

УДК 378.147:004.056

**Чичкань Іван Васильович**

кандидат фізико-математичних наук, доцент, доцент кафедри інформаційних систем та технологій Київський національний університет імені Тараса Шевченка, м. Київ, Україна  
ORCID ID 0000-0002-0854-389X  
*Chychkan@FIT.knu.ua*

**Спасітелєва Світлана Олексіївна**

кандидат фізико-математичних наук, доцент, доцентка кафедри інформаційної та кібернетичної безпеки Київський університет імені Бориса Грінченка, м. Київ, Україна  
ORCID ID 0000-0003-4993-6355  
*s.spasitieliieva@kubg.edu.ua*

**Жданова Юлія Дмитрівна**

кандидат фізико-математичних наук, доцент, доцентка кафедри інформаційної та кібернетичної безпеки Київський університет імені Бориса Грінченка, м. Київ, Україна  
ORCID ID 0000-0002-9277-4972  
*y.zhdanova@kubg.edu.ua*

## ОСВІТНЄ СЕРЕДОВИЩЕ ДЛЯ ФОРМУВАННЯ КУЛЬТУРИ БЕЗПЕКОВОГО ПОВОДЖЕННЯ У КІБЕРПРОСТОРІ ПРИ ПІДГОТОВЦІ ФАХІВЦІВ З ЕКОНОМІКИ ТА УПРАВЛІННЯ

**Анотація.** Стаття присвячена проблемі підготовки сучасних фахівців галузей знань 05 «Соціальні та поведінкові науки» та 07 «Управління і адміністрування» до безпекового поведіння у кіберпросторі. Запропоновано методику створення мережевого навчального середовища з можливостями поетапної віртуалізації, переходу до хмарних технологій та дистанційної форми навчання. Розглянуто питання формування у студентів спеціалізовано-професійних знань та умінь з інформаційної та кібернетичної безпеки. Зважаючи на результати досліджень у психолого-педагогічній літературі та власний 10-річний досвід, визначено обсяг теоретичних та практичних знань для формування навичок та умінь із захисту інформації в кібернетичному просторі. Сформульовано перелік вимог до рівня сформованості професійно значущих характеристик спеціаліста з економіки та управління у сфері захисту інформації. Обґрунтовано актуальність та доцільність формування сучасного мережевого навчального середовища з широким використанням відкритих освітніх ресурсів, мобільних додатків, хмарних технологій для підвищення рівня компетентності студентів з інформаційної та кібернетичної безпеки. Проведено порівняльний аналіз ресурсів відкритого інформаційно-освітнього простору, які можуть використовуватись як обов'язкові елементи навчальної дисципліни та залучатись для самостійної роботи студентів. Визначені критерії вибору відкритих навчальних ресурсів та запропонована методологія їх використання. Розглянуто форми організації навчального процесу, сучасні методи, інструменти та засоби навчання для мережевого навчального середовища закладу вищої освіти. Наведено шляхи реалізації запропонованої методики покрокового створення навчального середовища у Київському національному університеті імені Тараса Шевченка в межах навчальних дисциплін «Інформаційна безпека», «Захист інформації», «Кібербезпека» та в Київському університеті імені Бориса Грінченка. Обґрунтовано, що використання інноваційних технологій навчання, відкритих навчальних ресурсів провідних навчальних закладів, хмарних та мобільних сервісів, пов'язаних із захистом даних, дозволяє підготувати фахівців з практичними навичками із захисту інформації, які є затребуваними на ринку праці.

**Ключові слова:** інформаційна безпека; кібернетична безпека; хмаро орієнтоване навчальне середовище; відкритий інформаційно-освітній простір.

## 1. ВСТУП

Ознакою сучасного інформаційного суспільства є зростаючий вплив інформаційно-комунікаційних технологій (ІКТ) на всі сфери людської діяльності. Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки [1] передбачає здійснення заходів щодо впровадження відповідних стимулів для цифровізації економіки, інструментів розвитку цифрової інфраструктури, набуття громадянами цифрових компетенцій, використання та споживання цифрових технологій. Відповідно до концепції цифрової економіки сучасні фахівці повинні володіти цифровою компетентністю, яка є складовою професійної компетентності спеціаліста будь-якого профілю. Цифрова трансформація стає основою життєдіяльності суспільства, бізнесу, державного управління. В умовах цифрової економіки людський капітал та інформаційні технології відіграють вирішальну роль у забезпеченні сталого розвитку економіки. У зв'язку з цим підготовка висококваліфікованих фахівців з урахуванням потреб ринку та сучасних тенденцій розвитку цифрових технологій, набуває особливого значення. Щоб максимально використати потенціал цифрових технологій, потрібні нові фахівці, які володіють сучасними знаннями, цифровими навиками, здатні до самонавчання, вирішення складних завдань у постійно змінюваному середовищі [2]. У затверджених стандартах вищої освіти України з підготовки фахівців галузі знань 07 «Управління та адміністрування» (спеціалісти з обліку та оподаткування; фінансів, банківської справи та страхування; менеджменту; маркетингу; підприємництва, торгівлі та біржової діяльності) та галузі знань 05 «Соціальні та поведінкові науки» спеціальності «Економіка» визначені такі компетентності як здатність до застосовування спеціалізованих інформаційних систем і комп'ютерних технологій у відповідних сферах діяльності, уміння використовувати сучасні ІКТ для пошуку, обробки та аналізу ділової інформації.

Новітні інформаційні технології продукують не лише нові можливості, а й породжують нові і незнайомі ризики кіберзагроз, які можуть перешкодити компаніям та державним установам реалізувати свій цифровий потенціал. Однією із складових цифрової компетентності визначена інформаційна безпека: захист пристроїв, персональних даних і конфіденційність. Цифровізація повинна супроводжуватись підвищенням рівня довіри і безпеки. Інформаційна безпека, кібербезпека, захист персональних даних, недоторканність особистого життя та прав користувачів цифрових технологій, зміцнення довіри та захист у кіберпросторі є, зокрема, передумовами одночасного цифрового розвитку та відповідного попередження, усунення та управління супутніми ризиками [1]. Формування, розвиток та впровадження національної культури кібербезпеки є необхідною складовою на шляху боротьби з кіберзлочинністю. Підготовка спеціалістів з економіки та управління має відображати майбутні напрями розвитку робочого середовища та ІКТ для використання можливостей цифрових технологій в єдиному інформаційному просторі – кіберпросторі.

**Постановка проблеми.** На шляху реалізації стратегії цифрової економіки є важливим формування в майбутніх фахівців мотивацій та потреб використання «цифрових технологій» та формування професійних навичок роботи в сучасному високорозвиненому інформаційно-комунікаційному середовищі. В інноваційному розвитку вищої освіти відбувається постійне вдосконалення навчального середовища (НС) завдяки впровадженню сучасних ІКТ та нових методик навчання. НС підготовки фахівців з економіки та управління в закладах вищої освіти (ЗВО) повинно відповідати вимогам інформаційного суспільства та цифрового комунікативного середовища.

Управлінська та економічна діяльність відповідно до стандартів вищої освіти вимагає наявності професійних знань з менеджменту, банківської справи, підприємництва, торгівлі тощо, а також вимагає теоретичних та практичних знань з використання інтерактивного інформаційного середовища. Спеціалісти з економіки та управління мають бути здатними не тільки сприймати і оновлювати інформацію, а й обробляти її, зберігати та створювати нову в глобальному мережевому середовищі. Водночас важливою є підготовка спеціалістів з економіки та управління до виконання задачі захисту інформації, яка передбачає вміння використовувати комплекс спеціальних засобів захисту: нормативно-правових, фізичних, інженерно-технічних, крипто-графічних [3]. Питання захисту інформації вже давно вийшли на одне з перших місць серед інших завдань, що вирішуються в процесі використання сучасних інформаційно-комунікаційних систем. Останнім часом реальні збитки від несанкціонованого доступу до корпоративної інформації продовжують зростати. На думку спеціалістів, внутрішні витрати корпоративної інформації мають більш негативні наслідки, ніж зовнішні втручання. У 2018 році компанії втратили з вини власних співробітників у 3 рази більше корпоративних даних, ніж у результаті хакерських атак, 64,5% випадкових витоків даних сталися з вини співробітників компанії [4]. Більшість загроз цілісності і конфіденційності інформації, що циркулює в комп'ютерних системах, можна попередити завдяки використанню методів та засобів захисту при відповідній підготовці співробітників. Закон України від 05.11.2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» визначає необхідність «підвищення цифрової грамотності громадян та культури безпекового поведіння в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту...» [5]. Культура безпекового поведіння спрямована на забезпечення кібербезпеки особи як у межах бізнес процесів організації, так і в її повсякденному житті.

Все це підтверджує актуальність визначеної проблеми і спонукає до пошуків підходів до формування у майбутніх фахівців з економіки та управління знань із захисту інформації в кіберпросторі, визначення обсягу цих знань та пошуку сучасних інструментів для набуття таких знань шляхом створення сучасного НС. Таке середовище можна сформувати із застосуванням відкритого інформаційно-освітнього інтернет-простору, мережевого освітнього середовища ЗВО, що забезпечить співпрацю суб'єктів навчання, комунікації, зберігання великих обсягів навчального матеріалу, планування навчальних подій тощо.

