УДК 378.126:004.056

Олексюк Василь Петрович
кандидат педагогічних наук, доцент, доцент кафедри інформатики та методики її викладання
Тернопільський національний педагогічний університет імені Володимира Гнатюка, м. Тернопіль, Україна
ORCID ID 0000-0003-2206-8447
oleksyuk@fizmat.tnpu.edu.ua

Олексюк Олеся Романівна
кандидат педагогічних наук, викладач кафедри методики та змісту навчальних предметів
Тернопільський обласний комунальний інститут післядипломної педагогічної освіти, м. Тернопіль, Україна
ORCID ID 0000-0002-1454-0046
o.oleksyuk@ippo.edu.te.ua

СТАН СФОРМОВАНОСТІ КОМПЕТЕНТНОСТЕЙ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МАЙБУТНІХ УЧИТЕЛІВ ІНФОРМАТИКИ

Анотація. У статті досліджено поняття кібернетичної й інформаційної безпеки. На основі аналізу науково-методичної літератури доведено, що кібербезпека, як стан захищеності комп'ютерних систем, не може бути забезпечена повною мірою без інформування та роз'яснення користувачам принципів і правил інформаційної безпеки. Авторами проаналізовано специфіку навчання майбутніх учителів інформатики у контексті розвитку у них компетентностей, що необхідні для безпечної діяльності студентів у комп'ютерних мережах. Досліджено види загроз, які виникають внаслідок упровадження у навчальний процес різних сервісних моделей хмарних технологій. Описано методику й етапи педагогічного дослідження кореляції когнітивно-операційного й особистісно-рефлексивного складників фахових компетентностей майбутніх учителів інформатики.

Ключові слова: кібербезпека; інформаційна безпека; майбутній учитель інформатики; компетентність; хмарні технології; педагогічний експеримент.

1. ВСТУП

Постановка проблеми. Інформаційні технології породжують проблеми, які пов'язані із ситуаціями втручання у приватне життя людини, знищення особистих або корпоративних даних. З розвитком технологій комп'ютерних мереж виникають нові можливості для збирання, обробки, об'єднання та зберігання даних, що призводить до трансформації концепцій довіри, безпеки та конфіденційності. У процесі діяльності, яка опосередкована засобами ІКТ, у психіці особистості можуть виникати стани невизначеності та тривоги за власну інформаційну безпеку, які зменшують довіру до ресурсів мережі.

Нині чимало вищих навчальних закладів готують фахівців у галузі кібербезпеки. Проте системне розв'язання проблеми можливе за умови розвитку компетеностейз інформаційної безпеки, зокрема навичок безпечної діяльності в комп'ютерних мережах та Інтернеті. Зазначений процес повинен бути неперервним і здійснюватися упродовж усього життя, починаючи із загальноосвітньої школи. У цьому контексті важливою проблемою є навчання вчителів інформатики основ інформаційної безпеки. Наразі зазначеній проблемі приділяється недостатня увага – відповідна підготовка у педагогічних ВНЗ має епізодичний характер.

Аналіз останніх досліджень і публікацій. Чимало науковців у галузі методики застосування засобів ІКТ в освіті присвячують свої дослідження проблематиці інформаційної безпеки учасників навчально-виховного процесу.

Теоретичні аспекти інформатизації освіти, зокрема проблеми безпечного використання комп'ютерно-орієнтованих засобів навчання, досліджені у працях В. Ю. Бикова, А. М. Гуржія, М. І. Жалдака, О. Г. Глазунової, В. М. Кухаренка, Н. В. Морзе, Л. Ф. Панченко, С. А. Ракова, Ю. С. Рамського, О. М. Спіріна, С. О. Семерікова, О. В. Співаковського, Ю. В. Триуса, М. П. Шишкіної та інших.

Методологічною основою проблем інформаційної безпеки є філософія розвитку інформаційного суспільства й інформатизації освіти. Як зазначає Ю. С. Рамський невід'ємними складниками цих процесів є підготовка компетентних, високої культури фахівців, створення інформаційних ресурсів, що спрямовані на досягнення високого рівня якості та безпеки життя людей в національних і глобальних масштабах [1]Серед проблем інформаційної безпеки окремо виділяють проблему статусу самої інформації. При цьому постає питання щодо правильного співвідношення між даними, інформацією, знанням і четвертою категорією, яка сьогодні ще слабо окреслена, — мудрістю [2]. Отож, здатність розуміти s протистояти загрозам, які виникають внаслідок діяльності в комп'ютерних мережах, є складовою інформаційної культури особи.

В. Ю. Биков, досліджуючи проблематику навчального середовища відкритої освіти, серед вимог до його складу і структури виділяє вимоги щодо забезпечення інформаційно-комунікаційні потреб учасників навчально-виховного процесу, захисту засобів, технологій та інформаційних ресурсів від несанкціонованого доступу [3]. Розробленню методики забезпечення інформаційної безпеки старшокласників у комп'ютерно орієнтованому навчальному середовищі присвячені дослідження О. М. Спіріна та В. Н. Ковальчук [4]. Проблеми оцінювання компетентностей педагогів та учнів досліджуються у публікаціях В. Ю. 00Бикова, О. В. Овчарук, О. М. Спіріна та інших [5].

Н. П. Дементієвська зауважує, що вітчизняні педагогічні університети України не мають спеціальних навчальних дисциплін з формування критичного оцінювання ресурсів Інтернету [6]. Проте у підручниках і методичних розробках Н. В. Морзе, В. П. Вембер, О. В. Барни, О. Г. Кузьмінської у межах концепції навчання через діяльність чимало уваги приділено формуванню в учнів навичок критичного мислення [7]. У дослідженнях В. Ю. Бикова та М. П. Шишкіної міститься аналіз кіберзагроз, які виникають внаслідок впровадження в освітній процес хмарних технологій [8].

Мета статті. Проаналізувати вітчизняний і зарубіжний досвід забезпечення інформаційної безпеки у галузі освіти. Визначити основні складники фахових компетентностей майбутніх учителів інформатики, які стосуються їх інформаційної безпеки. Експериментально дослідити взаємозв'язок між когнітивно-операційним та особистісно-рефлексивним складниками фахових компетентностей з інформаційної безпеки у студентів спеціальності "014.09. Середня освіта. Інформатика".

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Теоретичну основу дослідження складають положення філософії інформаційного суспільства інформатизації освіти, теорія інформаційної безпеки і методологія захисту інформації, концепції розвитку особистості у навчально-виховному процесі, системний, особистісно-діяльнісний, компетентнісний та культурологічний підходи організації навчально-виховного процесу.

