



**Олексій Самоїленко** – кандидат педагогічних наук, доцент Навчально-наукового інституту інформаційної безпеки Служби Безпеки України, м. Київ, Україна.

**Коло наукових інтересів:** можливості освітньо-цифрового середовища, підготовка бакалаврів з кібербезпеки, кібербезпека.

**e-mail:** [samoilenko\\_aleksey@outlook.com](mailto:samoilenko_aleksey@outlook.com)

**ORCID iD:** <https://orcid.org/0000-0002-6374-4168>

УДК 37.014.623

<https://doi.org/10.32405/2411-1317-2020-4-199-206>

## ТЕХНОЛОГІЯ ВПРОВАДЖЕННЯ КОНСТРУКТИВНОЇ МОДЕЛІ ПІДГОТОВКИ БАКАЛАВРІВ З КІБЕРБЕЗПЕКИ В УМОВАХ ОСВІТНЬО-ЦИФРОВОГО СЕРЕДОВИЩА

У статті висвітлено технологію впровадження конструктивної моделі підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища. Визначено, що технологія впровадження конструктивної моделі закладає в основу методичні (методики, рекомендації з реалізації підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища з урахуванням дидактичних і психологічних аспектів), програмні (мережеві системні програми, комп'ютерні навчальні програми, інструментальні середовища для створення навчальних програм підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища. На основі аналізу психолого-педагогічної літератури визначено, що впровадження конструктивної моделі вимагає розробки освітніх програм силабусів та освітнього контенту, причому в електронному вигляді. Доведено, що робота в освітньо-цифровому середовищі може здійснюватися як в рамках аудиторного навчання, так і позааудиторного навчання. Зазначено, що за рахунок такої інтеграції підготовка бакалаврів з кібербезпеки в умовах окресленого середовища може здійснюватися за індивідуальною траєкторією навчання.

**Ключові слова:** технологія, конструктивна модель; підготовка бакалаврів; бакалаври з кібербезпеки; освітньо-цифрове середовище.

**Постановка проблеми.** Професійна підготовка бакалавра з кібербезпеки представляє собою цілеспрямований, системний і послідовний змодельований процес підпорядкований певній системі, яка забезпечує його ефективність. У Професійна діяльність фахівців із кібербезпеки щодо реалізації окреслених стратегічних напрямів безпеки кіберпростору України є недостатньо ефективною в аспекті виявлення й усунення прихованих і відкритих кіберзагроз. Розроблена автором конструктивна модель підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища, враховує потреби сьогодення та ключові педагогічні аспекти підготовки фахівців означеної категорії [1]. Але є потреба у

технології впровадження конструктивної моделі підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища.

**Аналіз останніх досліджень і публікацій.** Професійна підготовка бакалаврів з кібербезпеки спрямована на формування готовності магістра до професійної діяльності, що передбачає розуміння змісту професійної діяльності, усвідомлення мотивів, здібностей, можливостей і бажання ефективно провадити професійну діяльність, володіння професійними знаннями, уміннями й навичками. Водночас домінантою професійної підготовки є високий рівень науково-дослідницької діяльності в галузі кібербезпеки, що інтегрує професійні та науково-дослідницькі університет, компетентності, досвід, самоосвіту [2]. Професійна підготовка бакалаврів з кібербезпеки в Україні регульована законодавчо-нормативними документами, а саме: Законами України «Про освіту» [3], «Про вищу освіту» [4], «Про інформацію» [5], Стратегією кібербезпеки України [6], Законом «Про національну безпеку України» [7], та ін. Обґрунтування нових концептуальних підходів до вдосконалення професійної підготовки бакалаврів з кібербезпеки потребує в контексті інтеграції України до європейського освітньо-інформаційного простору ретельної уваги до результатів наукових пошуків і прогностичних ідей. Для України характерний високий рівень розвитку національної системи кібербезпеки, що уможливорює потужна стратегічна й законодавча база.