**Аналіз останніх досліджень і публікацій.** Проблеми переходу до цифрової економіки активно дискутуються у вітчизняній та зарубіжній літературі, зокрема в наукових роботах Карчевої Г.Т. зазначається необхідність удосконалення економічної освіти в умовах цифрової економіки [6]. Діордіца І.В. у своїх публікаціях підкреслює необхідність введення спеціальної та загальної кіберосвіти, що повинно стати Національною стратегією кіберосвіти [7]. Аналіз публікацій з питань кіберосвіти таких авторів, як Г. Остін (G. Austin), А. Генрі (A. Henry), М. Камінська (M. Kaminska) [8] Дж. Маршалл (G. Marshall), К. Даїмі (K. Daimi), Д. Торнтон (D.Thornton), С. Найт (S. Knight) [9], показав, що єдина система, методологія та зміст навчання з питань загальної кіберосвіти досі не сформовані. При підготовці фахівців (як технічного, так і гуманітарного напрямку) з інформаційної та кібернетичної безпеки необхідно використовувати сучасні освітні технології.

Проблемі формування та розвитку комп'ютерно орієнтованого освітнього середовища в закладах освіти значну увагу приділяли вітчизняні та зарубіжні вчені, зокрема В.Ю. Биков [10], А.М. Гуржій, В.В. Лапінський [11], С.Г. Литвинова [12],

О.Ю. Буров [13], Вілсон С., Шаферт С. та ін. В. Ю. Биков зазначає, що спроектувати НС – це "означає теоретично дослідити суттєві цільові і змістово-технологічні (методичні) аспекти навчально-виховного процесу, який повинен здійснюватися в НС, і на цій основі описати необхідний для цього склад і структуру НС (його статичну і динаміку, в тому числі передбачити і врахувати розвиток будови НС, вплив і особливості взаємозв'язків складових НС з іншими елементами ПС, з елементами оточуючого середовища) відповідно до динаміки розвитку цілей його створення і використання, а також обмежень психолого-педагогічного, науково-технічного і ресурсного характеру" [10]. Аналізуючи етапи формування НС можна зазначити постійне зростання вимог до нього відповідно до змін у розвитку ІКТ. Перехід людства до інформаційної ери супроводжується появою нових особливостей НС, які набувають стрімкого розвитку та можливостей [12]. У роботі С.Г. Литвинової, О.П. Пінчук, О.Ю. Бурава [13] розглядаються особливості розвитку мережевого, віртуального, мобільного, персоніфікованого, хмаро орієнтованого НС. Відзначається зростання ролі відкритого комп'ютерно орієнтованого НС з використанням комп'ютерних засобів навчання й електронних освітніх ресурсів, що належать до складу ІКТ-системи навчального закладу, а також засобів, ресурсів і сервісів відкритих інформаційно-комунікаційних мереж. Зміни у формах, методах і засобах освіти супроводжуються змінами в організації НС – пряме спілкування, опосередковане через цифровий простір, змішане, хмари, соціальні мережі, мобільні технології тощо. Фактично життя людини зміщується все більше у бік синтетичного середовища, а діяльність, спілкування, навчання, дозвілля відбувається все більше у віртуальному просторі зі своїми перевагами, недоліками та небезпеками. Визначається тенденція до перенесення навчально-розвивальної діяльності в синтетичне середовище.

**Мета статті.** Метою дослідження є теоретичне обґрунтування та розробка методики покрокового створення персоніфікованого, мобільного, хмаро орієнтованого навчального середовища для формування культури безпекового поведіння в кіберпросторі при підготовці спеціалістів з економіки та управління.

## 2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Відповідно до мети дослідження поставлено такі завдання:

1. Дослідити проблему використання мережевого середовища та сучасних засобів ІКТ у навчанні майбутніх економістів та управлінців. Визначити мету та завдання використання мережевого НС.
2. Визначити зміст навчання: обсяг теоретичних та практичних знань для формування комплексних знань, навичок та вмінь з інформаційної безпеки та захисту інформації в кіберпросторі при підготовці спеціалістів з економіки та управління.
3. Розробити критерії та показники вибору відкритих навчальних ресурсів з інформаційної безпеки та захисту інформації. До відкритих навчальних ресурсів належать як серверні (хмарні), так і мобільні ресурси.
4. Описати методику використання мережевого НС: визначити форми організації, методи та засоби навчання для формування знань, навичок та вмінь з інформаційної та кібернетичної безпеки.
5. Визначити шляхи поступової віртуалізації процесу навчання та переходу до хмаро орієнтованого НС.
6. Перевірити ефективність використання мережевого НС для отримання знань з інформаційної та кібернетичної безпеки спеціалістів економіки та управління.

Для дослідження питання щодо шляхів покращення якості організації навчального процесу було вибрано метод опитування, що, на думку авторів, найкраще враховує погляди студентів. Для цього використовуємо результати масового багатофункціонального опитування на основі анкетування студентів економічного факультету КНУ імені Тараса Шевченка у 2019-2020 навчальному році [14].

В опитуванні взяли участь 1209 респондентів – студентів 1-4 курсів бакалаврату та 1-2 курсів магістратури економічного факультету КНУ. Оцінювали студенти за 5-бальною шкалою: 1 – найнижча оцінка, 5 – найвища оцінка.

Пріоритетні напрями підвищення якості та необхідні зміни в організації навчального процесу на економічному факультеті відображені на діаграмі (рис.1).

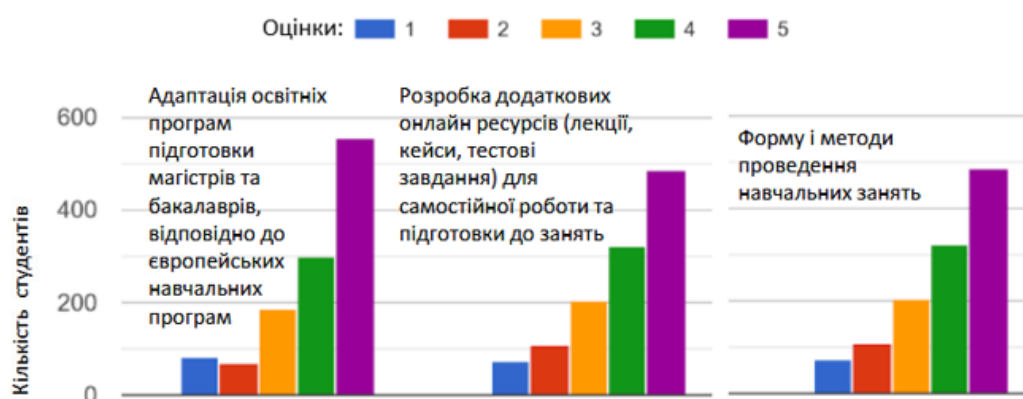


Рис. 1. Оцінка якості освітнього процесу

Як бачимо з рис. 1, студенти ЕФ найвище оцінюють (4-5 балів) європейське спрямування навчальних програм (72% студентів) із залученням навчальних курсів та спеціалістів відомих навчальних закладів, наявність онлайн ресурсів з використанням сучасних форм і методів проведення навчальних завдань (67% студентів).

Організаційні складові навчального процесу, що є важливими для підвищення якості освіти на економічному факультеті, показані на діаграмі рис. 2.

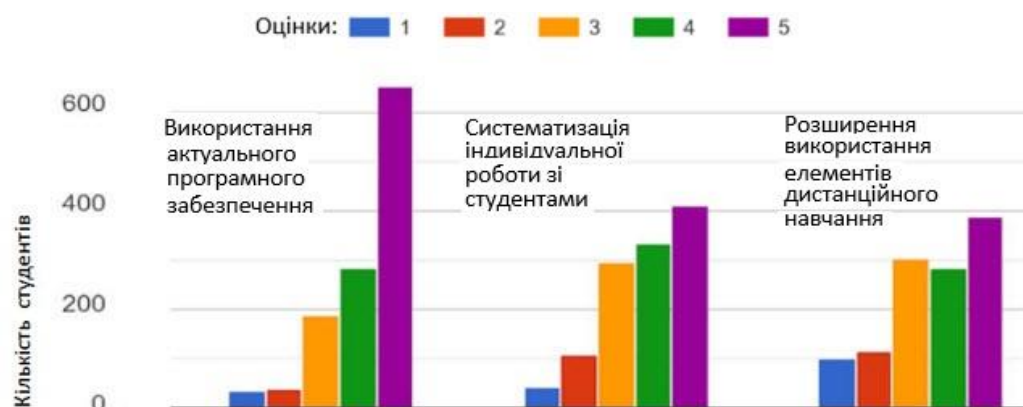


Рис. 2. Оцінка організації навчального процесу

Діаграми на рис. 2 переконливо демонструють бажання студентів (4-5 балів) використовувати сучасне програмне забезпечення (75%), збільшити обсяги самостійної, індивідуальної роботи з можливостями адаптації до їх потреб та інтересів (60%) та розширювати використання дистанційної форми навчання (58%).

Зокрема проведене анкетування студентів на початку навчальних курсів з інформаційної та кібернетичної безпеки щодо необхідності знань із захисту інформації в кіберпросторі за 5-бальною шкалою (1– зовсім не потрібні, 5 – дуже потрібні) у групах студентів спеціальностей «Економічна кібернетика», «Підприємництво, торгівля та біржова діяльність», «Менеджмент інноваційної діяльності» показало високий інтерес до цього напрямку – 78% студентів мотивовані до використання методів та засобів захисту інформації в професійній діяльності (обрали бали 4-5). Для отримання студентами необхідних теоретичних та практичних навичок із захисту інформації виникає потреба у створенні ефективного мережевого середовища навчання з використанням відкритого інформаційно-освітнього простору та сучасних комунікаційних технологій.