3. МЕТОДИКА ДОСЛІДЖЕННЯ

Під час дослідження використовувались такі методи: аналіз науково-методичної і технічної літератури у галузі інформаційної безпеки, хмарних технологій, офіційні документи Європейського Союзу, укази Президента України та державні стандарти вищої освіти. У процесі експериментального дослідження були застосовані методи спостереження, анкетування, експертних оцінок. Анкетування респондентів було проведене згідно методики Лайкерта з подальшою обробкою його результатів за допомогою методів математичної статистики.

4. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Інформаційна безпека традиційно визначається багатьма джерелами, як захист інформації від несанкціонованого доступу, розголошення, порушення, модифікації чи знищення [8]. У Національній доктрині інформаційної безпеки України інформаційну безпеку визначають як стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завданню шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій [9, 10].

Поряд з поняттям "інформаційна безпека" нині досить часто зустрічаємо термін "кібербезпека" (комп'ютерна безпека), під яким розуміють стан захищеності комп'ютерних систем та мереж. Якщо завдання комп'ютерної безпеки зосереджені на захисті даних, що опрацьовуються й передаються в технічних системах, то завдання інформаційної безпеки пов'язані з діяльністю користувача тобто полягають в захисті його інформації, не залежно від носія, на якому зберігаються відповідні дані [11].

Інформаційна і комп'ютерна безпека є особливо актуальними для України, оскільки ми перебуваємо у стані гібридної війни, одними із способів ведення якої є інформаційні і кібернетичні атаки. Враховуючи, що комп'ютерні мережі утворюють основу критично важливої інфраструктури сучасної держави, то інформаційну безпеку слід вважати важливим складником національної безпеки.

Розглядаючи співвідношення понять "інформаційна безпека" і "кібербезпека", постає актуальне питання щодо правильного розуміння понять"дані" та "інформація". У трактуванні інформаційної безпеки слід розглядати такі, притаманні лише людині, стани довіри та ідентичності, на яких засновані взаємодія і спілкування людей. Безпека комп'ютерних систем заснована на поняттях і процесах автентифікації та авторизації. При встановлені відповідності між станами особистості та цифровими функціями інформаційних систем їх розробникам і користувачам важливо розуміти, як можна зберегти механізми довіри та ідентифікації. Потреба конфіденційності виникла в суспільстві не лише як механізм захисту корпоративних прав, але і як зацікавленість особистості у забезпеченні власної свободи. Базові принципи конфіденційності відображені у статті 12 Загальної декларації прав людини Організації Об'єднаних Націй. Європейський Союз впровадив комплексну правову базу щодо захисту конфіденційності, зокрема законодавчо визначив принципи та правила щодо захисту фізичних осіб стосовно обробки їх особистих даних [12]. Чимало користувачів не усвідомлює, що при перегляді Інтернет-сайтів існує можливість опрацювання та зберігання їх особистих даних та операцій не лише розробниками веб-сторінок, а й сторонніми особами. Масове збирання даних через соціальні мережі, профілювання перегляду інформаційних ресурсів, створює ефект "цифрової тіні" особи [13].

Порушення кібербезпеки несумісні із захистом особистої інформації. Проте кібербезпека, як стан захищеності комп'ютерних систем і мереж та даних, які зберігаються та опрацьовуються в них,є необхідною, але недостатньою умовою"інформаційної безпеки". Основні цілі інформаційної безпеки пов'язані з збереженням конфіденційності, цілісності та доступності даних [145 I.A. – Confidentiality, Integrity, Availability). Конфіденційність даних передбачає, що вони є доступними лише уповноваженим особам. Дані є цілісними, якщо вони є точними і повними, а також захищеними від втручань і зміни зі сторони неавторизованих осіб. Доступність передбачає забезпечення того, що дані й обчислювальні ресурси є доступними для тих, хто має право використовувати їх, коли це потрібно. Втрата доступності означає, що дані або система недоступні користувачам, коли їм це необхідно.

Незважаючи на те, що зазначені принципи є базовими, фахівці у галузі інформаційної безпеки зауважують, що використання технічних засобів без належного залучення роз'яснення користувачам аспектів інформаційної безпеки не дає достатніх результатів [16[.

Аналіз документації і стандартів вищої школи показує, що питання інформаційної та кібербезпеки є важливою складовою підготовки майбутніх фахівців у галузі комп'ютерних наук як в Україні, так і за кордоном. Навчальні курси передбачені в університетьких програмах підготовки Європейського союзу [17] та США [18]. У 2001 році в Техаському університеті (UTSA – University of Texasat SanAntonio) був створений Центр гарантування безпеки IT-інфраструктури (CIAS – Center for Infrastructure Assurance and Security), одним з основних завдань якого є навчання та практична підготовка студентів до захисту інформаційних систем [19[.

Вітчизняні університети також здійснюють підготовку фахівців у галузі захисту інформаційних технологій. Зокрема у 2016 році в Україні затверджено стандарт спеціальності "125. Кібербезпека", у якому визначено загальні та спеціальні компетентності бакалаврів з кібербезпеки [20].

Поряд з фаховою підготовкою важливе значення має поінформованість користувачів комп'ютерних систем. Європейське агентство мереж та інформаційної безпеки (ENISA – European Union Agency for Network and Information Security) визначає рівень поінформованості як компоненту стратегії організації в організації освіти. Концепція визначає поінформованість користувачів як "першу лінію оборони" корпоративних мереж [21[.

Враховуючи, що проблеми інформаційної та кібернетичної безпеки мають вагоме значення в освіті, доцільним вважаємо дослідження процесів формування фахових компетентностей майбутніх та і практикуючих учителів інформатики. У проекті стандарту підготовки бакалаврів зі спеціальності "0.14.09. Середня освіта (Інформатика)"серед предметних компетеностей фахівця визначено здатність формувати уміння безпечної діяльності школярів у комп'ютерній мережі та здатність впроваджувати засоби і методи захисту інформації та безпеки в мережі Інтернет.

Як відомо поняття компетентності включає не лише когнітивну та операціонально-технологічну складові, але й мотиваційну, етичну, соціальну і поведінкову, систему ціннісних орієнтацій, звички тощо [22]. У колективні монографії [23] серед стандартів ІК-компетентностей педагогів та учнів виділено окремий – "безпека і приватність". Він містить вимоги,які розподілені у 5-ти складниках:

1. Знання про загрози – користувач усвідомлює, що дані, розміщені в Інтернеті, можуть бути доступними стороннім особам; розуміє ризики, які пов'язані з електронним листуванням, завантаженням програм, прийняттям запрошень у соціальних мережах.

