цінності, емоції. З однієї сторони, це засвоєння визначеного навчальними програмами переліку знань, набуття навиків та вмінь необхідних для виконання завдань за призначенням, з іншої –

формування професійно-важливих якостей та ціннісних настанов.

Оскільки навчання є цілеспрямованим педагогічним процесом організації й стимулювання активної навчально-пізнавальної діяльності учнів з оволодіння науковими знаннями, вміннями й навичками, процесом розвитку творчих здібностей, світогляду, морально-естетичних поглядів і переконань, то розуміння сутності Інтернет-загроз викладачем та курсантом є передумовою безпечного використання його ресурсів у навчально-пізнавальній діяльності [11]. І треба зазначити, що окрім надання майбутньому фахівцю необхідних професійних характеристик, у педагогічному процесі значна частина уваги відводиться на формування світогляду, морально-етичних цінностей особистості.

Події останніх років, що передували Революції Гідності, виявилися насичені інформаційними впливами, спрямованими на вимивання національної свідомості, підтриманням стереотипу про «братські слов'янські народи». Не останньої ролі у цьому процесі відігравали ресурси, розміщені у Інтернет-мережі.

Здійснюючи агресивні дії проти України Російська Федерація примножує спроби та розширює перелік засобів впливу на ідеї, ідеали, принципи та погляди українців. І чільне місце відводиться мережі Інтернет з її інформаційними та комунікаційними можливостями. До таких спроб можна віднести хибні чи фейкові інформаційні повідомлення, фотографії, ілюстрації, зображення, аудіо та відеотвори, записи трансляцій подій та передач, слогани, мотиватори, пости соціальних мереж різноманітного провокаційного змісту. Вони покликані відволікти увагу курсантів, забити канали сприйняття інформації різноманітними «резонансними» повідомленнями, принизити національних лідерів та державних діячів, посіяти сумнів у правильності свого вибору. Саме з цим стикаються курсанти у Інтернеті під час пошуку необхідної навчальної інформації чи під час спілкування у соцмережі. Не будучи озброєним дієвими механізмами протидії цим негативним інформаційним впливам, або просто не розуміючи їх спрямованість, курсанти мимоволі зазнають численних мотиваційних та змістових деформацій світогляду.

Зауважимо: при проведенні опитування ніхто з курсантів не вказав на те, що він проводить перевірку знайденої на певному Інтернет-ресурсі інформації за рахунок інших електронних чи друкованих джерел. Схожа

ситуація наводиться професором Університетського коледжу в Лондоні Я. Роуландсом. За даними досліджень пошук інформації у мережі Інтернет відбувається за заголовками, змістом й короткою анотацією, при цьому 60 % користувачів мережі переглядає не більше трьох перших сторінок і до 65 % з них ніколи не повертаються до переглянутого, оцінка авторитетності ресурсу і ступінь довіри до нього відбуваються миттєво, інформація не часто перевіряється на інших сайтах і в інших пошукових системах [12].

Отже, нині серед кіберзагроз, з якими стикаються у процесі навчально-пізнавальної діяльності курсанти, окрім тих, що перешкоджають доступу до Інтернету, ускладнюють пошук інформації, здатні заволодіти персональними даними, логінами та паролями, активізуються інформаційні кіберзагрози, які мають напрямком впливу когнітивну, мотиваційну та емоційно-вольову сфери.

Вивчення досліджень імовірних наслідків негативного впливу інформаційних кіберзагроз на особистість, дає можливість виокремити серед них наступні:

- по-перше, інформаційні, або пізнавальні:
 - формування поверхневого сприйняття подій як наслідок перегляду великої кількості інформації,
 - спотворення уявлень у результаті використання неперевіреної інформації;
- по-друге, емоційно-вольові:
 - роздвоєння особистості – Я-реальний і Я-віртуальний,
 - прагнення уникнути соціальних контактів у реальному житті,
 - виникнення синдрому дефіциту уваги,
 - втрата почуття співпереживання, емпатії;
- по-третє, біологічні:
 - поява у особи Інтернет-залежності,
 - зменшення рівня розвитку гіпокампу та порушення короткотривалої пам'яті як наслідок того, що у мережі можна знайти відповідь на будь-яке запитання.

