ПЕДАГОГІЧНА АКАДЕМІЯ:
НАУКОВІ ЗАПИСКИ

Інформаційно-комунікаційні технології в освіті

УДК 378.147.88:004.056(430)

DOI https://doi.org/10.5281/zenodo.18837596

Трансформація заочної форми навчання в онлайн-освіту: аналіз сучасних практик німецьких ЗВО у сфері ІТ

Амеліна Світлана Миколаївна

доктор педагогічних наук,

професор кафедри іноземної філології і перекладу

Національний університет біоресурсів і природокористування України

вул. Героїв Оборони, 15, м. Київ, 03041, Україна

ORCID: *0000-0002-6008-3122*

Пилипенко Павло Павлович

аспірант 1-го року навчання

кафедри управління та освітніх технологій

Національний університет біоресурсів і природокористування України

вул. Героїв Оборони, 15, м. Київ, 03041, Україна

Прийнято: 11.02.2026 | Опубліковано: 28.02.2026

Анотація: *У статті здійснено порівняльний аналіз моделей дистанційної підготовки бакалаврів із кібербезпеки у закладах вищої освіти Німеччини у контексті цифровізації заочної форми навчання та зростання попиту на фахівців з захисту інформації. Емпіричну базу становить вибірка бакалаврських програм з кібербезпеки, представлених на німецькому освітньому ринку. Встановлено, що частка дистанційних програм у цій галузі сягає близько 7% від загальної кількості університетів, що відображає обережний підхід Німеччини*

до віртуалізації інженерної підготовки та високі вимоги до якості й верифікації результатів навчання. Метою статті є виявлення організаційно-методичних особливостей дистанційних моделей підготовки та окреслення можливостей адаптації німецького досвіду до умов України. Методологія дослідження спирається на аналіз нормативно-організаційної документації освітніх програм, зіставлення навчальних планів (curricula) та опис моделей за критеріями: співвідношення синхронних/асинхронних компонентів; роль очних фаз і практик; інструменти академічної доброчесності та контролю. Порівняно дві моделі: державна Берлінська вища школа техніки (Berliner Hochschule für Technik, BHT) – програма IT-Sicherheit Online (B.Sc.) та приватна Міжнародна вища школа IU (IU Internationale Hochschule) – програма Cyber Security (B.Sc., Fernstudium). З'ясовано, що довіра до дистанційних кваліфікацій у Німеччині значною мірою підтримується спеціалізованим правовим регулюванням (FernUSG). Виявлено, що модель BHT ґрунтується на змішаному навчанні (blended learning) з фокусом на фундаментальну інженерну підготовку та обов'язкові очні сесії для лабораторних занять і верифікації результатів. Натомість модель IU реалізує концепцію «навчання на вимогу» (education on demand), забезпечуючи високу гнучкість, повну цифровізацію, використання віртуальних лабораторій та інструментів цифрової підтримки. Установлено відмінності у змісті навчання на цих бакалаврських програмах: BHT формує профіль інженера-дослідника, тоді як IU орієнтується на підготовку практико-спрямованих фахівців з акцентом на сучасні інструменти та модульні спеціалізації. За результатами дослідження розроблено комплекс рекомендацій для вітчизняної системи освіти, що передбачає: ініціювання мережевої взаємодії ЗВО через створення консорціумів для оптимізації розробки цифрових ресурсів; інтеграцію принципів адаптивності та модульності у систему післядипломної підготовки; а також удосконалення нормативно-правових

 ISSN: 2786-9458

механізмів сертифікації та моніторингу якості дистанційних освітніх продуктів.