**Мета статті** – оприлюднення технології впровадження конструктивної моделі підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища, що закладає в основу методичні, програмні, технічні, інформаційні та організаційні аспекти.

**Виклад основного матеріалу дослідження.** Технології впровадження конструктивної моделі підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища, закладають в основу методичні, програмні, технічні, інформаційні та організаційні аспекти.

Охарактеризуємо окреслені аспекти.

*Методичні* – методики, рекомендації з реалізації підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища з урахуванням дидактичних і психологічних аспектів.

*Програмні* – мережеві системні програми, комп'ютерні навчальні програми, інструментальні середовища для створення навчальних програм підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища. Сьогодні для створення комп'ютерних навчальних програм можна використати програмні середовища, розміщені на різних серверах (WebCT, First Class та ін.).

*Технічні* – персональні електронно-обчислювальні машини для організації сервера, персональні і мережеві комп'ютери.

*Інформаційні* – конспекти лекцій, підручники, та інші методичні матеріали на електронних носіях, довідники, різноманітні бази даних з методичних матеріалів, оперативних даних.

*Організаційні* – нормативні документи, що супроводжують освітній процес бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища.

Ефективність підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища заснована на тому, що самі бакалаври почувають необхідність подальшого навчання, а не піддаються тиску з боку. Вони мають можливість роботи з навчальними матеріалами в такому режимі й обсязі, який підходить безпосередньо їм. Ефект значною мірою залежить від того, наскільки регулярно вони займаються. Послідовне виконання контрольно-діагностичних завдань і випускної роботи, а також підтримка у всіх питаннях з боку викладача-координатора забезпечує планомірне засвоєння знань.

Технологія впровадження конструктивної моделі підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища представлена нижче.