Про реальність існуючих кіберзагроз для ціннісно-мотиваційної та смислової сфери доводять: моральна паніка у суспільстві, що виникла, як результат повідомлень про наявність у соцмережах суїцидальних «груп смерті», гри «Синій кит», чи пропозиції посадових осіб держави заборонити діяльність соціальних мереж «Вконтакте» та «Однокласники» як поширювачів антиукраїнського контенту.

Гібридний характер агресивних дій Росії на фоні всеосяжного проникнення Інтернету

у військову діяльність привертає увагу до інформаційних впливів у кібернетичному просторі та вимагає активізувати роботу по розробці заходів, які б сприяли протидії кіберзагрозам у процесі навчально-пізнавальної діяльності курсантів. Їх умовно можна об'єднати у заходи адміністративного, організаційного, світоглядного характеру.

Адміністративні: блокування шляхів доступу до Інтернет-мережі, вилучення чи заборона використання пристроїв, що надають доступ до Інтернету, заборона використовувати мережу конфіденційно.

Організаційні: створення локальних захищених інформаційних мереж, визначення переліку безпечних та «правдивих» інформаційних ресурсів, контроль за використанням інформаційних ресурсів, протидія ідентифікації осіб у мережі шляхом використання нік-неймів, керівництво процесом використання інформаційних ресурсів.

Світоглядні: формування у курсантів вміння критично сприймати одержану інформацію; аналізувати її походження, сферу впливу, призначення, шукати протилежні точки зору, розробляти систему доказів істинності цієї інформації та виважено приймати рішення.

Висновки і перспективи подальших розвідок напряму. Таким чином, Інтернет сьогодні – це місце зіткнення інтересів держав, різних соціальних груп, засіб впливу на особистість та людські спільноти, інструмент формування моральних приписів та настанов, способів поведінки, сфера вираження емоцій та почуттів. Одночасно, він залишається дієвим засобом активізації пізнавальної діяльності курсантів. Використання його при підготовці військових фахівців, з огляду на їх соціальне призначення, вимагає виваженого системного підходу. Легковажне ставлення до кіберзагроз у процесі підготовки військових фахівців може завдати шкоди бойовій готовності. Під впливом спотвореного інформаційного впливу виникає небезпека викривлення у курсантів світоглядних настанов, деформація або зміна їхніх моральних та життєвих цінностей. Основою подальших досліджень може бути розробка методик використання Інтернету у навчанні військових фахівців, створення та впровадження у освітній процес навчальних курсів та дисциплін, які вивчають способи безпечної поведінки у кіберпросторі.

СПИСОК ДЖЕРЕЛ

1. Дані досліджень Інтернет-аудиторії України. Дані установчих досліджень у I кварталі 2017 року. [Електронний ресурс]. – Режим

доступу:

http://inau.ua/sites/default/files/file/1704/i_kvartal_2017.pptx. – Назва з екрану.

2. Индекс Кібербезпеки Касперського. Дані установчих досліджень у 2 півріччі 2016 року. [Електронний ресурс]. – Режим доступу: <https://index.kaspersky.com/app/all/ukraine-h22016-all-all?global=0>. – Назва з екрану.

3. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія / Д. В. Дубов. – К.: НІСД, 2014. – 328 с.

4. Стратегія кібербезпеки України: за станом на 15 бер. 2016 р. / Верховна Рада України. [Електронний ресурс]. – Режим доступу <http://zakon0.rada.gov.ua/laws/show/96/2016> – Назва з екрану.

5. Security Fatigue. Can Cause Computer Users to Feel Hopeless and Act Recklessly, New Study Suggests. [Електронний ресурс] / B. Stanton, M. Theofanos, S. Prettyman, S. Furman // IT Professional (Volume: 18, Issue: 5, Sept.-Oct. 2016) Pages: 26–32. – Режим доступу: <https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly> – Назва з екрану.

6. Вірусна активність в Україні: троянські програми атакують частіше. [Електронний ресурс]. – Режим доступу: <http://zillya.ua/virusna-aktivnist-v-ukra-ni-troyanski-programi-atakuyut-chastishe> – Назва з екрану.

7. Топ-15 кіберзагроз в 2015 р. Європейське Агентство з мережевої та інформаційної безпеки.. [Електронний ресурс]. – Режим доступу: https://www.kv.by/sites/default/files/img_0992.jpg – Назва з екрану.