2. Уміння запобігти небезпекам в Інтернеті – користувач адекватно реагує на залякування, агресію, насилля, пов'язані з небезпечними стосунками в Інтернеті; створює надійні паролі; уміє класифікувати листи як спам.
3. Здійснення контролю за інформацією, що передбачає забезпечення конфіденційності власних паролів, критичне оцінювання достовірності отриманої з мережі інформації, усвідомлення загроз, пов'язаних з публікуванням відомостей про себе, розрізнення публічної та приватної інформації, розпізнавання небезпечних мережних контактів тощо.
4. Усвідомлення відмінностей між комунікацією в мережі й спілкуванням поза Інтернетом.
5. Застосування гігієнічних засад, пов'язаних із використанням комп'ютера.

Аналіз науково-педагогічних праць дослідників компетентнісного підходу дозволив виділити основні компоненти професійних компетентностей вчителя інформатики: мотиваційно-ціннісний, організаційно-змістовний, когнітивно-операційний та особистісно-рефлексивний.

Проаналізуємо діяльність учасників навчально-виховного процесу, як користувачів інформаційно-освітнього середовища, й визначимо взаємозв'язок компетентностей, які стосуються їх інформаційної безпеки. Для ефективного провадження професійної діяльності учитель інформатики повинен володіти належним рівнем фундаментальної підготовки, зокрема розуміння принципів функціонування комп'ютерних систем і загроз, які виникають внаслідок несанкціонованого доступу до них і як наслідок розуміти важливість інформаційної безпеки. Важливим є поведінковий, особистісно-рефлексивний складник, який передбачає трансформацію знань у навички безпечної діяльності та рефлексію власних дій.

Поведінка залежить не лише від знань людини, а й від її світогляду, переконань, ставлень, почуттів. Усі ці поняття є складниками інформаційної культури, як процесу, в ході якого особистість пізнає й перетворює інформаційне середовище, реалізуючи свої здібності, потреби й прагнення. У структурі інформаційного світогляду вчителя інформатики виділяють здатність до усвідомлення проблем інформаційної безпеки та кіберзлочинності, а також усвідомлення ризиків, які супроводжують інформаційну діяльність [24[. Аксіологічною стороною інформаційного світогляду є усвідомлення відповідальності за наслідки діяльності в інформаційно-освітньому середовищі. Недотримання у навчальному закладі правил безпеки може призвести до небажаних наслідків:

- знищення або пошкодження важливих даних для навчального закладу (документація, навчальні матеріали, засоби оцінювання навчальних досягнень);
- несанкціоноване одержання і розповсюдження персональних даних учнів, учителів, адміністрації;
- поширення серед молоді шкідливого контенту, який пропагує жорстокість, насильство, порнографію, окультизм;
- зростання витрат на інформаційну безпеку навчального закладу;
- репутаційні наслідки.

Інформаційну безпеку комп'ютерної мережі розглядають у трьох аспектах: фізичному, технічному та адміністративному. Фізичний аспект передбачає обмеження доступу сторонніх осіб до приміщень школи, у яких знаходяться комп'ютери, сервери, комутаційне обладнання;технічний – використання пристроїв і програмних засобів, призначених для захисту операційних систем та мереж; адміністративний – включає в себе керівні принципи ті правила організації навчального процесу з використанням інформаційних технологій.

Якщо взяти за основу походження загроз, то їх можна класифікувати як внутрішні

та зовнішні. Внутрішні загрози більшою мірою стосуються інформаційної безпеки та виникають як несистематичні порушення безпеки, пов'язані з діяльністю некомпетентних або недоброчесних користувачів. Зовнішні загрози стосуються кібербезпеки і спричиняються внаслідок дій вірусів хакерських атак, шахрайських маніпуляцій, надсилання спаму тощо. У контексті зовнішніх загроз постає питання відповідальних за розгортання та технічний супровід інформаційно-освітніх середовищ навчальних закладів. В університетах і коледжах зазначені завдання виконують окремо створені підрозділи (центри обслуговування комп'ютерних мереж, відділи дистанційного навчання). У загальноосвітніх школах проблема залишається невирішеною. Зазвичай завдання щодо технічного супроводу комп'ютерної мережі виходять за межі посадових обов'язків учителів інформатики. Через недофінансування системи загальної освіти у школах відсутні фахівці відповідної спеціалізації, або їх кваліфікація бажає бути кращою. За таких умов супровід інформаційно-освітніх середовищ навчальних закладів можливий згідно аутсорсингової моделі [25]. На нашу думку, її впровадження вимагає науково-методичного і технічного обґрунтування, а також централізованої координації та контролю з боку органів державної влади.

На користь аутсорсингової моделі свідчить широке впровадження в галузі освіти хмарних технологій. Як наслідок інформаційно-освітнє середовище навчального закладу трансформується у хмаро-орієнтоване. Проте поряд із перевагами повсюдності, гнучкості налаштувань, фінансового заощадження ресурсів використання хмарних технологій привносить й додаткові ризики. Вони пов'язані з тим, що специфіка функціонування хмаро-орієнтованого навчального середовища не завжди відображена у керівних положеннях і правилах інформаційної безпеки освітнього закладу. Наслідком впровадження хмарних технологій є надання студентам повсюдного доступу до обчислювальних ресурсів корпоративної мережі університету. Досить часто такий доступ здійснюється з відкритих, загальнодоступних мереж, а також з використанням персональних пристроїв.

Проблеми безпеки і конфіденційності, які вникають внаслідок застосування хмарних технологій, залежать від їх базових моделей розгортання [26[. Проаналізувавши таксономію зазначених моделей [27], можна прийти до висновку, про у міру підвищення функціоналу хмари зростає відповідальність провайдера за забезпечення її безпеки.

Постачальники хмарних сервісів згідно моделі "програмне забезпечення як сервіс" (SaaS) пропонують свої засоби з великою кількістю інтегрованих функцій. Як наслідок саме розробники відповідають за безпеку та конфіденційність даних. Особливо актуальною є проблема для загальнодоступних хмарних платформ, які, зазвичай використовують загальноосвітні навчальні заклади. Їх розробники, які є потужними наднаціональними корпораціями (Google, Microsoft), чимало уваги приділяють питанням інформаційної безпеки. Проте не достатньо компетентне адміністрування хмарних платформ може призвести до одержання доступу до персональних даних учнів, поширення небажаного контенту, кіднепінгу тощо.