Основними трендами сучасної системи освіти є персоналізація навчання, адаптивне навчання, розвиток неформальної освіти, відкритість і доступність освіти, мобільне навчання. Навчання все більше переноситься у віртуальний простір. ЗВО не встигають за таким бурхливим розвитком ІКТ та сучасними методами та засобами навчання. У ЗВО використовують закрите НС з використанням системи управління навчанням, що реалізована на базі відкритої платформи, наприклад, MOODLE. Це структуроване багатовимірне НС, яке поєднує можливості традиційного навчання з сучасними інформаційними технологіями, що базуються на автоматизації взаємодії викладача та студента [12]. Таке середовище є обмеженим щодо складу та структури своїх компонентів і тому має обмежене дидактичне застосування. Зважаючи на те, що на кафедрі інформаційних систем і технологій Київського національного університету імені Тараса Шевченка традиційно використовують закрите НС з використанням систем дистанційного навчання, виникає потреба в розробці методики формування мережевого НС з можливостями подальшої поетапної віртуалізації та переходу у хмари. Практична реалізація такого підходу почалася з формування мережевого НС при підготовці спеціалістів економічного факультету (спеціальності економіки та управління) у межах навчальних курсів «Інформаційна безпека», «Захист інформації», «Кібербезпека». Покроковий перехід до створення хмаро орієнтованого НС з широким використанням відкритого інформаційно-освітнього простору та інноваційних технологій навчання дозволить адаптуватись викладачам до індивідуальних потреб та можливостей кожного студента в набутті необхідних фахових компетенцій.

Метою формування сучасного мережевого НС при вивченні навчальних дисциплін «Інформаційна безпека», «Захист інформації», «Кібербезпека» є підвищення рівня сформованості комплексних знань, навичок і вмінь з інформаційної та кібернетичної безпеки у студентів економічного факультету. Завданням використання НС з інформаційної та кібернетичної безпеки є удосконалення навчально-методичного комплексу вищезазначених дисциплін. Для отримання необхідних практичних навичок із захисту інформації в кіберпросторі необхідно використовувати різноманітні навчальні ресурси, форми організації навчального процесу, сучасні методи та інструменти навчання. Поєднання різних форм, методів та інструментів навчання дозволить досягти бажаного рівня засвоєння навчального матеріалу.

## **2.1. Зміст навчання**

Сучасний спеціаліст з економіки та управління відповідно до стандартів вищої освіти має вміти працювати з інформацією, використовувати сучасні ІКТ для накопичення, обробки, представлення операційних даних та аналізу отриманих результатів. Не менш важливим є отримання знань із захисту отриманої інформації та розробки стратегій інформаційної безпеки.

Отримання комплексних знань, навичок та вмінь з інформаційної та кібернетичної безпеки передбачається при вивченні навчальних дисциплін «Інформаційна безпека», «Захист інформації», «Кібербезпека», які належать до варіативної частини освітньої програми підготовки спеціалістів відповідних спеціальностей з економіки та управління. Відповідно до затверджених робочих програм вищезазначених навчальних дисциплін, студенти в результаті навчання повинні:

- знати основні поняття та визначення з основ інформаційної безпеки;
- знати проблеми та основні загрози інформаційної безпеки;
- знати базові технології мережевої безпеки;
- знати принципи багаторівневого захисту корпоративних інформаційних систем, технології виявлення та запобігання вторгнень, управління інформаційною безпекою;
- знати етапи проєктування систем інформаційної безпеки;
- вміти аналізувати інформаційні потоки та визначати загрози;
- вміти програмно реалізовувати алгоритми захисту інформації;
- вміти вибирати методи захисту інформації і застосовувати їх на практиці для захисту інформації від несанкціонованого доступу.

Це вимагає вивчення ряду тем, пов'язаних з розглядом проблем інформаційної безпеки, базових технологій мережевої безпеки та багаторівневого захисту корпоративних інформаційних систем та управління інформаційною безпекою. У авторській робочій програмі передбачено вивчення таких питань і тем:

- кібербезпека: світ експертів і злочинців;
- кібербезпека: загрози, вразливості та атаки;
- парадигми захисту сучасних ІС;
- мистецтво захисту таємниць;
- мистецтво забезпечення цілісності;
- захист домену кібербезпеки;
- технології захисту від шкідливих програм та спаму;
- захист мереж;
- технології віртуальних захищених мереж VPN;
- загрози інформаційної безпеки в ІС, категорії атак;
- принципи і механізми побудови захисту ІС, діяльність хакерів;
- методи атак, виявлення методів атак;
- технологія автентифікації;
- служби і політики інформаційної безпеки;
- основи криптографії та криптографічний захист інформації;
- шифрування та розробка Інтернет-додатків шифрування;
- використання електронного підпису;
- міжмережеві екрани, перспективи розвитку ІС та технологій;
- забезпечення безпеки хмарних технологій;
- багаторівневий захист та управління інформаційною безпекою.

Класичні форми навчання з вивченням необхідних теоретичних положень, математичних методів перетворення інформації, побудовою відповідних алгоритмів і програм та їх дослідження щодо різних характеристик є неприйнятними у зв'язку з обмеженням обсягу годин і недостатньою технічною підготовкою студентів. Як скоротити час вивчення таких тем без втрати якості майбутнього фахівця – ось цікава задача, з якою зустрічаються різні ЗВО. Ця задача вимагає аналізу можливого

використання вже існуючих відкритих ресурсів і застосуванням нових форм і методів проведення занять.

## 2.2. Відкриті навчальні ресурси з інформаційної безпеки та захисту інформації в кіберпросторі

Як показало вище згадуване опитування щодо шляхів покращення навчального процесу [14], студенти визначають необхідність використання різноманітних типів освітніх ресурсів та використання відкритих сертифікованих курсів за фахом у відповідних навчальних дисциплінах. Можливість отримання практичних знань та сертифікатів від провідних навчальних закладів та компаній світу мотивує студентів до проведення самостійної дослідницької роботи і набуття фаху у сфері інформаційної та кібернетичної безпеки. У зв'язку з переходом на дистанційну форму навчання в умовах карантину така можливість набуває особливої актуальності. Наприклад, на факультеті інформаційних технологій та управління Київського університету імені Бориса Грінченка для студентів пропонується безкоштовне вивчення 4262 курсів університету Coursera, які розроблені провідними університетами світу з отриманням сертифіката (<https://www.coursera.org/browse>). У табл. 1 наведена головна інформація про навчальні ресурси, пов'язані із безпекою.

Таблиця 1

### Порівняння відкритих ресурсів з інформаційної та кібернетичної безпеки

Назва ресурсу	Адреса	Курси	Мова	Платні (+/-)	Опис
Networking Academy CISCO	<a href="https://www.netacad.com/">https://www.netacad.com/</a>	Introduction to Cybersecurity Cybersecurity Essentials CCNA Cybersecurity Operations CCNA Security	Укр. Англ. і ін.	–	Вимагає сертифікації викладача. Для отримання знань у галузі кіберзлочинності, технологій та процедур захисту мереж. Для спеціалістів у галузі мережевої безпеки початкового рівня. Рекомендується для студентів з підготовки до сертифікації CISCO.
Microsoft Virtual Academy	<a href="https://docs.microsoft.com/en-us/learn/modules/security-in-m365/">https://docs.microsoft.com/en-us/learn/modules/security-in-m365/</a> <a href="https://docs.microsoft.com/en-us/learn/modules/security-with-microsoft-365/">https://docs.microsoft.com/en-us/learn/modules/security-with-microsoft-365/</a>	Introduction to security in Microsoft 365 (7 Units) Secure your organization with built-in, intelligent security from Microsoft 365 (6 Units)	Англ.	–	Рішення Microsoft для управління безпекою в організації. Забезпечення цілісного підходу до безпеки, захисту даних, програм та пристроїв у локальній, хмарній та мобільній мережі.
Coursera	<a href="https://www.coursera.org/browse/information-technology/security">https://www.coursera.org/browse/information-technology/security</a>	Introduction to Cybersecurity for Business Cybersecurity for Business Specialization IT Fundamentals for Cybersecurity Specialization	Англ.	+/-	Пропонується 41 курс для початківців від провідних університетів та компаній світу
Magnetic One Academy	<a href="https://magneticoneacademy/course/information-safe/">https://magneticoneacademy/course/information-safe/</a>	Базовий курс з інформаційної безпеки (10 тем, тестові завдання, допоміжні матеріали,	Укр.	+	Для підвищення рівня інформаційної безпеки компанії, забезпечення захисту інфраструктури,



Назва ресурсу	Адреса	Курси	Мова	Платні (+/-)	Опис
		прикладні та практичні відеоуроки)			інтелектуальної власності та збереження конфіденційності інформації. Подано понад 150 практичних рекомендації щодо мінімізації ризиків інформаційної безпеки.
Pro-metheus	<a href="https://edx.prometheus.org.ua/courses/KPI/IS101/2014_T1/about">https://edx.prometheus.org.ua/courses/KPI/IS101/2014_T1/about</a>	Основи інформаційної безпеки	Укр.	–	Платформа масово відкритих онлайн курсів. Надані базові правила поведіння з персональною інформацією в умовах реального зближення фізичного та віртуального світів. Правила безпеки електронних фінансів.
Computer Security and Networks	<a href="https://www.coursehero.org/learn/cybersecurity-domain">https://www.coursehero.org/learn/cybersecurity-domain</a> <a href="https://www.coursehero.org/learn/usable-security">https://www.coursehero.org/learn/usable-security</a>	Cybersecurity and Its Ten Domains  Usable Security	Англ.	–	Відкритий онлайн курс для отримання професіоналами знань з кібербезпеки та її складових. Правила спільної дискусії та взаємодії в Інтернеті.
Using Future Learn	<a href="https://www.futurelearn.com/courses/introduction-to-cybersecurity">https://www.futurelearn.com/courses/introduction-to-cybersecurity</a>	Introduction to Cyber Security	Англ.	–	Отримання основних знань та навичок з кібербезпеки. Правила захисту цифрового життя.