***Ключові слова**: дистанційна освіта, кібербезпека, професійна підготовка, вища освіта Німеччини, BHT, IU, змішане навчання.*

Transforming Part-Time Study into Online Delivery: German Cybersecurity Bachelor Program Models

Svitlana Amelina

Doctor of Pedagogical Sciences, Professor, Professor of the Department of Foreign Philology and Translation,

National University of Life and Environmental Sciences of Ukraine

15 Heroiv Oborony St., Kyiv, 03041, Ukraine

ORCID: https://orcid.org/0000-0002-6008-3122

E-mail: svetlanaamelina@ukr.net

Pavlo Pylypenko

First-year PhD student, Department of Management and Educational Technologies,

National University of Life and Environmental Sciences of Ukraine

15 Heroiv Oborony St., Kyiv, 03041, Ukraine

***Abstract:** The article presents a comparative analysis of distance-based bachelor training models in cybersecurity at German higher education institutions (HEIs) in the context of the digital transformation of part-time study formats and the growing demand for information security specialists. The study aims to identify the organizational and methodological features of digital delivery models in cybersecurity education and to outline the possibilities for adapting German practices to the Ukrainian higher education system. The empirical basis comprises a sample of*

bachelor-level cybersecurity programmes available on the German higher education market. The research methodology includes an analysis of regulatory and organizational documents, a comparison of curricula, and model descriptions based on the following criteria: the ratio of synchronous and asynchronous components; the role of in-person phases and workshops; and the tools for academic integrity and assessment control. Two institutional models are compared: the public Berliner Hochschule für Technik (BHT) – the IT-Sicherheit Online (B.Sc.) programme, and the private IU Internationale Hochschule – the Cyber Security (B.Sc., Fernstudium) programme. The study reveals that the proportion of distance-based programmes in this field remains limited (approx. 7% of the total offerings), reflecting Germany's cautious approach to the virtualization of engineering training and its emphasis on quality assurance. It is established that trust in distance qualifications in Germany is significantly supported by specialized legal regulation (FernUSG). The BHT model is based on blended learning and emphasizes fundamental engineering training with mandatory in-person sessions for laboratory work. In contrast, the IU model implements an "education-on-demand" approach characterized by high flexibility, full digitalization, virtual laboratories, and digital learner support instruments. Substantial differences in programme content are identified: BHT shapes the profile of an engineer-researcher, whereas IU is oriented toward practice-oriented specialists with modular specializations. The findings inform recommendations for the Ukrainian education system, including: initiating network cooperation among HEIs through consortia; integrating adaptability and modularity into postgraduate training; and improving regulatory mechanisms for the certification and quality monitoring of distance educational products.

Keywords: *cybersecurity programmes; digital delivery models; blended learning; virtual laboratories; FernUSG; curriculum comparison; academic integrity; quality assurance/*

Постановка проблеми. В умовах глобальної цифровізації та повоєнної відбудови України модернізація форм навчання, особливо у сфері IT та кібербезпеки, стає критично важливим завданням. Традиційна заочна форма («настановча сесія – самостійне опрацювання – іспит») сьогодні демонструє неефективність у формуванні інженерних «hard skills», що вимагає переходу до повноцінної дистанційної онлайн-освіти (online distance learning) з використанням віртуальних лабораторій та адаптивних систем. Цей тренд є загальносвітовим: наприклад, у Бразилії кількість студентів, що вчаться дистанційно, зросла майже в 9 разів [11], у Туреччині майже 50% здобувачів навчаються дистанційно [26]. Потрібно зауважити, що у Європі таке навчання набуло широкої інституціоналізації [15, с. 7]. Вагому роль у цьому процесі відіграють «мегауніверситети» з контингентом більше 100 000 осіб [10, с. 8]. В Україні генеза дистанційної освіти триває з 2002 р., коли експеримент МОН заклав підґрунтя для процесу її нормативної регламентації.

Винятковий інтерес для модернізації вітчизняної системи становить досвід Німеччини, де успішно співіснують державні консорціуми (VFH/BHT) та приватні платформи (IU Internationale Hochschule).