Хмарні технології згідно моделі "платформа як сервіс" (PaaS), зазвичай, використовуються при створенні власних програмних продуктів. Як наслідок першочергово за захист власних програм відповідають клієнти. Постачальники послуг мають ізолювати один від одного додатки клієнтів та їх середовища розробки.

Використання найбільш розширюваної моделі "інфраструктура як сервіс" (IaaS) надає чимало функціональних можливостей й створює чимало кіберзагроз. Захист хмарної інфраструктури покладається на її користувачів, але й постачальники послуг також мають забезпечити базові можливості низького рівня захисту власних платформ.

Як показує досвід, використання хмарних технологій згідно двох останніх

моделей (PaaS та IaaS), зазвичай здійснюється у вищих навчальних закладах. Корпоративні хмари ВНЗ створюються з метою забезпечення більшої розширюваності й інтеграції їх власних обчислювальних потужностей і забезпечення до них індивідуального повсюдного доступу студентів. При цьому,зазвичай, використовується технологія віртуалізації, яка також збільшує ризики вторгнення. Отож, системні адміністратори хмарних платформ та інфраструктур мають працювати над забезпеченням ізоляції, опосередкованого і безпечного обміну даними між віртуальними машинами. Це може бути зроблено за допомогою гнучкого механізму контролю доступу, який керує можливостями контролю і спільного використання VM у хості хмари.

Важливою безпековою проблемою є створення єдиного інформаційно-освітнього середовища ВНЗ [27, 28] . Інтеграція у ньому хмарних і традиційних сервісів забезпечує легкий та уніфікований доступ викладачів і студентів до їх особистих даних, зокрема й через мережу Інтернет. Зазвичай, для автентифікації користувачів середовища використовують традиційний засіб – введення логіна й пароля. У інформаційно-освітньому середовищі навчальних закладів використовують єдину автентифікацію – доступ до різних (усіх) сервісів здійснюється за допомогою одного й того ж логіна й пароля [29]. Такими сервісами можуть бути сайти, система електронного навчання, електронна пошта, віртуальна приватна мережа, бездротові мережі Wi-Fi тощо. Фахівці з безпеки, викладачі інформатики, а також студенти мають розуміти, що такий підхід несе суттєві загрози, особливо у випадку використання відкритих (тих, які не шифруються) протоколів передавання даних. Наприклад, у випадку використання LDAP-каталогів, передавання даних у мережі має здійснюватися за криптованими протоколами з використанням ключів шифрування (LDAPS, HTTPS, SMTPS, IMAPS).

Нині в освіті набуває поширення концепція використання персональних пристроїв у навчальному процесі (BYOD) [30]. Університети можуть надавати віддалений доступ викладачам і студентам до власної корпоративної мережі за допомогою технологій віртуальних приватних мереж (VPN). Зазвичай саме особисті пристрої використовують студенти як VPN-клієнти, з метою одержання віддаленого доступу до інформаційних ресурсів університету. Отож, ще однією загрозою кібербезпеці освітнього середовища є той факт, що студенти ,й учні отримують доступ з пристроїв, якими не управляють ІТ-фахівці навчальних закладів.

Підходом для забезпечення єдиної автентифікації є використання інтеграції баз облікових записів користувачів на основі протоколів авторизації (наприклад, OAUTH). Він не вимагає повторення процедури автентифікації користувача, натомість при доступі до ресурсів здійснює його авторизацію за допомогою механізму токенів. Удосконалення безпеки навчального закладу можливе за умови використання двофакторної авторизації. Провідні провайдери хмарних платформ можуть надати обидві з вищезгаданих технологій. Єдина система автентифікації потребує належного обліку дій користувачів при доступі до кожного із сервісів. Користувачі також повинні розуміти небезпеку втрати своїх паролів, адже у такому випадку зловмисник отримає доступ до усіх ресурсів і даних користувача.

Для вивчення взаємозв’язку знань, умінь у галузі інформаційної безпеки з повсякденною поведінкою студентів – майбутніх учителів інформатики нами було проведено дослідження. Основним завданням було визначення взаємозв’язку знань, умінь студена у галузі кібербезпеки з його поведінкою тобто кореляції когнітивно-операційного й особистісно-рефлексивного складників фахових компетентностей. Для дослідження нами було обрано метод анкетування, яке проводилося упродовж таких етапів:

1. Формулювання гіпотези, визначення латентних показників.
2. Формулювання тверджень, які дають змогу виміряти значення латентних показників, створення анкети.
3. Проведення пілотного дослідження й уточнення питань анкети.
4. Проведення основного дослідження.
5. Статистична обробка результатів і підведення підсумків.

Робочою гіпотезою було твердження про те, що достатній рівень знань та вмінь майбутніх учителів інформатики у галузі кібербезпеки є необхідною, але не достатньою умовою для забезпечення інформаційної безпеки їх діяльності.

На пілотному етапі дослідження з анкетою працювали 24 експерти – практикуючі вчителі інформатики. На підставі отриманих від них даних, ми визначили судження, які дійсно пов'язані з досліджуваним латентним показником. Решта суджень ми вилучили з анкети.

Респондентами основного дослідження були студенти, 32 студенти 2-4 курсів спеціальності "014.09. Середня освіта. Інформатика". Пропонована студентам анкета містила 3 блоки питань: інформаційний, блок вивчення когнітивно-операційного та особистісно-рефлексивного складників. З метою одержання об’єктивних показників анкета була анонімною. Завданням інформаційного блоку було визначення віку, статі, місця використання сервісів мережі Інтернет респондентів. Також у цьому блоці ми запитали, скільки часу протягом доби та якими саме сервісами користуються студенти. Аналіз відповідей показує (рис. 1), що студенти щоденно проводять за комп’ютером не менше 3-5 годин.

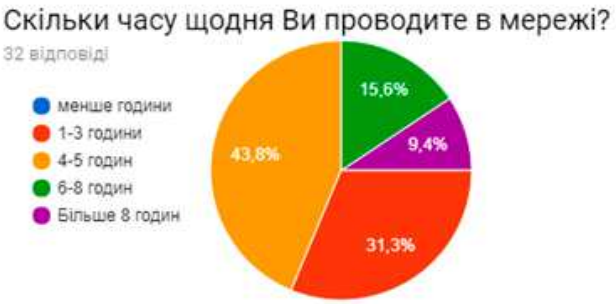

Рис. 1. Розподіл респондентів за часом роботи в мережі

Стосовно доступу до мережі, то можна стверджувати, що він є повсюдним, оскільки практично всі опитані мають доступ до Інтернету у навчальному закладі й удома. Також виявлено значний відсоток студентів (71,9%), які використовують мобільні пристрої для роботи в Інтернеті (рис. 2).