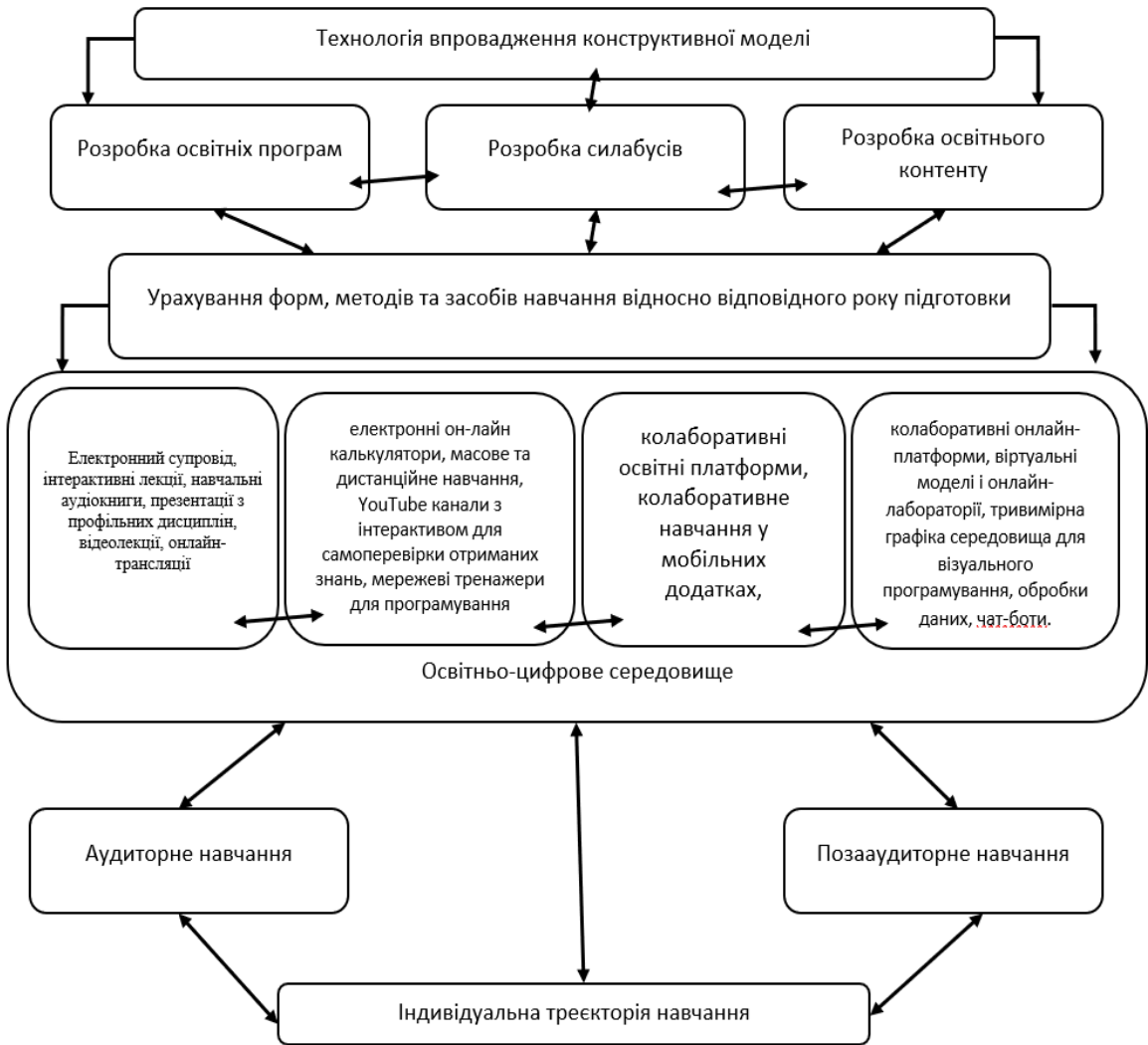


Рис. 1. Технологія впровадження конструктивної моделі підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища

Впровадження конструктивної моделі вимагає розробки освітніх програм, силябусів та освітнього контенту причому в електронному вигляді. При розробці освітніх програм та силябусів, а також освітнього контенту мають бути враховані форми, методи, а також засоби навчання відносно відповідного року підготовки бакалаврів з кібербезпеки.

Переважно на першому курсі підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища використовується електронний супровід, інтерактивні лекції, навчальні аудіокниги, презентації з профільних дисциплін, відеолекції, онлайн-трансляції. На другому курсі підготовки – це електронні онлайн-калькулятори, масове та дистанційне навчання, YouTube канали з інтерактивом для самоперевірки отриманих знань, мережеві тренажери для програмування. На третьому курсі використовуються колаборативні освітні платформи, колаборативне навчання у мобільних додатках. На четвертому – колаборативні

онлайн-платформи, віртуальні моделі і онлайн-лабораторії, тривимірна графіка середовища для візуального програмування, обробки даних, чат-боти.

Робота в освітньо-цифровому середовищі може здійснюватися як в рамках аудиторного навчання, так і позааудиторного навчання. За рахунок такої інтеграції підготовка бакалаврів з кібербезпеки в умовах окресленого середовища можлива за індивідуальною траєкторією навчання.

Розробка навчального курсу для бакалаврів з кібербезпеки в освітньо-цифровому середовищі має врахувати модульну структуру. Кожний модуль має вміщувати теоретичні аспекти, практичні, а також контроль. Вивчення освітнього контенту в процесі підготовки бакалаврів з кібербезпеки в освітню цифровому середовищі має супроводжуватись такими матеріалами, як посилання на зовнішні ресурси, робота із закладками, віртуальні екскурсії, тури та альбоми, а також медіа сховище.