Інституційне оформлення німецької дистанційної освіти (Fernstudium) відбулося ще в середині 1970-х рр. із заснуванням Гаґенського заочного університету (FernUniversität in Hagen) та ухваленням Закону про захист учасників дистанційного навчання (FernUSG) [16]. Згідно з цим законом, дистанційне навчання визначається сукупністю трьох ознак: систематичне передавання знань, просторова роз’єднаність та моніторинг результатів [16]. Сучасна німецька модель поєднує університетські програми та регульовані державою курси, забезпечуючи високу якість інженерної підготовки.

Специфіку професійної підготовки у Німеччині досліджували С. Амеліна [1], О. Пилипенко [4]. Фундаментальні аспекти розвитку відкритої та дистанційної освіти, а також перехід від традиційної заочної форми до e-learning

ґрунтовно висвітлено у працях таких вітчизняних вчених, як В. Биков [2], В. Кухаренко [3]. Проте німецький досвід саме онлайн-підготовки інженерних кадрів залишається висвітленим фрагментарно.

Дослідження сучасного стану підготовки фахівців з кібербезпеки свідчить про перехід від суто технічного навчання до комплексних міждисциплінарних стратегій. Важливим внеском у цьому напрямі є робота Е. Собєскі та співавторів [24], які обґрунтовують багаторівневий та мультидисциплінарний підхід до кіберосвіти. Автори наголошують, що кібербезпека вимагає інтеграції знань з управління, права та етики, що корелює з концепцією «T-shaped фахівця».

Проблема оцінки ефективності таких програм та їх відповідності ринку праці детально розглянута у праці К. Сахарінена, Я. Баклунда та Я. Невали (K. Saharinen, J. Backlund, J. Nevala). Дослідники здійснили кількісний аналіз європейських та американських освітніх програм, використовуючи рамку NICE (National Initiative for Cybersecurity Education) як еталон для порівняння. Це підтверджує актуальність вашого аналізу щодо необхідності трансформації заочних моделей у гнучкі онлайн-платформи, які здатні оперативно заповнювати ці прогалини [23].

Методологічний аспект покращення якості навчання через практичну діяльність розкривається в роботі А. Карінсало (A. Karinsalo), який пропонує педагогічний підхід до кібервправ. Такий підхід дозволяє студентам не лише відпрацьовувати «hard skills», а й аналізувати власну стратегію прийняття рішень, що є критично важливим для підготовки кадрів у сфері захисту критичної інфраструктури [20].

Аналіз публікацій за останні роки засвідчує фокус дослідників на проблемі розриву між академічною підготовкою та реальними потребами індустрії кібербезпеки. Б. Блажіч обґрунтовує необхідність переходу до міждисциплінарності для забезпечення кадрів [8]. Проблематика синхронізації навчальних планів з кібербезпеки з потребами індустрії розкрита у працях

Г. Тохіді та Дж. Прідмора [25], Дж. Еквіста [13]. У методичному аспекті А. Аламмарі [5] пропонує модель компетентностей у логіці KSA (knowledge–skills–abilities), а Дж. Катал [9] і А. Надім [22] наголошують на інтеграції безпекових концепцій як наскрізних елементів.

Мета статті. Метою роботи є аналіз сучасних моделей дистанційної підготовки бакалаврів з кібербезпеки в Німеччині (на прикладі державної та приватної моделей) та визначення шляхів адаптації цих практик для трансформації заочної форми навчання в Україні.

Виклад основного матеріалу дослідження. Для визначення специфіки впровадження дистанційних технологій на бакалаврських програмах з кібербезпеки було здійснено цільовий відбір акредитованих освітніх пропозицій німецьких ЗВО. До вибірки увійшли виключно програми ступеня бакалавра наук, що спеціалізуються на інформаційній та кібербезпеці й реалізуються у форматі Fernstudium або Online-Studium.