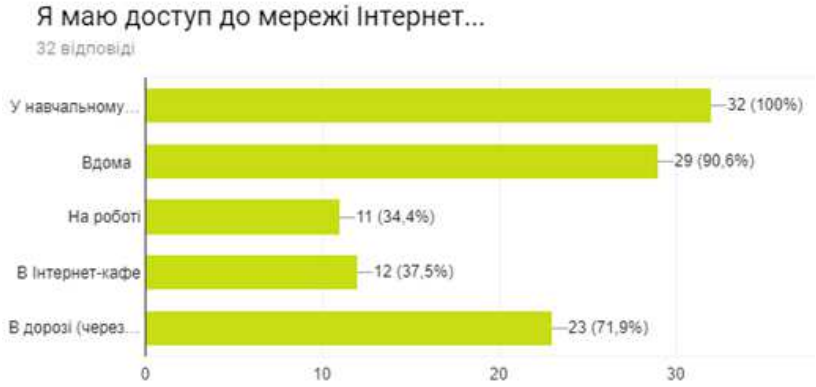

Рис. 2. Характеристика доступності респондентам мережі Інтернет

Питання наступних двох блоків були створені за методикою Лайкерта. Шкала Лайкерта дає змогу визначати ставлення респондентів до певних тверджень чи положень за варіантами відповіді, що знаходяться у певному діапазоні. Як правило, таким діапазоном обирають 5-бальну шкалу із значеннями:

- 1 бал – повністю не згодний;
- 2 бали – не згодний;
- 3 бали – нейтральне ставлення;
- 4 бали – згодний;
- 5 балів – повністю згодний.

У шкалі Лайкерта можуть бути використані й інші назви значень. Наприклад ми використовувати такі: "1 – ніколи не використовую; 5 – завжди не використовую;", "1 – взагалі не важливо; 5 – дуже важливо".

Питання анкети, при побудові якої використовується шкала Лайкента, спрямовані на вимірювання латентної змінної, у вигляді так званого "кафетерію" – таблиці, рядки якої відповідають досліджуваним ознакам, а стопці містять їх відповідні числові значення [31]. У контексті нашого дослідження такою латентною змінною є складники знань, умінь, ставлень та поведінки майбутніх учителів інформатики, які стосуються інформаційної безпеки. Оцінку респондентом кожного з тверджень анкети можна розглядати як деяку функцію від загального латентного фактора (когнітивно-операційного та особистісно-рефлексивного складників). Тобто, чим більш позитивною є оцінка респондентом певного твердження, тим більш значним є рівень розвитку відповідних його компетентностей.

Використання шкали Лайкерта у дослідженні може мати недоліки: уникнення в оцінюванні респондентами максимальних або мінімальних оцінок (тенденція до усереднення), введення не достатньо відвертих оцінок, вимоги рівномірності інтервальної шкали. З метою забезпечення об’єктивності оцінювання респондентами питань анкети у процесі розроблення анкети ми дотримувалися таких вимог:

- переважного вживання змістовних позначень інтервальної шкали замість числових (1 бал – 5 балів);
- використання однополярних (від "повнісню не згоден" до "повнісню згоден") шкал оцінювання у всіх питаннях;
- уникання формулювання питань у заперечній формі (за можливості);
- дублювання англомовних термінів та понять українською мовою;
- лаконічне формулювання питань у вигляді простих речень.
- Питання другого блоку анкети стосувалися оцінювання студентами:
- власного рівня розуміння основних понять кібербезпеки (брандмауер, антивірус, сеанс роботи, проксі-сервер, віртуальна приватна мережа, підміна IP-адреси, історія переглядів, приватне вікно браузера, Cookie, TOP-маршрутизація, спам, Adware, пошуку у тимчасових файлах (Dumpster Diving));
- частоти та систематичності використання засобів кібербезпеки, які стосуються вищезазначених понять.

З метою перевірки показника узгодженості запитань після дослідження ми обчислили коефіцієнт альфа Кронбаха. Для другого блоку анкети, який містив 30 запитань, величина альфа Кронбаха склала α_{Kr}=0,914, що перевищує мінімально прийнятне значення (0,7).

Завданням другого блоку анкети було визначення коефіцієнта кореляції між рівнем ІК-компетентності студентів та рівнем розуміння понять і використання відповідних засобів. Студентам було запропоновано оцінити власний рівень ІК-

компетентності. Для перевірки об'єктивності такого самооцінювання ми досліджували кореляцію між одержаними величинами самооцінки та середнім балом, отриманим респондентом на іспитах із фахових дисциплін. Оскільки розподіл балів за критерієм Колмогорова-Смірнова виявився нормальним, то нами був обчислений коефіцієнт кореляції Пірсона r_{ki}. Для рівня значущості α=0,01 він виявився досить значним – $r_{ki=}$0,827, що свідчить про достатньо об'єктивне самооцінювання.

Для кожного респондента латентними показниками рівня розуміння та використання засобів кібербезпеки ми вважали, середнє значення балів, отриманих ним при оцінюванні усіх 30 питань та нормований індекс I_n, який знаходили із співвідношення:

, (1),

де s_i – сума балів і-го респондента, s_{max} – максимально можлива сума балів, N – кількість запитань. Для досліджуваної групи респондентів середнє значення нормованого індексакогнітивно-операційного складника виявилося рівним I_{n1}=0,68, що свідчить наявність латентного показника.

Перевіривши на нормальність розподілів вибірок середнього значення та одержаного внаслідок самооцінювання рівня ІТ-компетентностей, ми обчислили коефіцієнт кореляції Пірсона r_{ks}. Для рівня значущості α=0,01 він виявився меншим, хоча й прийнятним – $r_{ki=}$0,647, що свідчить про наявність взаємозв'язку між рівнем ІК-компетентності. Порівнюючи рівні знань та володінь засобами забезпечення кібербезпеки, можна зробити висновок про існування кореляціїї між ними (рис. 3).

Рис. 3. Рівень володіння студентами термінологією та використання засобів кібербезпеки

Як видно з діаграми, існує незначне відхилення досліджуваних значень в сторону розуміння термінології та засобів. Це можна пояснити тим, що серед респондентів є частина студентів, які розуміють термінологію та загрози інформаційної безпеки, проте не достатньо використовують відповідні програмні засоби.

Завданням третього блоку анкети було дослідження особистісно-рефлексивного складника через визначення взаємозв'язку компетентності та їх поведінки майбутніх учителів інформатики. Питання третього блоку передбачали оцінювання студентами тверджень, які стосуються інформаційної безпеки:

- використання паролів (їх складності та повторюваності);
- перегляду сайтів та передавання до них особистих даних;
- завантаження програмних засобів з Інтернету;
- публікування даних у соціальних мережах;
- резервного копіювання важливих даних.