Набуття практичних навичок у цифровому середовищі бакалаврській безпеки може бути здійснено в лабораторних практикумах та ресурсах для самостійного опрацювання, а також дослідницьких проектах. Лабораторні практикуми супроводжуватись методичними рекомендаціями, прикладами щодо виконання тих чи інших завдань, завдання, а також критерії оцінювання. Ресурси для самостійної роботи можуть супроводжуватись також завданнями, відео елементами, математичними формулами, дослідницькими проектами, можуть покладати в основу колаборативне навчання. Сюди можна віднести роботу у команді, веб-конференції, тощо. Контрольний блок кожного з модулів, передбачених для підготовки бакалаврів з кібербезпеки, мають містити критерії оцінювання, контрольні завдання, тести та тренажери, опитувальники та рефлексію.

Для створення освітньо-цифрового середовища використовуються такі ресурси як: веб-сторінка, урок та посилання на файл. У кожний з цих ресурсів необхідно вбудувати навчальні відео фрагменти, які розміщені на відео порталі; зробити посилання на повнотекстові електронні версії навчальних посібників, які містяться в електронній бібліотеці; зробити посилання на наукові матеріали, які містяться в інституційному репозитарії та наукометричних базах даних, до яких університет має доступ; дати посилання на відкриті онлайн-курси та інші веб-ресурси, які стануть додатковим джерелом навчальних матеріалів.

Для створення ресурсів для підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища до лабораторних та самостійних робіт використовуються скрінкасти з прикладами розв'язування завдань, які розміщені на відео порталі; посилання на методичні рекомендації з електронної бібліотеки; сервіси колективної роботи, які можуть забезпечуватись електронні освітні системи навчального закладу або зовнішніми ресурсами. Одним з найбільш важливих компонентів завдань для лабораторних та самостійних робіт бакалаврів з кібербезпеки – є доступ до програмних пакетів для виконання завдань. Такий доступ створюється через забезпечення віртуального робочого місця з повним набором необхідних програм для кожного студента. Таку можливість надає освітньо-цифрове середовище з єдиною точкою входу. Бакалаври з кібербезпеки, відкривши зміст завдання в електронному навчальному курсі, отримують посилання на віртуальний робочий стіл, який відкриває доступ йому до всіх доступних програм, і таким чином студент має змогу виконати завдання. Кожній групі студентів доступні ті пакети програм, які зараз використовуються у навчальному процесі.

Технологія впровадження конструктивної моделі підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища також враховує елементи розробки освітнього курсу. Такий курс має містити повну назву, показується як посилання в списках курсів на головній та інформаційній сторінці і в звітах. Вона може використовуватись і в рядку заголовка браузера, коли цей курс видимий. Адміністратор може визначити, чи має право викладач самостійно змінювати цей параметр. Навчальний курс в освітньо-

цифровому середовищі може містити коротку назва курсу, яка буде показуватися у навігаційному рядку при відкритті даного курсу та в темах електронних листів, які будуть приходити користувачам курсу.

Навчальний курс має враховувати дату початку навчання. Особливо, якщо курс розроблено в тижневому форматі. Ідентифікатор курсу – використовується тільки при зіставленні курсу від зовнішніх систем і не показується ніде на сайті. У переважній більшості випадків це поле залишайте порожнім.

Опис до курсу освітньо-цифрового середовища повинен містити анотацію курсу – резюме курсу відображається в списку курсів. При видачі результатів пошуку курсів резюме курсу додається до назви курсу. Файли, що подаються у курсі мають також містити коротке пояснення.

Формат курсу освітньо-цифрового середовища визначає, як буде виглядати головна сторінка курсу.

- Єдиної діяльності формат – для показу однієї діяльності або ресурсу (наприклад, Тест або SCORM пакет) на сторінці курсу.
- Соціальний формат – на першій сторінці курсу показується форум.
- Тематичний формат – сторінка курсу організовується у вигляді тематичних секцій.
- Тижневий формат – сторінка курсу організовується у вигляді тижневих секцій, де перший тиждень відповідає даті початку курсу.