8. Выготский Л. С. Педагогическая психология / Л. С. Выготский. – М. : Педагогика, 1991. – 387 с.

9. Назаров А. И. Обобщенная модель познавательной деятельности индивида / А. И. Назаров // Психологическая наука и образование : журнал / гл. ред. Рубцов В. В. – 2000. – № 3. – С. 40–60.

10. Тернавська Т. А. Педагогічні умови активізації пізнавальної діяльності студентів ВНЗ у процесі вивчення психолого-педагогічних дисциплін / Т. Тернавська // Психолого-педагогічні проблеми сільської школи: зб. наук. праць / Уманський держ. пед. ун-т ім. П. Тичини. – Умань: Софія, 2008. – С. 96–102.

11. Харламов И. Ф. Педагогика / И. Ф. Харламов - М. : Высшая школа, 1990. – 576 с.

12. Роуландс Я. Информационное поведение будущих исследователей [Текст] / Ян Роуландс, пер. Е. И. Зиминной // Библиотечное дело – XXI век. – 2009. – № 1. – С. 222–247.

2017 року. [The data of research of the Internet audience of Ukraine. The data of constituent studies in the first quarter of 2017]. [Elektronnyj resurs]. Rezhym dostupu: http://inau.ua/sites/default/files/file/1704/i_kvartal_2017.pptx.

2. Indeks Kiberbezpeky Kasperskogho. Dani ustanovchykh doslidzhenj u 2 pivrichchi 2016 roku. [The Index Of Cyber Security Virus. The data of constituent studies in the 2nd half of 2016]. [Elektronnyj resurs]. Rezhym dostupu: <https://index.kaspersky.com/app/all/ukraine-h22016-all-all?global=0>.

3. Dubov, D. V.(2014). *Kiberprostir jak novyj vymir gheopolitychnogho supernyctva: monoghracija*. [Cyberspace as a new dimension of geopolitical rivalry: the monograph]. Kyiv.

4. *Strateghija kiberbezpeky Ukrajinj: za stanom na 15 ber. 2016 r.* [Cybersecurity strategy of Ukraine] / Verkhovna Rada Ukrajinj. [Elektronnyj resurs]. Rezhym dostupu <http://zakon0.rada.gov.ua/laws/show/96/2016>

5. Security Fatigue. Can Cause Computer Users to Feel Hopeless and Act Recklessly, New Study Suggests. [Electronic resource] / B. Stanton, M. Theofanos, S. Prettyman, S. Furman // IT Professional (Volume: 18, Issue: 5, Sept.-Oct. 2016) Pages: 26 – 32. – Available online: <https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly>.

6. *Virusna aktyvnistj v Ukrajinj: trojanski programi atakujutj chastishe.* [the activity of a virus in Ukraine: the Trojans attack more often]. [Elektronnyj resurs]. Rezhym dostupu: <http://zillya.ua/virusna-aktivnist-v-ukra-ni-troyanski-programi-atakuyut-chastishe>.

7. *Top-15 kiberzagroz v 2015 r. Jevropejskje Aghenstvo z merezhevoji ta informacijnoji bezpeky.* [Top 15 cyber-threats in 2015] / [Elektronnyj resurs]. Rezhym dostupu: https://www.kv.by/sites/default/files/img_0992.jpg

8. Vygotskij, L. S. (1991). *Pedagogicheskaja psihologija*. [Educational psychology]. Moscow.

9. Nazarov, A. I. (2000). *Obobshhennaja model' poznavatel'noj dejatel'nosti individa*. [A generalized model of the cognitive activity of the individual]. Moscow.

10. Ternavsjska, T. A. (2008). *Pedagoghichni umovy aktyvizaciji piznavaljnoji dijajlnosti studentiv VNZ u procesi vuvchemja psykologhopedagoghichnykh dyscyplin*. [Pedagogical conditions of activation of cognitive activity of students in the process of studying psychological and pedagogical disciplines]. Umanj: Sofija.

11. Harlamov, I. F. (1990). *Pedagogika*. [Pedagogy]. Moscow.

12. Roulands, Ja. (2009). *Informacionnoe povedenie budushhih issledovatelej*. [Information behaviour of future researchers]. Moscow.