Обчисливши коефіцієнт кореляції Пірсона, було з'ясовано, що для рівня значущості α=0,01 він виявився достатнім – $r_{kp=}$0,556, що свідчить про існування взаємозв'язку між досліджуваними складниками компетентностей. Середнє значення нормованого індекса особистісно-рефлексивного складника ІК-компетентностей дорівнює I_{n2}=0,51

Порівнюючи значення нормованих індексів I_{n1} та I_{n2} та врахувавши одержані коефіцієнти кореляції r_{ki} та r_{kp}, можна зробити висновок про існування множини респондентів, які мають необхідні знання у галузі кібербезпеки, проте не дотримуються відповідних рекомендацій у повсякденній діяльності.

5. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Однією з актуальних проблем управління комп'ютерними системами є реалізація заходів щодо їх захисту. Розвиток засобів ІКТ та їх упровадження у навчальний процес, з одного боку, надає додаткові можливості для підвищення рівня кібербезпеки, а з іншого, створює додаткові загрози захищеності інформаційно-освітнього середовища навчального закладу. Важливим аспектом здійснення навчально-виховного процесу є дотримання його учасниками правил інформаційної безпеки, яка нерозривно пов'язана з інформаційною культурою особистості.

Як показує досвід, провідним фахівцем у галузі інформаційної безпеки у загальноосвітній школі є вчитель інформатики. Формування у майбутніх учителів фахових компетентностей у галузі інформаційної безпеки є актуальною проблемою теорії і методики навчання інформатики. Проведене експериментальне дослідження свідчить, про наявність взаємозв'язку між знаннями студентів у галузі інформаційної безпеки та їх уміннями використовувати відповідні програмні засоби. Статистична обробка експериментальних даних показала, що достатній рівень розвитку когнітивно-операційного складника ІК-компетеності студента не має обов'язковим наслідком дотримання ним правил безпечної діяльності в комп'ютерних мережах. Отож, підготовка майбутніх учителів інформатики має передбачати розвитку когнітивно-операційного й особистісно-рефлексивного складників їх компетентостей.

Перспективи подальших досліджень вбачаємо у розробці методики навчання основ інформаційної безпеки майбутніх учителів інформатики. На нашу думку, вона має здійснюватися неперервно впродовж усього терміну підготовки, як опосередковано (під час навчання базових дисциплін), так і безпосередньо – у межах окремо виділеного спецкурсу за вибором.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Ю. С. Рамський, "Професійна діяльність вчителя в епоху інформатизації освіти" [Електронний ресурс]. Доступно: http://enpuir.npu.edu.ua/handle/123456789/9387.

[2] Д. Лайон, "Інформаційне суспільство: проблеми та ілюзії", Сучасна зарубіжна соціальна філософія, 1996. [З мережі]. Доступно: http://www.philsci.univ.kiev.ua/biblio/lajon.html.

[3] В. Ю. Биков, "Навчальне середовище сучасних педагогічних систем. Професійна освіта: педагогіка і психологія", Вища Педагогічна Школа у Честохові, Ченстохов, с. 59–80, 2004.

[4] О. М. Спірін, та В. Н. Ковальчук, "Методика забезпечення он-лайн безпеки старшокласників у

навчально-виховному процесі школи", Інформаційні технології і засоби навчання, №1(21), 2011 [Електронний ресурс]. Доступно: https://journal.iitta.gov.ua/index.php/itlt/article/view/411/368.

[5] В. Биков та ін., *Оцінювання інформаційно-комунікаційної компетентності учнів та педагогів в умовах євроінтеграційних процесів в освіті,* К, Україна: Педагогічна думка, 2017.

[6] Н. П. Дементієвська, "Критичне оцінювання інтернет-ресурсів при вивченні природничих наук" [Електронний ресурс]. Доступно: http://lib.iitta.gov.ua/4586/1/Кіровоград_2014_Дементієвська_тези1.pdf.

[7] Н. В. Морзе, В. П. Вембер, О. В. Барна, та О. Г. Кузьмінська, "Інформатика-6: навчання через діяльність", Інформатика та інформаційні технології в навчальних закладах, №4 (52), 2014. [Електронний ресурс]. Доступно: http://elibrary.kubg.edu.ua/6323/.

[8] В. Ю. Биков, М. П. Шишкіна, "Хмарні технології як імператив модернізації освітньо-наукового середовища вищого навчального закладу", Теорія і практика управління соціальними системами. № 4, 2016, [Електронний ресурс]. Доступно: http://nbuv.gov.ua/UJRN/Tipuss_2016_4_8.

[9] "Online Browsing Platform (OBP)", Iso.org, 2017. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en.

[10] "Концепція інформаційної безпеки України", Osce.org, 2017. [Електронний ресурс]. Доступно: http://www.osce.org/uk/fom/175056?download=true.

[11] Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України" (2017, Лют. 25). [Електронний ресурс]. Доступно: http://zakon2.rada.gov.ua/laws/show/47/2017#n12.

[12] В. Ковальчук, "Забезпечення інформаційної безпеки старшокласників у комп'ютерно орієнтованому навчальному середовищі", дис. канд. пед. наук., Інститут інформаційних технологій і засобів навчання НАПН України, Київ, 2013.

[13] Directive (EU) 2016/680 Of The European Parliament And Of The Council.(2016, April 27)"on the protection of natural persons with regard to the processing of personal data by competent authorities. Council Framework Decision 2008/977/JHA", Eur-lex.europa.eu, [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN.

[14] D. Van Rooyand J. Bus, "Trust and privacy in the future Internet—a research perspective", Identity in the Information Society, vol. 3, no. 2, pp. 397-404, 2010.[Online]. Available: https://doi.org/10.1007/s12394-010-0058-7.

[15] M. Whitmanand H. Mattord, Principles of information security. Boston, MA: Course Technology, 2012.

[16] J. L. Spears "Defining information security". In:5th security conference, LasVegas, Nevada, The Information Institute, Washington Dc, Usa. 2006.[Online]. Available:http://www.isy.vcu.edu/~gdhillon/Old2/secconf/pdfs/11.pdf.

[17] "Subject Benchmark", Qaa.ac.uk, 2016. [Online]. Available: http://www.qaa.ac.uk/en/Publications/Documents/SBS-Computing-16.pdf. [Accessed: 11- Oct- 2017].