Модульність курсу освітньо-цифрового середовища – цей параметр визначає, чи буде весь курс показуватися на одній сторінці або розділити на кілька сторінок. Налаштування не впливає на певні формати, такі як формат SCORM.

Журнал оцінок освітньо-цифрового середовища визначає, чи матиме можливість бакалавр з кібербезпеки бачити список всіх своїх оцінок за курс у власному журналі оцінок (через посилання в блоці Керування). Звіти про виконання завдань є для кожного учасника, який проявляє активність на курсі. Вони виглядають як список їх внесків, таких як повідомлення на форумах, виконання завдань, а також включають події доступу. Цей параметр визначає, чи будуть студенти бачити власні звіти про діяльність на сторінці свого профілю.

Максимальний обсяг завантажуваних файлів в освітньо-цифрове середовище визначає максимальний обсяг файлу, який може бути завантажений на курс, обмежений на рівні сайту налаштуваннями встановленими адміністратором. Діяльності також включають налаштування максимального розміру файлу для подальшого обмеження його обсягу.

Також є можливість гостьового доступу освітньо-цифрового середовища – це налаштування визначає, чи може бакалавр з кібербезпеки отримати доступ до курсу у якості гостя без потреби зарахування. Гості повинні будуть вводити пароль кожного разу, коли вони отримують доступ до курсу.

Система освітньо-цифрового середовища також передбачає групову роботу. Це налаштування має три опції:

- Без груп – окремі групи не виділяються, а всі студенти працюють єдиною спільнотою
- Окремі групи – кожен член групи може бачити тільки колег по своїй групі, а решта будуть невидимі
- Видимі групи – кожен член групи може бачити всіх колег по своїй групі, а також бачити інші групи

Тип роботи груп визначається на рівні курсу для всіх діяльностей. Кожна діяльність також підтримує режими групової роботи, але у випадку, коли на рівні курсу вибрано примусовий режим, то в межах активності його змінювати не можна. Якщо тип роботи з групами вибрано примусово, то цей тип буде використовуватися в усіх видах діяльності курсу. Тип груп для кожної діяльності окремо не буде використовуватися.



Переименование роли даёт змогу змінити показ назви ролі в курсі. Зміниться тільки назва ролі – на її права це не вплине. Нова назва ролі буде показуватися на сторінці учасників курсу та скрізь в цьому курсі. Якщо перейменована роль належить до управлінських ролей курсу, то нова її назва буде показуватися як частина в списку курсів.

**Висновки та перспективи подальших досліджень.** Так, технологія впровадження конструктивної моделі підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища закладає основу системний, компетентнісний, соціокультурний, технологічний, особистісно-діяльнісний, кредитно-блоковий, тематичний і лексико-термінологічний підходи. Впровадження конструктивної моделі вимагає розробки освітніх програм силабусів та освітнього контенту причому в електронному вигляді. При розробці освітніх програм та силабусів, а також освітнього контенту мають бути враховані форми, методи, а також засоби навчання відносно відповідного року підготовки бакалаврів з кібербезпеки. Переважно на першому курсі підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища використовується електронний супровід, інтерактивні лекції, навчальні аудіокниги, презентації з профільних дисциплін, відеолекції, онлайн-трансляції. На другому курсі підготовки – це електронні онлайн-калькулятори, масове та дистанційне навчання, YouTube канали з інтерактивом для самоперевірки отриманих знань, мережеві тренажери для програмування. На третьому курсі використовуються колаборативні освітні платформи, колаборативне навчання у мобільних додатках. На четвертому – колаборативні онлайн-платформи, віртуальні моделі і онлайн-лабораторії, тривимірна графіка середовища для візуального програмування, обробки даних, чат-боти. Робота в освітньо-цифровому середовищі може здійснюватися в рамках як аудиторного навчання, так і позааудиторного навчання. За рахунок такої інтеграції підготовка бакалаврів з кібербезпеки в умовах окресленого середовища може здійснюватись за індивідуальною траєкторією навчання. Перспективами подальших розробок є впровадження сучасних онлайн-каналів з інтерактивом для самоперевірки отриманих знань та з використанням електронних онлайн-калькуляторів в систему підготовки фахівців з кібербезпеки та статистична перевірка отриманих результатів.