Аналіз освітнього ландшафту Німеччини свідчить, що загальна кількість бакалаврських програм за профілем «Кібербезпека» (Cyber Security / IT-Sicherheit) варіюється в межах 38–45. Ця варіативність зумовлена включенням до статистики вузькопрофільних спеціалізацій, таких як цифрова форензика (Allgemeine und Digitale Forensik), розслідування кіберзлочинів (IT-Forensik/Cybercrime) та управління ризиками безпеки (Risiko- und Sicherheitsmanagement). Серед провідних закладів, що реалізують такі програми у традиційному або дуальному форматах, можна виділити Дуальну вищу школу Баден-Вюртемберга (DHBW Mannheim) [12] та Вищу школу прикладних наук малого та середнього бізнесу (FHM) [14].

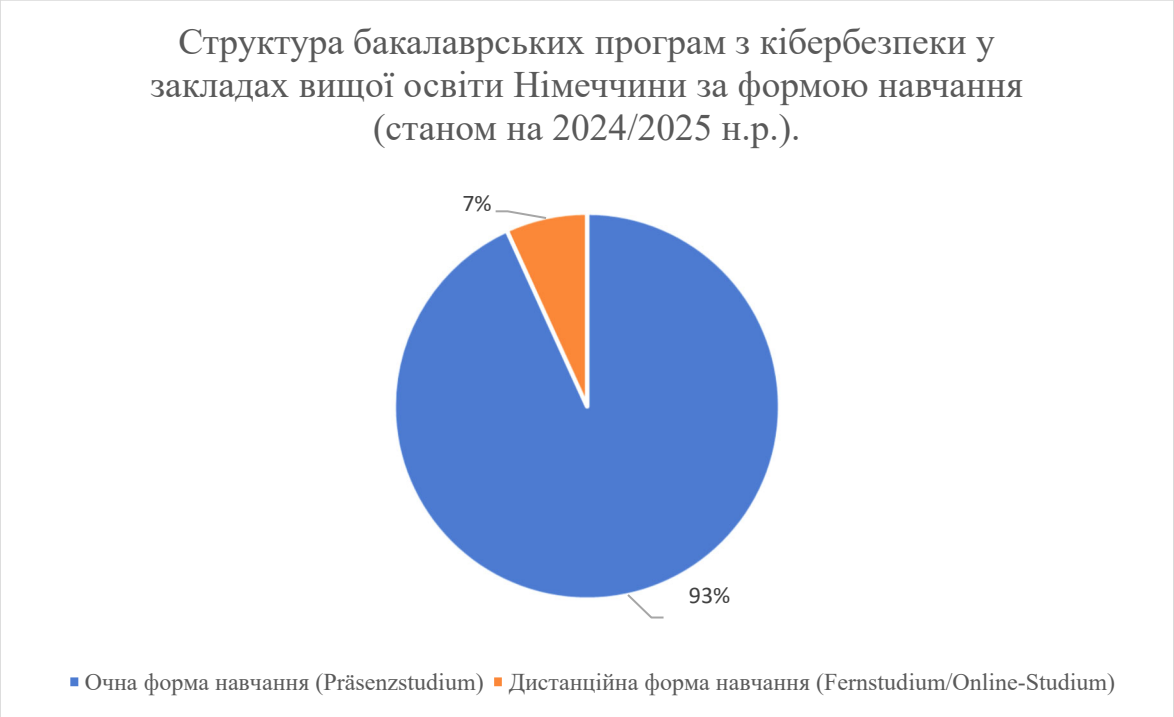
Окремий сегмент становить підготовка у форматі повного дистанційного навчання (Fernstudium), що є предметом нашого дослідження. Цей формат пропонують як приватні, так і державні заклади, зокрема: Міжнародна вища школа IU (програма B.Sc. Cyber Security), Вища школа ім. Вільгельма Бюхнера

 ISSN: 2786-9458

(програма B.Sc. IT-Sicherheit) та державна Берлінська вища школа техніки (програма B.Sc. IT-Sicherheit Online).