[18] "Alabama Cyber Security Programs", Cyber Degrees, 2017. [Online]. Available: http://www.cyberdegrees.org/listings/alabama/.

[19] "CIAS Home", Cias.utsa.edu, 2017. [Online]. Available: http://jic.nv.gov/uploadedFiles/jicnvgov/content/Events/P%20ICM%20NV.pdf.

[20] "Стандарт вищої освіти підготовки бакалаврів спеціальності 125 Кібербезпека" [Електронний ресурс]. Доступно: http://mon.gov.ua/content/Новини/2016/07/07/01/125-kiberbezpeka.doc

[21] ENISA, "The newusers' guide: How to raise information security awareness (EN) – ENISA", Enisa.europa.eu, 2010. [Online]. Available: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide.

[22] И. А. Зимняя "Компетенция и компетентность в контексте компетентностного подхода в образовании" [Електронний ресурс]. Доступно: http://www.rusreadorg.ru/ckeditor_assets/attachments/63/i_a_zymnaya_competency_and_competence.pdf

[23] Ю. С. Рамський, "Методична система формування інформаційної культури майбутніх вчителів математики", дис. д-ра. пед. наук., НПУ імені М. П. Драгоманова, Київ, 2013.

[24] В. Биков, "Технології хмарних обчислень, ІКТ-аутсорсінг та нові функції ІКТ-підрозділів навчальних закладів і наукових установ", *Інформаційні технології в освіті,* Вип. 10, с. 8-23, 2011.

[25] H. Takabi, J. Joshi, G-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security and Privacy Magazinepp. 24-31, 8, 2011. [Online]. Available: https://www.researchgate.net/publication/224202015_Security_and_Privacy_Challenges_in_Cloud_Computing_Environments.

[26] Технология облачных вычислений. [Електронний ресурс]. Доступно: http://sd-company.su/article/cloud/technology

[27] O. G. Glazunova, T. V. Voloshyna, "Hybrid Cloud-Oriented Educational Environment for Training

Future IT Specialists". Proc. 12-th Int. Conf. ICTERI 2016, 2016. [Online]. Available: http://ceur-ws.org/Vol-1614/paper_64.pdf (2016)[Accessed: 11- Oct- 2017]
[28] M. P. Shyshkina,The Hybrid Cloud-based Service Model of Learning Resources Access andits Evaluation. Proc. 12-th Int. conf. ICTERI 2016, 2016. [Online]. Available: http://ceur-ws.org/Vol-1614/paper_57.pdf
[29] В. П. Олексюк "Проектування моделі хмарної інфраструктури ВНЗ на основі платформи ApacheCloudstack", *Інформаційні технології і засоби навчан*ня, Вип. 4 (54), с. 153-164, 2016.
[30] M. Sundgren, "Blurring time and place in higher education with bring your own device applications: a literature review", Education and Information Technologies, pp. 1-39, 2017. [Online]. Available: https://doi.org/10.1007/s10639-017-9576-3.
[31] P. Y. Chen, P. M. Popovich,Correlation. Parametric and nonparametric measures. Papers Series on Quantitative Applications in the Social Sciences, CA: Sage, 2002.

Матеріал надійшов до редакції 15.10.2017 р.

СОСТОЯНИЕ СФОРМИРОВАННОСТИ КОМПЕТЕНТНОСТЕЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БУДУЩИХ УЧИТЕЛЕЙ ИНФОРМАТИКИ

Олексюк Василий Петрович
кандидат педагогических наук, доцент, доцент кафедры информатики и методики ее преподавания
Тернопольский национальный педагогический университет имени Владимира Гнатюка, Тернополь, Украина
ORCID ID 0000-0002-3121-7005
oleksyuk@fizmat.tnpu.edu.ua

Олексюк Олеся Романовна
кандидат педагогических наук, преподаватель кафедры содержания и методов учебных предметов
Тернопольский областной коммунальный институт последипломного педагогического образования, Тернополь, Украина
ORCID ID 0000-0002-1454-0046
o.oleksyuk@ippo.edu.te.ua

Аннотация. В статье исследованы понятия кибернетической и информационной безопасности. На основе анализа научно-методической литературы доказано, что кибербезопасность, как состояние защищенности компьютерных систем не может быть обеспечена в полной мере, без информирования и разъяснения пользователям принципов и правил информационной безопасности. Авторами проанализирована специфика обучения будущих учителей информатики в контексте развития у них компетентностей, необходимых для безопасной деятельностив компьютерных сетях и Интернете. Исследованы виды угроз, которые возникают в результате внедрения в учебный процесс различных сервисных моделей облачных технологий. Описана методика и этапы педагогического исследования корреляции когнитивно-операционного и личностно-рефлексивного компонентов профессиональных компетенций будущих учителей информатики.

Ключевые слова: кибербезопасность; информационная безопасность; будущий учитель информатики; компетентность; облачные технологии; педагогический эксперимент.

THE STATUS OF INFORMATION SECURITY COMPETENCE FORMEDNESS OF FUTURE COMPUTER SCIENCE TEACHERS

Vasyl P. Oleksiuk
PhD (pedagogical sciences), Associate Professor of the Department of Informatics and methods of its teaching
Ternopil V. Hnatiuk National Pedagogical University, Ternopil, Ukraine
ORCID ID0000-0002-3121-7005
oleksyuk@fizmat.tnpu.edu.ua

Olesia R. Oleksiuk
PhD (pedagogical sciences), Teacher of the department of contents and methods of subjects
Ternopil regional municipal institute of postgraduate education, Ternopil, Ukraine
ORCID ID0000-0002-1454-0046
o.oleksyuk@ippo.edu.te.ua

Abstract. In **t**he article there are explored the concepts of cybersecurity and information security. It is proved that cybersecurity can't be fully ensured without teaching to principles and rules of information security. The authors have analyzed the specificity of the future computer science teachers' study in the context of developing of their competences necessary for safe students' activity in the computer networks and Internet. Particular attention is paid to the threats arising after introduction cloud technologies various service models into the educational process. The article focuses on methods and stages of the pedagogical investigation of correlation between the operational and reflective components of the professional competencies of future computer science teachers.