Для обґрунтування вибору відкритих навчальних ресурсів визначено такі критерії вибору:

- організаційний (доступність, зручність використання, кількість користувачів, ролі користувачів);
- функціонально-дидактичний (програма курсу, модульність, представлення навчального матеріалу в різних форматах, тестування, журнал, календар).

За цими критеріями як базовий ресурс були обрані безкоштовні курси Міжнародної мережевої академії CISCO [15]. На рис. 3 представлені наявні курси.

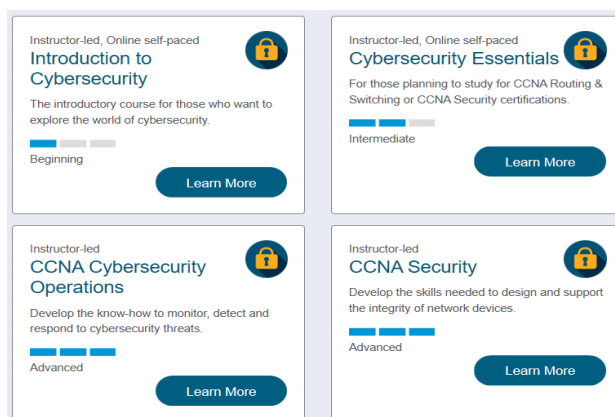


Рис. 3. Тематичні курси Cisco Networking Academy (<https://www.netacad.com/portal/teaching>)

Серед виокремлених навчальних ресурсів, курс «Cybersecurity Essentials» Networking Academy CISCO (див. рис. 4) використовується як елемент навчальних дисциплін «Інформаційна безпека», «Захист інформації», «Кібербезпека». Курси Microsoft Virtual Academy та інші запропоновано використовувати для самостійної роботи студентів.



Рис. 4. Сторінка курсу «Cybersecurity Essentials» Cisco Networking Academy (з екрану курсу)

### 2.3. Мобільні додатки з інформаційної та кібернетичної безпеки

До відкритих навчальних ресурсів належать не тільки серверні (хмарні) а й мобільні ресурси, які можна використати для організації мобільного навчання студентів. Студенти прагнуть до зручності та мобільності у сферах навчальної та дослідницької діяльності (написання статей, участь у конференціях, розробка наукових тем) [14]. Мобільні технології спільно з іншими інформаційними та комунікаційними технологіями, такими як хмарні сховища даних та хмарні обчислення, дозволяють значно підвищити ефективність самостійної роботи студентів [16]. Мобільне навчання (M-Learning) – сучасний напрямок розвитку систем дистанційної освіти із застосуванням мобільних телефонів, смартфонів, планшетів, кишенькових комп'ютерів [17]. Освітні ресурси і інформацію можна зберігати у хмарних сховищах і мати доступ до них з різних мобільних пристроїв незалежно від місця знаходження і часу. Потужність і можливості мобільних пристроїв постійно зростають, тому вони можуть широко використовуватися як зручні та сучасні освітні інструменти, які сприяють отриманню нових знань.

Мобільні пристрої полегшують розуміння навчального матеріалу за допомогою різноманітних предметних мобільних додатків. Мобільні додатки доповненої реальності дозволяють побудувати візуальну модель навчального матеріалу, що розвиває просторову уяву студентів та забезпечує розуміння процесів, властивостей навчальних об'єктів [18]. На рисунку 5 представлені мобільні додатки пов'язані з кібербезпекою. Представлені антивірусні програми, програми з захисту пристроїв та додатків.

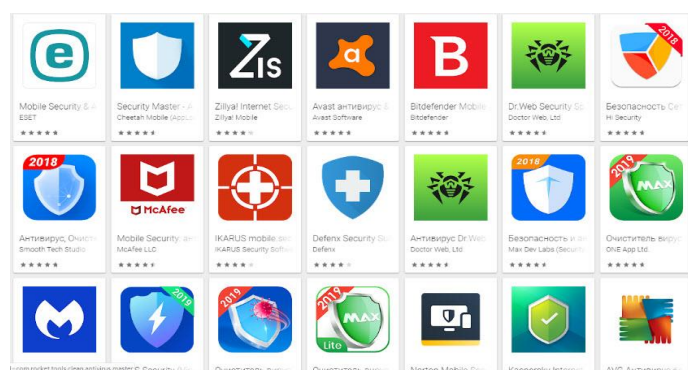


Рис. 5. Мобільні додатки пов'язані з кібербезпекою  
(Play Market – <https://play.google.com/store/search?q=кібербезпека>)

Використовуючи мобільні додатки для самостійної роботи, студент отримує в зручній компактній формі додаткову інформацію про засоби та методи захисту інформації, програми захисту мобільних пристроїв тощо. Із наведеного переліку мобільних додатків, який постійно поповнюється, студент за обраною темою досліджень має доступ до теоретичного матеріалу, може розглянути модель певного процесу, отримати аналіз роботи певного алгоритму тощо. На рис. 6 як приклад представлено деякі додатки за напрямком, пов'язаним з шифруванням даних. Додатки демонструють різні алгоритми шифрування, моделюють роботу шифрувальних машин.

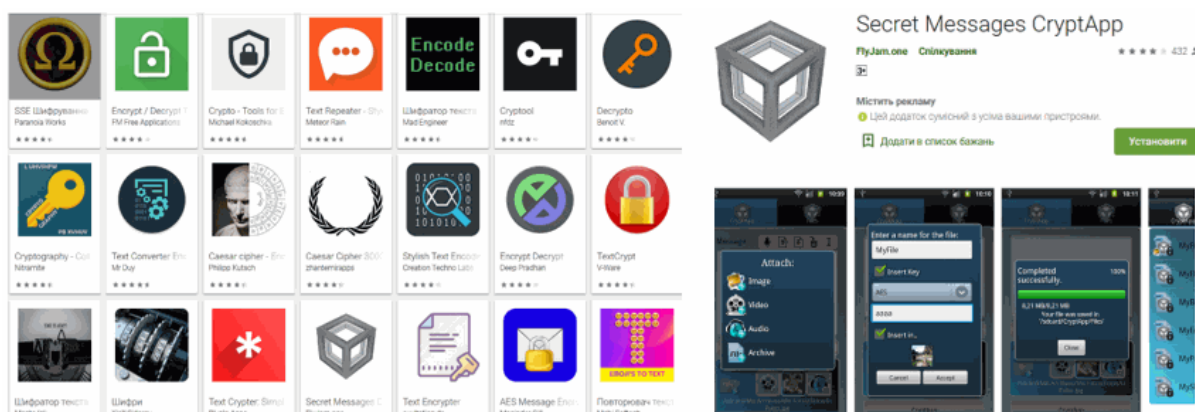


Рис. 6. Мобільні додатки пов'язані з шифруванням тексту  
(Google Play Market – [https://play.google.com/store/search?q=шифрування тексту&c=apps](https://play.google.com/store/search?q=шифрування%20тексту&c=apps))

Використовуючи такий додаток студент вивчає тему «алгоритми шифрування», отримує навички з шифрування та розшифрування тексту.

За допомогою мобільних технологій студенти залучаються до неперервного навчального та дослідницького процесу, який відповідає сучасним вимогам і не залежить від обладнання для доступу до ресурсів.

#### 2.4. Навчальне середовище з інформаційної безпеки та захисту інформації в кіберпросторі

НС має забезпечити управління навчальним процесом, планування навчальних подій, створення та збереження навчальних матеріалів, організацію комунікацій, перевірку та аналіз результатів навчання і створюється на базі систем управління

навчанням (Learning Management System – LMS). Таке середовище має постійно вдосконалюватися завдяки впровадженню інноваційних технологій навчання та широкого використання відкритого інформаційно-освітнього простору.

Мережеве НС створене з використанням таких засобів:

- управління навчанням на базі відкритої LMS MOODLE (або хмаро орієнтовної LMS Canvas);
- збереження навчальних матеріалів з використанням MOODLE, Google Drive або інших хмарних сховищ файлів;
- організації співпраці за допомогою MOODLE, Wiki, Google Docs, Google Sheets, Google Slides або MS Office 365;
- організації комунікації за допомогою MOODLE, електронної пошти, форумів, систем відеозв'язку, віртуальних аудиторій: Gmail, Google Chat, Google Meet, BigBlueButton, Zoom, Webex, MS Teams тощо);
- перевірки знань за допомогою MOODLE, Google Forms, Kahoot та інших хмарних і мобільних засобів проведення тестів, вікторин, навчальних ігор;
- планування навчальних подій за допомогою MOODLE, Google Calendar;
- навчання інформаційній безпеці з використанням відкритих інтернет-ресурсів Networking Academy CISCO, Microsoft Virtual Academy, мобільних додатків, конструкторів доповненої реальності.

Навчання студентів з використанням НС здійснюється за традиційними формами: навчальні заняття (теоретична підготовка), самостійна робота, практична підготовка, контрольні заходи (модульний проміжний контроль, підсумковий контроль). Лекційний матеріал представлено в текстовому, графічному та мультимедійному форматах, який зберігається в хмарному сховищі файлів Google Drive, що дозволяє використовувати гнучку систему доступу до навчальних ресурсів. LMS MOODLE дозволяє інтегрувати до навчальних курсів хмарні сервіси, зокрема відео з Youtube, для розміщення відеолекцій. Посилання на лекції з відповідними правами доступу міститься в електронному навчальному курсі в системі MOODLE. Також додатково використовуються портали знань, відеоматеріали відкритих освітніх ресурсів, які постійно поповнюються. У такий спосіб створюється збірка матеріалів за напрямом навчання відповідно до програми навчання за кожним із змістових модулів. Для вивчення окремих тем передбачено проходження курсів у Networking Academy CISCO з отриманням відповідних сертифікатів.