REFERENCES

1. *Dani doslidzhenj Internet-audytorijj Ukrajinj. Dani ustanovchykh doslidzhenj u I kvartali*

ВІДОМОСТІ ПРО АВТОРА

ШКАТУЛА Олександр Павлович – старший викладач кафедри суспільних наук Житомирського військового інституту ім. С. П. Корольова, підполковник запасу.

Наукові інтереси: інформаційні технології в навчальному процесі, особистість у кіберпросторі, формування психологічної стійкості військовослужбовців.

INFORMATION ABOUT THE AUTHOR

SHKATULA Alexander Pavlovich – senior lecturer of social Sciences Department of the Zhytomyr military Institute of Sergei Korolev Zhytomyr Military Institut, reserve colonel

Circle of scientific interests: information technology in the educational process, personality in cyberspace, the formation of psychological stability of troops.

УДК: 37(09)

БОЙКО Наталя Олександрівна –

аспірант кафедри педагогіки та освітнього менеджменту
Центральноукраїнського державного педагогічного університету
імені Володимира Винниченка
e-mail: spinelly86@ukr.net

ПІДГОТОВКА ПЕДАГОГІЧНИХ ПРАЦІВНИКІВ ЗАСОБАМИ РЕФЛЕКСОЛОГІЇ У КИЇВСЬКОМУ ІНСТИТУТІ НАРОДНОЇ ОСВІТИ

Постановка та обґрунтування актуальності проблеми. Розбудова української держави, соціально-економічна та політична трансформація суспільства зумовили необхідність кардинального оновлення освітніх процесів, а отже зміну наукової концепції формування особистості педагога в системі вищої педагогічної освіти.

Розв'язання цієї проблеми можливе на основі ґрунтовного аналізу історико-педагогічного досвіду становлення і розвитку національної вищої педагогічної школи та професійної підготовки педагогічних працівників.

Аналіз останніх досліджень і публікацій. Фундаментальними щодо проблем історії вищої педагогічної освіти України є праці різних часів Н. Дем'яненко, Т. Корнейчика, Ф. Корольова, І. Лікарчука, В. Майбороди, Ф. Паначина, З. Равкіна, В. Чавдарова, М. Ярмаченка, Г. Ясницького. Питання професійно-педагогічної підготовки, методи, прийоми роботи вчителя в 20-30-х рр. вивчалися дослідниками Л. Вовк, Н. Гузій, С. Гусевим, Н. Калениченко, П. Груздевим, О. Сухомлинською, М. Зотіним, О. Радул, М. Рубінштейном та ін. Питанням розвитку української школи рефлексології займалися В. Протопопов, О. Залужний, І. Соколянський, А. Володимирський, Г. Костюк, Я. Чепіга.

Рефлексологія знайшла своє відображення і в суто педагогічній літературі. Найвідомішими працями, в яких у 1925–1929 рр. популяризувалася рефлексологія були «Рефлексологічний підхід в педагогіці»

А. Дернової-Ярмоленко, «Рефлексологія і педагогіка» І. Арямова, «Учіння про умовні рефлекси як основа педагогіки» Ю. Фролова.

Найбільш виважено й ґрунтовно витоки та основи розвитку української школи рефлексології було проаналізовано О. Сухомлинською в роботі «Нариси історії українського шкільництва» (1996).

Рефлексологія як навчальний предмет в інститутах народної освіти недостатньо проаналізована в сучасній історико-педагогічній науці.

Метою статті є з'ясування історії викладання рефлексології при підготовці вчительських кадрів у Київському інституті народної освіти.

Виклад основного матеріалу дослідження. З утвердженням радянської влади в Україні в 20-х роках стара освітня система була повністю зруйнованою: ліквідовано середні школи, семінарії, університети, а сама система стала зорієнтованою на соціальне виховання дітей, на професійну освіту молоді і дорослих. Це наклало відбиток в цілому на педагогічні вищі навчальні заклади. Вони були реорганізовані в Інститути народної освіти та 3-річні педагогічні курси, причому базою організації ІНО слугували колишні університети. Теоретики і практики педагогічної науки України М. Зарецький, Д. Орехов, Я. Ряпло, М. Шатунов акцентували на тому, що особливо університети гальмували швидкий і рішучий перехід до педагогічного типу вищого навчального закладу освіти і не могли