Keywords: cybersecurity; information security; future teacher of computer science; competence; cloud technologies; pedagogical experiment.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] Iu.S. Ramskyi, "Professional activity of the teacher in the era of informatization of education".[Online]. Available: http://enpuir.npu.edu.ua/handle/123456789/9387. (in Ukrainian)
[2] D. Laion, "Information Society: Problems and Illusions", Modern Foreign Social Philosophy, 1996. [Online]. Available: http://www.philsci.univ.kiev.ua/biblio/lajon.html. (in Ukrainian)
[3] V.Yu. Bykov, "Educational environment of modern pedagogical systems: vocational education: pedagogy and psychology", Higher Pedagogical School in Czestochov, Czestochov, pp. 59–80, 2004. (in Ukrainian)
[4] O.M. Spirin, and V.N. Kovalchuk, "Methodic of the on-line safety of the senior pupils in the teaching and educational process at school", Information technologies and learning tools, №1(21), 2011.[Online]. Available:https://journal.iitta.gov.ua/index.php/ itlt/article/view/411/368. (in Ukrainian)
[5] V.Yu. Bykov and others, Evaluation of information and communication competence of pupils and teachers in the conditions of European integration processes in education. K, Ukraine: Pedahohichnadumka, 2017. (in Ukrainian)
[6] N.P. Dementiievska, "Critical evaluation of Internet resources in the study of natural sciences" [Online]. Available: http://lib.iitta.gov.ua/4586/1/ Кіровоград_2014_Дементієвська_тези1.pdf. (in Ukrainian)
[7] N.V. Morze, V.P.Vember, O.V.Barna, ta O.H. Kuzminska, " Informatics-6: learning through activity", Informatics and information technologies in educational institutions, №4 (52), 2014. [Online]. Available: http://elibrary.kubg.edu.ua/6323/. (in Ukrainian)
[8] V.Yu. Bykov, M.P.Shyshkina, "The cloud computing as imperative of the university education and research environment modernization".The theory and practice of social systems management. № 4, 2016, [Online]. Available: http://nbuv.gov.ua/UJRN/Tipuss_2016_4_8 (in Ukrainian)
[9] "Online Browsing Platform (OBP)", Iso.org, 2017. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en. (in English)
[10] "The Concept of Information Security of Ukraine ", Osce.org, 2017. [Online]. Available: http://www.osce.org/uk/fom/175056?download=true. (in Ukrainian)
[11] Decree of the President of Ukraine "On the Information Security Doctrine of Ukraine" (2017, Feb. 25). [Online]. Available: http://zakon2.rada.gov.ua/laws/show/47/2017#n12. (in Ukrainian)
[12] V.N. Kovalchuk, "Providing information security in a computer-oriented educational environment", PhD thesis, Institute of Information Technologies and Learning Tools of NAES of Ukraine, Kyiv, 2013. (in Ukrainian)
[13] Directive (EU) 2016/680 Of The European Parliament And Of The Council.(2016, April 27)"on the protection of natural persons with regard to the processing of personal data by competent authorities. Council Framework Decision 2008/977/JHA", Eur-lex.europa.eu, [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN. (in English)
[14] D. van Rooy and J. Bus, "Trust and privacy in the future Internet—a research perspective", Identity in the Information Society, vol. 3, no. 2, pp. 397-404, 2010.[Online]. Available: https://doi.org/10.1007/s12394-010-0058-7. (in English)
[15] M. Whitman and H. Mattord, Principles of information security. Boston, MA: Course Technology, 2012. (in English)

[16] J.L. Spears "Defining information security". In:5th security conference, Las Vegas, Nevada, The Information Institute, Washington Dc, Usa. 2006.[Online]. Available:http://www.isy.vcu.edu/~gdhillon/Old2/secconf/pdfs/11.pdf. (in English)
[17] "Subject Benchmark", Qaa.ac.uk, 2016. [Online]. Available: http://www.qaa.ac.uk/en/Publications/Documents/SBS-Computing-16.pdf. (in English)
[18] "Alabama Cyber Security Programs", Cyber Degrees, 2017. [Online]. Available: http://www.cyberdegrees.org/listings/alabama/.(in English)
[19] "CIAS Home", Cias.utsa.edu, 2017. [Online]. Available: http://jic.nv.gov/uploadedFiles/jicnvgov/content/Events/P%20ICM%20NV.pdf. (in English)
[20] "Standards for higher education of bachelors of specialty 125 Cybersecurity." [Online]. Available: http://mon.gov.ua/content/Новини/2016/07/07/01/125-kiberbezpeka.doc. (in Ukrainian)
[21] ENISA, "The new users' guide: How to raise information security awareness (EN) – ENISA", Enisa.europa.eu, 2010. [Online]. Available: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide. [Accessed: 11- Oct- 2017]. (in English)
[22] I.A. Zimnjaja" Competence and competence in the context of a competence approach in education" [Online]. Available:http://www.rusreadorg.ru/ckeditor_assets/ attachments/63/i_a_zymnaya_competency_and_competence.pdf (in Russian)
[23] Iu.S. Ramskyi, "The methodical system of information culture forming of future teachers of Mathematics ", the dissertation of the doctor of sciences.,NPU named after M.P. Drahomanov, Kyiv, 2013.(in Ukrainian)
[24] V.Yu. Bykov, " ICT-outsourcing and new functions of ICT departments of educational and scientific institutions", Information Technologies in education, 10, pp. 8-23, 2011.(in Ukrainian)
[25] H. Takabi, J. Joshi, G-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security and Privacy Magazine pp. 24-31, 8, 2011. [Online]. Available: https://www.researchgate.net/publication/224202015_Security_and_Privacy_ Challenges_in_Cloud_Computing_Environments. (in English)
[26] Cloud computing technology. [Online]. Available:http://sd-company.su/article/cloud/technology (2017) (in English)
[27] O. G. Glazunova, T. V. Voloshyna, "Hybrid Cloud-Oriented Educational Environment for Training Future IT Specialists". Proc. 12-th Int. Conf. ICTERI 2016, 2016. [Online]. Available: http://ceur-ws.org/Vol-1614/paper_64.pdf (2016)
[28] M. P. Shyshkina, The Hybrid Cloud-based Service Model of Learning Resources Access and its Evaluation. Proc. 12-th Int. conf. ICTERI 2016, 2016. [Online]. Available: http://ceur-ws.org/Vol-1614/paper_57.pdf (in English)
[29] V.P Oleksiuk "Designing of university cloud infrastructure based on Apache Cloudstack", Information technologies and learning tools,4 (54), pp. 153-164, 2016.(in Ukrainian)
[30] M. Sundgren, "Blurring time and place in higher education with bring your own device applications: a literature review", Education and Information Technologies, pp. 1-39, 2017.[Online]. Available: https://doi.org/10.1007/s10639-017-9576-3. (in English)
[31] P. Y. Chen, P. M. Popovich, Correlation. Parametric and nonparametric measures. Papers Series on Quantitative Applications in the Social Sciences, CA: Sage, 2002. (in English)