У Київському національному університеті імені Тараса Шевченка факультетом інформаційних технологій, задовго до появи COVID-19, накопичений певний досвід проведення дистанційних нарад, засідань кафедр, лекцій, практичних та лабораторних занять. Це забезпечувалося, як правило, шляхом використання створеної віртуальної лекційної аудиторії у MOODLE. Для цього були використані засоби відкритого програмного забезпечення BigBlueButton. Головний контингент студентів знаходився в різних районах м. Києва, декілька студентів слухали лекції, перебуваючи за кордоном. Практика дистанційних занять показала достатню якість зв'язку та високу ефективність одночасного проведення занять для невеликої кількості (до 20) [19].

З розповсюдженням в Україні COVID-19, введенням карантинних заходів в освіті та у зв'язку з широким використанням різних платформ дистанційного навчання, у КНУ була створена робоча група за участю одного з авторів щодо функціонування інформаційного та методичного забезпечення освітнього простору в умовах карантинних обмежень. Зокрема були зроблені висновки щодо необхідності розширення існуючого НС шляхом впровадження новітніх інформаційних технологій для підвищення зацікавленості та успішності студентів.

При виконанні практичних завдань використовують антивірусне програмне забезпечення, служби інформаційної безпеки, міжмережеві екрани, системи шифрування, системи виявлення загроз та вразливостей, встановлення віртуальних машин, використання цифрових підписів тощо. Результати виконання практичних завдань представляються у вигляді текстових, табличних звітів та презентацій з використанням Google Docs, Google Sheets, Google Slides та хмарних сервісів із створення інтерактивних презентацій (Prezi), інфографіки (Easel.ly).

Зручним засобом взаємодії викладача та студента є сервіси тестування та опитування. За допомогою таких сервісів кожен студент може сформувати індивідуальний темп навчання та досліджень, усунути прогалини у підготовці за обраним напрямом досліджень. Такі сервіси можна розділити на дві категорії, які відрізняються способом формування питань і відповідей, доступністю і зручністю: хмарні та мобільні. До найвідоміших мобільних сервісів опитування та тестування належать Kahoot, Quizlet, Plickers, Easy Test Maker. Наприклад, Kahoot – це безкоштовний сервіс не тільки для створення різноманітних форм тестів, але й для проведення онлайн вікторин за допомогою спеціального клієнта, що встановлюється на смартфонах студентів (ОС Android, iOS, Windows Phone). Цей сервіс дозволяє викладачу діагностувати відповіді студентів та аналізувати їх.

Після завершенні вивчення кожного змістового модуля студенти проходять проміжний контроль з використанням тестових завдань системи MOODLE, Google Forms та онлайн вікторин за допомогою мобільного сервісу Kahoot.

Консультації у НС переважно здійснювались дистанційно з використанням системи MOODLE, електронної пошти, обговорення, чатів, що допомагає студентам подолати труднощі, які виникають під час вивчення матеріалу як в аудиторії, так і самостійно.

Самостійна робота студентів у НС передбачала проходження запропонованих відкритих навчальних курсів, наприклад, у Microsoft Virtual Academy («Introduction to security in Microsoft 365»), використання порталів знань та відеоматеріалів відкритого освітнього простору. За допомогою мобільних пристроїв (див. рис. 7) можна

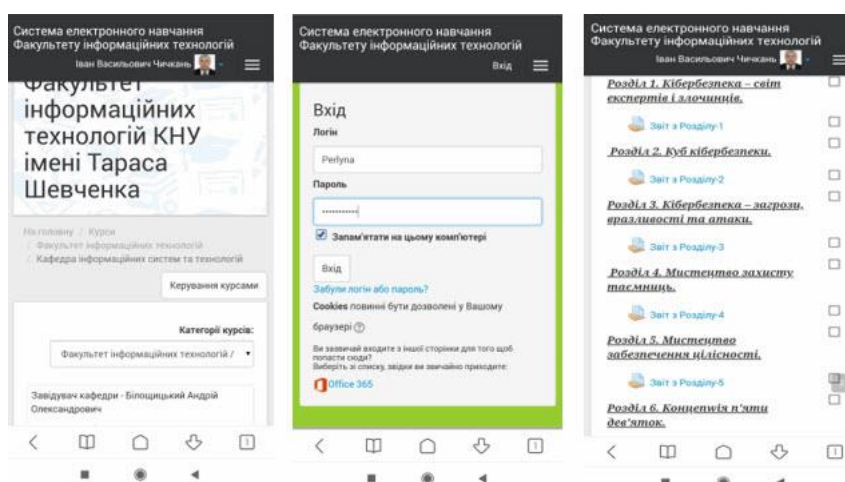


Рис. 7. Доступ до LMS Moodle для ОС Android (з екрана смартфона автора)

організувати самостійну дослідницьку діяльність студента з використанням мобільних систем навчання, систем відеоконференцз'язку, дистанційних курсів, мобільних додатків, електронних публікацій, проєктів, тестових мобільних сервісів, соціальних мереж, електронної пошти тощо. Для доступу до платформи MOODLE з

мобільних пристроїв студенти встановлюють безкоштовний додаток з App Store на iOS для iPhone та iPad та з Google Play Store для ОС Android (рис. 7).

## 2.5. Етапи створення навчального середовища

Сучасне НС має бути інноваційним, насиченим ІКТ. Хмари, соціальні інструменти, мобільні технології, віртуальна та доповнена реальність, технології мультимедіа створили безліч можливостей для нового досвіду навчання настільки, що технологія стала найвищим пріоритетом з питань навчання та розвитку. Зміст навчання зміщується в бік самонавчання і проектноорієнтованої діяльності [13].

В основному закриті комп'ютерно орієнтовані НС ЗВО поступово мають ставати відкритими, персоніфікованими, хмаро орієнтованими, мобільними, віртуальними. Як показує досвід авторів, удосконалення та розвиток НС, впровадження новітніх технологій, форм та засобів навчання є неперервним процесом. Модель розвитку НС інформаційної та кібернетичної безпеки з використанням відкритого інформаційного простору та інноваційних технологій навчання представлена на рис. 8.



Рис. 8. Модель неперервного покрокового розвитку НС з інформаційної та кібернетичної безпеки

Для покрокового переходу до відкритого сучасного НС необхідно:

- інтегрувати в LMS хмарні сховища файлів для збереження матеріалів курсу, наприклад, Google Drive;
- залучити до навчання інтернет-ресурси відкритого освітнього середовища з можливостями отримання сертифікатів та доступу до порталів знань;
- використовувати в навчальному процесі мобільні додатки для доступу до системи навчання, організації комунікацій, фахової підготовки тощо;

- інтегрувати в LMS хмарні сервіси для фахової підготовки, перевірки знань, представлення результатів тощо;
- розширити функціонал LMS за рахунок використання популярних хмарних сервісів для проведення телеконференцій, вебінарів, віртуальних аудиторій, організації онлайн спілкування, навчальних і професійних спільнот тощо;
- інтегрувати LMS з програмним забезпеченням інших розробників, наприклад, з електронними навчальними курсами інших LMS, а також обмін навчальними матеріалами між ними;
- використовувати в навчальному процесі систем доданої реальності (Augmented reality – AR) та віртуальної реальності (Virtual reality – VR) для візуалізації навчальних об'єктів та процесів;
- перемістити LMS у хмару.

Першим кроком може стати використання хмарних сховищ даних для збереження навчальних матеріалів курсу, використання відкритого інформаційно-освітнього середовища для залучення інтернет-ресурсів за фахом від провідних навчальних закладів та компаній світу, організація дистанційного навчання шляхом створення віртуальної лекційної аудиторії, використання мобільних додатків та технологій візуалізації, широке використання хмарних сервісів для фахової підготовки та представлення результатів. Такий підхід до створення НС також впроваджується при підготовці студентів із спеціальності 125 «Кібербезпека» у Київському університеті імені Бориса Грінченка [20].

Наступним кроком може стати перенесення системи управління навчальним процесом у хмари, створення віртуальних лабораторій для практичної підготовки майбутніх спеціалістів. Це дозволить не встановлювати і не супроводжувати власні LMS самостійно на своїх внутрішніх ресурсах. Отримання навчальним закладом у провайдера відповідної послуги за хмарною моделлю SaaS (Software as a Service) передбачає використання LMS як створеної провайдером Web-платформи для управління навчанням. Водночас усі роботи по забезпеченню інсталяції, налагодження, підтримання працездатності та поновлення програмного і технічного забезпечення покладається на провайдера. Це дозволяє використовувати сучасні LMS навіть невеликим навчальним закладам і окремим педагогічним працівникам [17]. Існує інтеграція Moodle з хмарною версією. MoodleCloud – це доступна платформа, що характеризується простотою, безкоштовним обслуговуванням, автоматичним оновленням версії Moodle, безкоштовним використанням для обмеженої кількості користувачів (до 50) [21]. Система MOODLE була розгорнута на хмарному сервері <https://moodlecloud.com/> для викладання магістрам (9 студентам) навчальної дисципліни «Кібербезпека» у межах спеціальності 076 «Підприємництво, торгівля та біржова діяльність». Сторінка курсу «Кібербезпека» в LMS MoodleCloud (<https://security.moodlecloud.com/courses/view.php?id=3>).

## **2.6. Аналіз результатів навчання з інформаційної та кібернетичної безпеки спеціалістів економіки та управління**

Проведене анкетування студентів після закінчення вищезазначених навчальних курсів щодо готовності до використання хмарних сервісів, мобільних додатків, систем дистанційного навчання показало, що 89% студентів оцінило на 4-5 за 5-ти бальною шкалою необхідність та зручність використання цих технологій у навчанні. Студенти мотивовані до проходження сертифікованих курсів з інформаційної та кібернетичної безпеки. На рис. 9 представлена аналітика проходження курсу «Cybersecurity

Essentials» Академії CISCO, яка демонструє високі показники активності студентів групи «Менеджмент інноваційної діяльності» (магістри).