#### Використані джерела

- [1] О. О. Самойленко, «Конструктивна модель підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища», *Вісник Черкаського національного університету імені Богдана Хмельницького Серія «Педагогічні науки», № 2*, с. 102-106, 2020.
- [2] Б. В. Брайко, *Професійна підготовка магістрів з кібербезпеки в університетах Великої Британії*, Хмельницький, 2020.
- [3] Закон України «Про освіту», 2019. [Електронний ресурс]. Available: <https://zakon.rada.gov.ua/laws/show/2145-19#Text>. [Дата звернення: 20. 07. 2020].
- [4] Законодавство України, «Закон України про вищу освіту» 2014. [Електронний ресурс]. Available: <https://zakon.rada.gov.ua/laws/show/2984-14/ed20020117/find?text=%CF%F0%EE%F4%E5%F1%B3%E9%ED%E0+%EF%B3%E4%E3%EE%F2%EE%E2%EA%E0>. [Дата звернення: 08 08 2019].
- [5] Законодавство України, «Закон України «Про інформацію», 2017. [Електронний ресурс]. Available: <http://zakon2.rada.gov.ua/laws/show/2657-12>. [Дата звернення: 02. 01. 2018].
- [6] Законодавство України, «Закон «Про основні засади забезпечення кібербезпеки України», 2017. [Електронний ресурс]. Available: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>. [Дата звернення: 07. 07. 2020].
- [7] Закон України «Про національну безпеку України», 2020. [Електронний ресурс]. Available: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>. [Дата звернення: 20. 07. 2020].

### Reference

- [1] O. O. Samoilenko, «Konstruktivna model' pi'dgotovki bakalavri'v z ki'berbezpeki v umovakh osvı'tn`o-czifrovogo seredovishha,» Vi'snik Cherkas'kogo naci'onal'nogo uni'versitetu i'meni Bogdana Khmel'nicz'kogo Seri'ya «Pedagogi'chni` nauki», # 2, pp. 102-106, 2020.
- [2] B. V. Brajko, Profesi'jna pi'dgotovka magi'stri'v z ki'berbezpeki v uni'versitetakh Velikoyi Britani`yi, Khmel'nicz'kij, 2020.
- [3] «Zakon Ukrayini «Pro osvı'tu»,» 2019. [Onlajnovij]. Available: <https://zakon.rada.gov.ua/laws/show/2145-19#Text>. [Data zvernennya: 20. 07. 2020].
- [4] Zakonodavstvo Ukrayini, «Zakon Ukrayini pro vishhu osvı'tu»,» 2014. [Onlajnovij]. Available: <https://zakon.rada.gov.ua/laws/show/2984-14/ed20020117/find?text=%CF%F0%EE%F4%E5%F1%B3%E9%ED%E0+%EF%B3%E4%E3%EE%F2%EE%E2%EA%E0>. [Data zvernennya: 08 08 2019].
- [5] Zakonodavstvo Ukrayini, «Zakon Ukrayini «Pro i'nformaczi'yu»,» 2017. [Onlajnovij]. Available: <http://zakon2.rada.gov.ua/laws/show/2657-12>. [Data zvernennya: 02. 01. 2018].
- [6] Zakonodavstvo Ukrayini, «Zakon «Pro osnovni` zasadi zabezpechennya ki'berbezpeki Ukrayini»,» 2017. [Onlajnovij]. Available: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>. [Data zvernennya: 07. 07. 2020].
- [7] «Zakon Ukrayini «Pro naci'onal'nu bezpeku Ukrayini»,» 2020. [Onlajnovij]. Available: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>. [Data zvernennya: 20. 07. 2020].