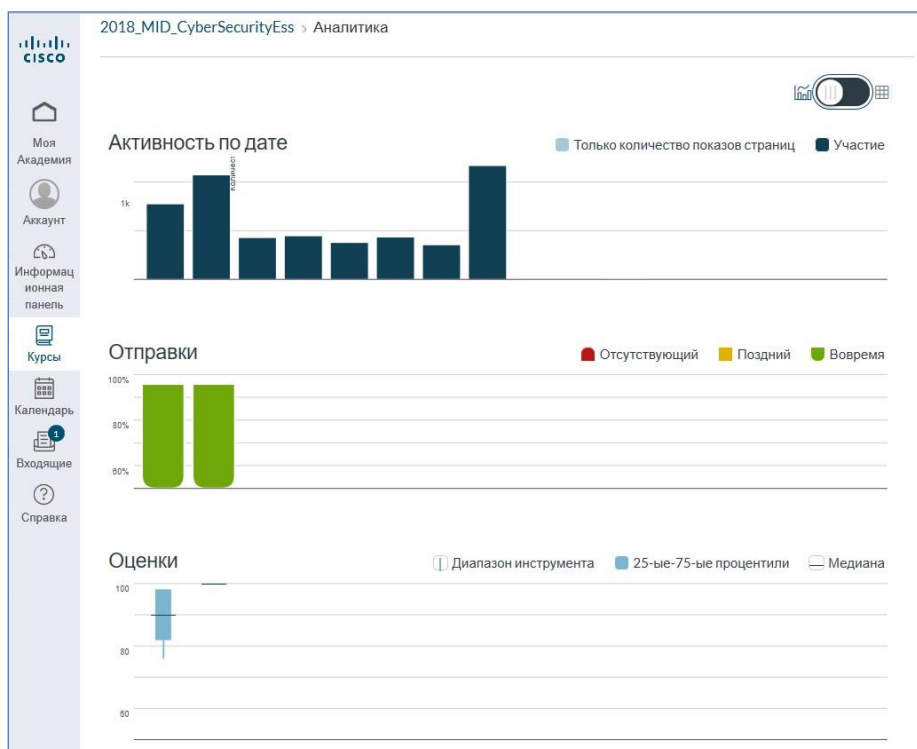


Рис. 9. Аналітика вивчення курсу «Cybersecurity Essentials» групи студентів

Студенти працюють за затвердженим викладачем графіком, вчасно відправляють завдання. Викладач має дані про активність виконання завдань за датами та іншими показниками. Зокрема бачимо на рис.8, що відсутнє пізні виконання або не виконання завдань. На рис. 10 показана успішність студентів освітньої програми «Економічна кібернетика» навчальної дисципліни «Захист інформації» у 2019 році (порівняння оцінок за курс CISCO та інших елементів навчання).

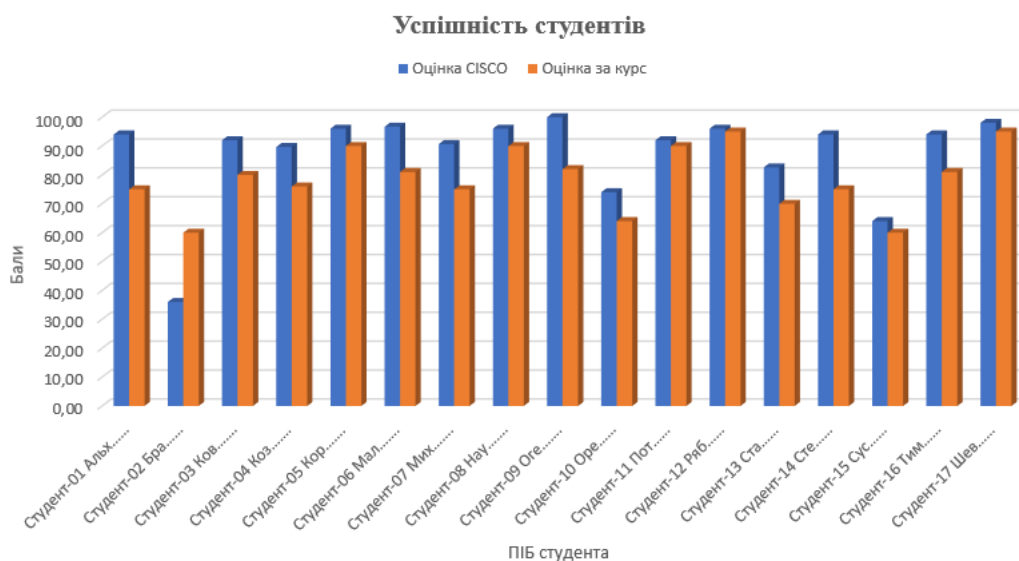


Рис. 10. Результати вивчення курсу «Захист інформації» групи студентів



Водночас результати проходження курсу (виконання 100% завдань) «Cybersecurity Essentials» Academy CISCO у 94,2 % студентів є вищими по відношенню до виконання інших завдань навчальної дисципліни з використанням традиційних аудиторних форм навчання. Робота в системі Academy CISCO дозволяє студентам планувати і виконувати завдання в зручний час у межах затвердженого графіка діяльності, можливість отримання сертифіката підвищує активність студентів і результати навчання (рис.11).

Ім'я	Фамил	ІД ст	Адрес ел	последний вход	Итог	Бал	Финал	ВЫПОЛНИТЬ	Получить сертификат
Студент	Звич...	✓	kurpiu@g...	17 Фев 2019	-	-		<input type="checkbox"/>	
Карина	Казб...	✓	karina.ka...	3 Apr 2019	97.33%	-		<input checked="" type="checkbox"/>	⚙
Андрій	Репе...	✓	arepeczk...	3 Apr 2019	90.83%	-		<input checked="" type="checkbox"/>	⚙
Анастасія	Анд...	✓	anastasi...	1 Apr 2019	76.17%	-		<input checked="" type="checkbox"/>	⚙
Анастасія	Пузи...	✓	ruzirevic...	1 Apr 2019	86.00%	-		<input checked="" type="checkbox"/>	⚙
Ірина	Тімч...	✓	irishatim...	3 Apr 2019	97.50%	-		<input checked="" type="checkbox"/>	⚙
Yelyzaveta	Rud...	✓	inflieta@...	7 Apr 2019	95.00%	-		<input checked="" type="checkbox"/>	⚙
Svitlana	Svid...	✓	svidersk...	1 Apr 2019	97.00%	-		<input checked="" type="checkbox"/>	⚙
Roman	Kotyky	✓	sleepors...	28 Июнь 2019	84.00%	-		<input checked="" type="checkbox"/>	⚙
Ihor	Mykh...	✓	igorr.thl...	1 Apr 2019	91.50%	-		<input checked="" type="checkbox"/>	⚙
Anna	Pryk...	✓	anna.v.pr...	1 Apr 2019	80.33%	-		<input checked="" type="checkbox"/>	⚙
Anastasia	Filina	✓	fnastia52...	1 Apr 2019	82.00%	-		<input checked="" type="checkbox"/>	⚙

Рис. 11. Результати проходження курсу «Cybersecurity Essentials», %

Усі студенти групи «Економічна кібернетика» (бакалаври) отримали сертифікати Academy CISCO (див. рис. 11). У цій групі найнижча оцінка за курс –76,17%, найвища – 97,5%.

93,1% студентів, які навчаються за освітніми програмами «Менеджмент інноваційної діяльності» (магістри) та «Економічна кібернетика» (бакалаври) успішно пройшли курси і отримали сертифікати Academy CISCO. Робота 6,9% студентів оцінена як задовільна, тому вони не отримали. Не зафіксовано жодного студента, який би отримав незадовільну оцінку.

### 3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Діловий світ стає більш глобальним, мобільним й цифровим, тому необхідно підвищувати рівень підготовки майбутніх фахівців, зокрема з економіки та управління відповідно до потреб цифрових технологій. У зв'язку з цим необхідно розвивати національну стратегію кіберосвіти, тобто розгортати спеціальну та загальну систему кіберосвіти, зокрема приділяти більше уваги формуванню «культури кібербезпеки» у майбутніх фахівців цифрової економіки.

Відповідно до окреслених у статті вимог до навчального середовища з інформаційної та кібернетичної безпеки розроблена методика поетапного впровадження нових інноваційних технологій навчання з використанням відкритого інформаційно-освітнього простору, технологій мобільного навчання, хмарних додатків та сервісів. У результаті дослідження визначені етапи поступового переходу від закритого мережевого навчального середовища до відкритого, персоналізованого, хмаро орієнтованого. Неперервне

вдосконалення навчального середовища з можливостями поетапної віртуалізації дозволяє поступово переходити до дистанційного навчання з використанням віртуальних аудиторій та лабораторій, технології доповненої реальності для побудови візуальної моделі навчального матеріалу, що зміщує зміст навчання в бік самонавчання та проєктноорієнтованої діяльності.

Результати дослідження показали, що використання запропонованого навчального середовища сприяє отриманню студентами необхідних знань, умінь та навичок з інформаційної та кібернетичної безпеки, підвищує зацікавленість та успішність студентів. Використання відкритих навчальних ресурсів з можливістю отримання сертифікатів, мобільних та хмарних додатків дозволяє студентам обрати зручні для них форми та засоби навчання для отримання практичних навичок із захисту інформації в кіберпросторі.

Напрямки подальших досліджень вбачаємо у впровадженні нових технологій навчання, розробці навчального середовища з інформаційної та кібернетичної безпеки для здобувачів вищої освіти у галузях знань, що охоплюють гуманітарні та природничі науки.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Кабінет міністрів України. (2018, Січ. 17) *Розпорядження No 67–р. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації*. [Електронний ресурс]. Доступно: <http://zakon3.rada.gov.ua/laws/show/67-2018-р>. Дата звернення: Груд. 26, 2019.
- [2] Цифрова адженда України – 2020 ("Цифровий порядок денний" – 2020). Концептуальні засади (версія 1.0). Першочергові сфери, ініціативи, проєкти "цифровізації" України до 2020 року. NITECH office. Грудень 2016. 90 с. [Електронний ресурс]. Доступно: <https://ucsi.org.ua/uploads/files/58e78ee3c3922.pdf>. Дата звернення: Квіт. 21, 2020.
- [3] Ю. Д. Жданова, С. О. Спасітелева, С. М. Шевченко, "Формування у студентів IT-спеціальностей компетентностей в області захисту інформації з використанням криптографічних служб .NET FRAMEWORK", *Фізико-математична освіта*. Випуск 1(19). С.48-54, 2019.
- [4] Глобальное исследование утечек конфиденциальной информации в первом полугодии 2018 года. [Електронний ресурс]. Доступно: [https://www.infowatch.ru/report2018\\_half](https://www.infowatch.ru/report2018_half). Дата звернення: Груд. 26, 2019.
- [5] Верховна Рада України. (2017, Жовт. 05) *Закон № 2163-VIII, Про основні засади забезпечення кібербезпеки України*. [Електронний ресурс]. Доступно: <https://zakon.rada.gov.ua/laws/show/2163-19>. Дата звернення: Квіт. 17, 2020.
- [6] Г. Т. Карчева, І. Я. Карчева "Удосконалення освіти в умовах цифрової економіки" на *VII Всеукр. наук.-практ. конф. Проблеми забезпечення ефективного функціонування та стабільного розвитку банківської системи та економіки*, Київ, 2017, с.320–322.
- [7] І. В. Діордіца, "Стан підготовки фахівців у сфері кібербезпеки". *Visegrad Journal of Human Rights*, №6/1, с.53– 59, 2016.
- [8] G. Austin, Eds. *Cyber Security Education. Principles and Policies*. New York, NY, UK and New York: Routledge, 2020.
- [9] K. Daimi, and G. Francia, Eds. *Innovations in Cybersecurity Education*. London, UK: Springer, 2020, doi: <https://doi.org/10.1007/978-3-030-50244-7>.
- [10] В. Ю. Биков, "Відкрите навчальне середовище та сучасні мережні інструменти систем відкритої освіти", *Науковий часопис НПУ імені М. П. Драгоманова. Серія 2: Комп'ютерно-орієнтовані системи навчання*, № 9, с. 9-15, 2010. [Електронний ресурс]. Доступно: [http://nbuv.gov.ua/UJRN/Nchnpu\\_2\\_2010\\_9\\_4](http://nbuv.gov.ua/UJRN/Nchnpu_2_2010_9_4). Дата звернення: Квіт. 17, 2020.
- [11] А. М. Гуржій, В. В. Лапінський, "Електронні освітні ресурси як основа сучасного навчального середовища загальноосвітніх навчальних закладів", *Інформаційні технології в освіті*, № 15, с. 30-37, 2013. [Електронний ресурс]. Доступно: [http://nbuv.gov.ua/UJRN/itvo\\_2013\\_15\\_5](http://nbuv.gov.ua/UJRN/itvo_2013_15_5) [17 квітня 2020 р.].
- [12] С. Г. Литвинова, "Розвиток навчального середовища загальноосвітнього навчального закладу як наукова проблема" *Науковий вісник Мелітопольського державного педагогічного університету. Сер.: Педагогіка*. № 1, с. 39-47, 2014. [Електронний ресурс]. Доступно: [http://nbuv.gov.ua/UJRN/Nvmdpu\\_2014\\_1\\_7](http://nbuv.gov.ua/UJRN/Nvmdpu_2014_1_7). Дата звернення: Січ. 07, 2020.

- [13] О. П. Пінчук, С. Г. Литвинова, та О. Ю. Буров, "Синтетичне навчальне середовище – крок до нової освіти", *Інформаційні технології та засоби навчання*, 4(60), с.28-45, 2017. [Електронний ресурс] Доступно: <https://journal.iitta.gov.ua/index.php/itlt/article/view/1831>. Дата звернення: Груд. 30, 2019.
- [14] Результати опитування студентів економічного факультету КНУ, 2019/2020 н.р [Електронний ресурс] Доступно: <http://econom.univ.kiev.ua/wp-content/uploads/2019/12/Результати-опитування-студентів-2019.pdf>. Дата звернення: Квіт. 21, 2020.
- [15] CISCO Networking Academy: Security courses. [Електронний ресурс]. Доступно: <https://www.netacad.com/portal/teaching>. Дата звернення: Квіт. 07, 2020.
- [16] О. М. Кривонос, О. В. Коротун, "Етапи проектування хмаро орієнтованого середовища у навчанні баз даних майбутніх вчителів інформатики", *Інформаційні технології і засоби навчання*, 1(63), с. 130-145, 2018. [Електронний ресурс]. Доступно: <https://journal.iitta.gov.ua/index.php/itlt/article/view/1866>. Дата звернення: Квіт. 08, 2020.
- [17] ЮНЕСКО (2013). *Рекомендації по політике в області мобільного обучения*. [Електронний ресурс]. Доступно: <http://iite.unesco.org/pics/publications/ru/files/3214738.pdf>. Дата звернення: Січ. 10, 2020.
- [18] "Дополненная реальность в образовании" *VR-Journal | Портал о виртуальной и дополненной реальности, 2017*. [Електронний ресурс]. Доступно: <https://vr-j.ru/stati-i-obzory/dopolnennaya-realnost-v-obrazovanii>. Дата звернення: Січ. 10, 2020.
- [19] BigBlueButton - Open Source Web Conferencing (2020) *Engage Your Online Students: BigBlueButton is a web conferencing system designed for online learning*. [Електронний ресурс] Доступно: <https://bigbluebutton.org>. Дата звернення: Січ. 05, 2020.
- [20] Ю. Д. Жданова, С. О. Спасітелева, С. М. Шевченко, "Застосування бібліотеки класів Security.Cryptography для практичної підготовки спеціалістів з кібербезпеки", *Кібербезпека: освіта, наука, техніка: науково-технічний журнал*, 4(4), с.44-53, 2019.
- [21] Л. В. Ноздріна, "Інноваційні CLOUD COMPUTING: виклики для освіти", *Інформаційні технології в освіті*, 1 (38), с.19-50, 2019.

Матеріал надійшов до редакції 12.01.2020р.

## ОБРАЗОВАТЕЛЬНАЯ СРЕДА ДЛЯ ФОРМИРОВАНИЯ КУЛЬТУРЫ БЕЗОПАСНОГО ПОВЕДЕНИЯ В КИБЕРПРОСТРАНСТВЕ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ЭКОНОМИКИ И УПРАВЛЕНИЯ

### Чичкань Иван Васильевич

кандидат физико-математических наук, доцент, доцент кафедры информационных систем и технологий Киевский национальный университет имени Тараса Шевченко, г. Киев, Украина  
ORCID ID 0000-0002-0854-389X  
[Chychkan@FIT.knu.ua](mailto:Chychkan@FIT.knu.ua)

### Спасителева Светлана Алексеевна

кандидат физико-математических наук, доцент, доцент кафедры информационной и кибернетической безопасности Киевский университет имени Бориса Гринченко, г. Киев, Украина  
ORCID ID 0000-0003-4993-6355  
[s.spasitielieva@kubg.edu.ua](mailto:s.spasitielieva@kubg.edu.ua)

### Жданова Юлия Дмитриевна

кандидат физико-математических наук, доцент, доцент кафедры информационной и кибернетической безопасности Киевский университет имени Бориса Гринченко, г. Киев, Украина  
ORCID ID 0000-0002-9277-4972  
[y.zhdanova@kubg.edu.ua](mailto:y.zhdanova@kubg.edu.ua)

**Аннотация.** Статья посвящена проблеме подготовки современных специалистов областей знаний 05 «Социальные и поведенческие науки» и 07 «Управление и администрирование» к безопасному поведению в киберпространстве. Предложена методика создания сетевой обучающей среды с возможностями дальнейшей поэтапной виртуализации, перехода к облачным технологиям и дистанционной форме обучения. Рассмотрены вопросы формирования у студентов специализированно-профессиональных знаний и умений по

информационной и кибернетической безопасности. По результатам изучения психолого-педагогической литературы и собственного 10-летнего опыта определен объем теоретических и практических знаний для формирования навыков и умений по защите информации в кибернетическом пространстве. Изложен перечень требований к уровню сформированности профессионально значимых характеристик специалиста по экономике и управлению в сфере защиты информации. Обоснована актуальность и целесообразность формирования современной сетевой обучающей среды с широким использованием открытых образовательных ресурсов, мобильных приложений, облачных технологий для повышения уровня компетентности студентов по информационной и кибернетической безопасности. Проведен сравнительный анализ ресурсов открытого информационно-образовательного пространства, которые могут использоваться как обязательные элементы учебной дисциплины и привлекаться для самостоятельной работы студентов. Определены критерии выбора открытых учебных ресурсов и предложена методология их использования. Рассмотрены формы организации учебного процесса, современные методы, инструменты и средства обучения для сетевой обучающей среды высших учебных заведений. Представлены пути реализации предложенной методики поэтапного создания образовательной среды в Киевском национальном университете имени Тараса Шевченко в рамках учебных дисциплин «Информационная безопасность», «Защита информации», «Кибербезопасность» и в Киевском университете имени Бориса Гринченко. Обосновано, что использование инновационных технологий обучения, открытых учебных ресурсов ведущих учебных заведений, облачных и мобильных сервисов, связанных с защитой данных, позволяет подготовить специалистов с практическими навыками по защите информации, востребованных на рынке труда.