*Алексей Самойленко, кандидат педагогических наук, доцент, Учебно-научный институт информационной безопасности Службы безопасности Украины, г. Киев, Украина.*

### ТЕХНОЛОГИЯ ВНЕДРЕНИЯ КОНСТРУКТИВНОЙ МОДЕЛИ ПОДГОТОВКИ БАКАЛАВРОВ ПО КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ОБРАЗОВАТЕЛЬНО ЦИФРОВОЙ СРЕДЫ

В статье освещается технология внедрения конструктивной модели подготовки бакалавров по кибербезопасности в условиях образовательно-цифровой среды. Определено, что технология внедрения конструктивной модели закладывает в основу методические (методики, рекомендации по реализации подготовки бакалавров по кибербезопасности в условиях образовательно-цифровой среды с учетом дидактических и психологических аспектов), программные (сетевые системные программы, компьютерные обучающие программы, инструментальные среды для создание учебных программ подготовки бакалавров по кибербезопасности в условиях образовательно-цифровой среды. На основе анализа психолого-педагогической литературы определено, что внедрение конструктивной модели требует разработки образовательных программ силабусив и образовательного контента причем в электронном виде. Доказано, что работа в образовательно-цифровой среде может осуществляться как в рамках аудиторного обучения, так и внеаудиторной обучения. Отмечено, что за счет такой интеграции подготовка бакалавров по кибербезопасности в условиях выраженного среды может осуществляться по индивидуальной траектории обучения.

**Ключевые слова:** технология, конструктивная модель; подготовка бакалавров; бакалавры по кибербезопасности; образовательно-цифровая среда.

*Oleksii Samoilenko, Candidate of Pedagogical Sciences, Associate Professor, Educational and Scientific Institute of Information Security of the Security Service of Ukraine, Kyiv, Ukraine,*

### **TECHNOLOGY OF IMPLEMENTATION OF THE CONSTRUCTIVE MODEL OF PREPARATION OF BACHELORS ON CYBER SECURITY IN THE CONDITIONS OF THE EDUCATIONAL AND DIGITAL ENVIRONMENT**

The article highlights the technology of implementing a constructive model of training bachelors in cybersecurity in an educational and digital environment. It is determined that the technology of implementation of the constructive model is based on methodical (methods, recommendations for the implementation of bachelors in cybersecurity in the educational and digital environment, taking into account didactic and psychological aspects), software. Based on the analysis of psychological and pedagogical literature, it is determined that the implementation of a constructive model requires the development of educational programs of syllabuses and educational content in electronic form. It has been proved that work in the educational and digital environment can be carried out on an individual trajectory of study. It is noted that due to such integration, the training of bachelors in cybersecurity in a defined environment can be carried out on an individual trajectory of study. The digital environment uses resources such as a web page, a tutorial, and a link to a file. In each of these resources it is necessary to embed educational video fragments which are placed on a video portal; make references to full-text electronic versions of textbooks contained in the electronic library; make references to scientific materials contained in the institutional repository and scientometric databases to which the university has access; provide links to open online courses and other web resources that will be an additional source of learning materials. It is noted that to create resources for the preparation of bachelors in cybersecurity in an educational and digital environment for laboratory and independent work, screencasts with examples of problem solving are used, which are posted on the video portal; links to guidelines from the electronic library; teamwork services that can be provided by electronic educational systems of the educational institution or external resources. One of the most important components of tasks for laboratory and independent work of bachelors in cybersecurity is access to software packages for tasks. The system of educational and digital environment also provides for group work. The type of group work is determined at the course level for all activities. Each activity also supports group work modes, but if a forced mode is selected at the course level, it cannot be changed within the activity.

**Keywords:** technology, constructive model; preparation of bachelors; bachelors in cybersecurity; educational and digital environment.