**Ключевые слова:** информационная безопасность; кибернетическая безопасность; облачно-ориентированная образовательная среда; открытое информационно-образовательное пространство.

## THE EDUCATIONAL ENVIRONMENT FOR FORMING SECURE BASE BEHAVIOR IN CYBERSPACE OF FUTURE PROFESSIONALS IN ECONOMICS AND MANAGEMENT

### Ivan V. Chychkan

PhD of Physical and Mathematical Sciences, Associate Professor, Associate Professor at the Department of Information Systems and Technologies

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ORCID ID 0000-0002-0854-389X

*Chychkan@FIT.knu.ua*

### Svitlana O. Spasiteleva

PhD of Physical and Mathematical Sciences, Associate Professor, Associate Professor at the Department of Information and Cyber Security

Borys Grinchenko Kyiv University, Kyiv, Ukraine

ORCID ID 0000-0003-4993-6355

*s.spasiteliava@kubg.edu.ua*

### Yuliia D. Zhdanova

PhD of Physical and Mathematical Sciences, Associate Professor, Associate Professor at the Department of Information and Cyber Security

Borys Grinchenko Kyiv University, Kyiv, Ukraine

ORCID ID 0000-0002-9277-4972

*y.zhdanova@kubg.edu.ua*

**Abstract.** The article deals with the problem of training modern specialists in the fields of knowledge 05 «Social and behavioral sciences» and 07 «Management and administration» for secure base behavior in cyberspace. The technique of creating a network learning environment with the possibilities of step-by-step virtualization, the use of cloud technologies and distance learning has been described. Issues of providing students with specialized and professional knowledge and skills in information security and cyber security are considered. Based on the

results of research in the psycho-pedagogical literature and our own 10 years of experience, we have determined the amount of theoretical and practical knowledge for the formation of skills and abilities in information protection of cyberspace. The list of requirements for professionally significant characteristics of the economics and management specialists in the field of information protection has been determined. The article substantiates the need to use a modern networked learning environment with wide use of open educational resources, mobile applications, cloud technologies to increase the level of competence of students in information and cyber security. Comparative analysis of open information educational space resources, which can be used as elements of the academic discipline and used for independent work of students, has been made. The criteria for selecting open learning resources has been defined and the methodology for their use has been proposed. The organization forms of the educational process, modern methods and teaching tools for the network learning environment of a higher education institution have been described. The ways of implementation of the proposed methodology step-by-step creation of a learning environment at the Taras Shevchenko National University of Kyiv and Borys Grinchenko Kyiv University have been presented on the example of academic disciplines «Information Security», «Information Protection», «Cybersecurity». It is proved that the use of innovative training technologies, open learning resources of leading educational institutions, cloud and mobile services from data protection allows training professionals with practical information security skills that are in demand in the labor market.

**Keywords:** Information Security; Cyber security; cloud-based learning environment; open information and educational space.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

- [1] Cabinet of Ministers of Ukraine. (2018, Jan. 17) Ordinance *No 67-r*. On Approval of the Concept of Development of the Digital Economy and Society of Ukraine for 2018-2020 and Approval of the Plan of Measures for its Implementation. [Online]. Available: <http://zakon3.rada.gov.ua/laws/show/67-2018-p> Accessed on: Dec. 26, 2019. (in Ukrainian).
- [2] Digital Agenda of Ukraine - 2020. Conceptual principles (version 1.0). Priority areas, initiatives, projects of "digitalization" of Ukraine until 2020. HITECH office. Gruden` 2016. 90 p. [Online] Available: <https://ucc.org.ua/uploads/files/58e78ee3c3922.pdf>. Accessed on: Apr. 21, 2020. (in Ukrainian).
- [3] Yu. D. Zhdanova, S. O. Spasiteleva, S. M. Shevchenko. "Formation Of Information Protection Competence To Students Of It-Specialties With Using .NET FRAMEWORK Cryptographic Services", *Physical and Mathematical Education*, 19(1), pp.48-54, 2019 (in Ukrainian).
- [4] Global study of confidential information leaks in the first half of 2018. [Online]. Available: [https://www.infowatch.ru/report2018\\_half](https://www.infowatch.ru/report2018_half). Accessed on: Dec. 27, 2019. (in Russian).
- [5] Verkhovna Rada of Ukraine. (2017, Oct. 05) *Law № 2163-VIII, On the Basic Principles of Cyber Security of Ukraine*. [Online] Available: <https://zakon.rada.gov.ua/laws/show/2163-19>. Accessed on: Apr. 17, 2020. (In Ukrainian).
- [6] G.T. Karcheva, I.Ya.Karcheva. "Improving education in a digital economy" in VII *All-Ukrainian scientific-practical conf. Problems of ensuring the efficient functioning and stable development of the banking system and economy*, Kiyv, 2017, pp.320–322. (in Ukrainian).
- [7] I.V. Diordicza, "The state of training of specialists in the field of cybersecurity" *Visegrad Journal of Human Rights*, 2016. no. 6/1, pp.53– 59. (in Ukrainian).
- [8] G. Austin, Eds. *Cyber Security Education. Principles and Policies*. New York, NY, UK and New York: Routledge, 2020. (in English).
- [9] K. Daimi, and G. Francia, Eds. *Innovations in Cybersecurity Education*. London, UK: Springer, 2020, doi: <https://doi.org/10.1007/978-3-030-50244-7>. (In English).
- [10] V. Yu. Bykov, "Open learning environment and modern network tools of open education systems" *Naukovij chasopis NPU imeni M. P. Dragomanova. Seriya 2: Komp'yuterno-orientovani sistemi navchannya*, no. 9. pp. 9-15, 2010. [Online] Available: [http://nbuv.gov.ua/UJRN/Nchnpu\\_2\\_2010\\_9\\_4](http://nbuv.gov.ua/UJRN/Nchnpu_2_2010_9_4). Accessed on: Apr. 17, 2020. (in Ukrainian).
- [11] A.M Gurzhiy, V.V. Lapins'kij, "Electronic educational resources as the basis of the modern educational environment of secondary schools", *Informacziyni tehnologii v osviti*, no. 15, pp. 30-37, 2013. [Online] Available: [http://nbuv.gov.ua/UJRN/itvo\\_2013\\_15\\_5](http://nbuv.gov.ua/UJRN/itvo_2013_15_5). Accessed on: Apr. 17, 2020. (in Ukrainian).
- [12] S. H. Lytvynova, "Development of educational environment of a comprehensive educational institution as a scientific problem". *Naukovyy visnyk Melitopol's'koho derzhavnoho pedahohichnoho universytetu. Ser:*

- Pedahohika*. no. 1. pp. 39-47, 2014. [Online]. Available: [http://nbuv.gov.ua/UJRN/Nvmdpu\\_2014\\_1\\_7](http://nbuv.gov.ua/UJRN/Nvmdpu_2014_1_7). Accessed on: Jan. 7, 2020. (in Ukrainian).
- [13] O.P. Pinchuk, S. H. Lytvynova, and O. Yu. Burov, "Synthetic learning environment – a step towards a new education", *Information Technologies and Learning Tools*, 4(60), pp. 28-45, 2017. [Online]. Available: <https://journal.iitta.gov.ua/index.php/itlt/article/view/1831>. Accessed on: Dec. 30, 2019. (in Ukrainian).
- [14] The results of a survey of students of the Faculty of Economics of KNU, 2019/2020 academic year. [Online] Available: <http://econom.univ.kiev.ua/wp-content/uploads/2019/12/Rezultati-opituvannya-studentiv-2019.pdf>. Accessed on: Apr. 21, 2020. (in Ukrainian).
- [15] CISCO Networking Academy: Security courses. [Online]. Available: <https://www.netacad.com/portal/teaching>. Accessed on: Jan. 7, 2020.
- [16] O.M. Kryvonos, O.V. Korotun, "Stages of Designing a Cloud-Oriented Environment in Learning Databases of Future Teachers of Informatics", *Information Technologies and Learning Tools*, 1(63), pp. 130-145, 2018. [Online]. Available: <https://journal.iitta.gov.ua/index.php/itlt/article/view/1866>. Accessed on: Jan. 8, 2020. (in Ukrainian).
- [17] UNESCO Policy Guidelines for Mobile Learning, [Online]. Available: <http://iite.unesco.org/pics/publications/ru/files/3214738.pdf>. Accessed on: Jan. 10, 2020. (in Russian).
- [18] Augmented reality in education. *VR-Journal / Virtual and augmented reality portal* [Online] Available: <https://vr-j.ru/stati-i-obzory/dopolnennaya-realnost-v-obrazovanii>. Accessed on: Jan. 10, 2020. (in Russian).
- [19] Engage Your Online Students: BigBlueButton is a web conferencing system designed for online learning. [Online]. Available: <https://bigbluebutton.org>. Accessed on: Jan. 5, 2020. (in English).
- [20] Yu. D. Zhdanova, S.O. Spasiteleva and S.M. Shevchenko, "The Application of the Security.Cryptography Class Library for the Practical Training of Cyber Security Specialists" *Kiberbezpeka: osvita, nauka, tekhnika: naukovo-tehnichnyy zhurnal*, 4(4), pp.44-53, 2019. (in Ukrainian).
- [21] L.V. Nozdrina, "Innovative CLOUD COMPUTING: Challenges for Education", *Informatsiyni tekhnolohiyi v osviti*, 1(38), pp. 19-50, 2019. (in Ukrainian).