Згідно з даними дослідження, представленого на рис. 1, ринок бакалаврських програм з кібербезпеки в Німеччині залишається переважно орієнтованим на очний формат (93%). Частка дистанційних програм (7%) є незначною у кількісному вимірі та репрезентує найбільш інноваційний сегмент освітніх послуг.

Рис. 1. Структура бакалаврських програм з кібербезпеки у закладах вищої освіти Німеччини за формою навчання (станом на 2024/2025 н.р.)



Бакалаврська програма «IT-безпека онлайн» (IT-Sicherheit online) реалізується Берлінською вищою школою техніки (Berliner Hochschule für Technik, BHT) міжуніверситетського консорціуму «Віртуальна фахова школа» (Virtuelle Fachhochschule, VFH) [17]. До цього об'єднання входять також технічні вищі школи Любека, Бранденбурга, Бремергафена, Емдена/Лера, Кіля, Альбштадт-Зігмарінгена, Яде, Остфалія та Франкфуртський університет прикладних наук. Функціонування VFH базується на моделі «shared economy»

(спільного використання ресурсів). Замість автономної розробки всіх дисциплін університети розподіляють виробничі функції (наприклад, один ЗВО розробляє модуль Kryptographie, інший – Rechnernetze), що забезпечує економічну ефективність та єдність академічних стандартів на спільній платформі. Нормативною основою реалізації цієї бакалаврської програми виступає «Положення про навчання та іспити» (Studien- und Prüfungsordnung), узгоджене з рамковими регламентами BHT та VFH (Rahmenstudien- und -prüfungsordnung) [7].

Бакалаврська програма «IT-безпека онлайн» (IT-Sicherheit online) від Берлінської вищої школи техніки (Berliner Hochschule für Technik, BHT) має нормативний строк 6 семестрів (180 кредитів ECTS) із фіксованим річним набором, що задає чітку «академічну рамку», відмінну від «потокових» моделей приватних ЗВО. Формат навчання є гібридним: понад 80% часу відводиться на дистанційне опрацювання, а для забезпечення прикладної якості передбачено «фази присутності» (Präsenzphasen) – мінімум чотири очні зустрічі на семестр (формат «довгих вікендів») або вебконференції (Web-Konferenz) [6].

Структура університетської програми реалізує модель підготовки «T-shaped фахівця», що передбачає поступову еволюцію від загальних фундаментальних знань до глибокої спеціалізації. На початковому етапі, який охоплює перші два семестри, студенти опановують базовий блок Computer Science. До нього входять такі дисципліни, як «Комп'ютерна архітектура та операційні системи», «Теоретична інформатика» та «Основи математики». Важливим елементом ранньої професіоналізації виступає модуль «Цифровий захист», який вводиться вже на старті навчання. Наступним етапом є засвоєння професійно-орієнтованого блоку Core Security, спрямованого на формування технічних навичок (Hard Skills). Цей процес реалізується через дворівневе вивчення криптографії (основи та прикладний рівень), поглиблення у мережеву безпеку, а також вивчення інженерії захисту, що включає розробку безпечних

програмних систем, IT-форензику та апаратну безпеку. Важливою складовою підготовки є гуманітарно-управлінський блок, що забезпечує інтеграцію «м'яких навичок» (Soft Skills) та правових аспектів. Студенти вивчають комунікацію, лідерство, самоменеджмент, англійську мову для IT-фахівців, IT-право та економіку підприємства. Особливої уваги заслуговує унікальний модуль «Етика в IT-безпеці», який формує ціннісні орієнтири майбутнього фахівця. Практична підготовка та індивідуалізація освітньої траєкторії зосереджені переважно у п'ятому семестрі. На цьому етапі передбачено виконання обов'язкового практичного проєкту (Praxisprojekt) обсягом 15 кредитів ECTS. Паралельно студенти обирають дисципліни з блоку вільного вибору (Wahlpflichtmodule, 20 ECTS), що дозволяє опанувати трендові напрями, такі як хмарні обчислення, етичний хакінг або безпека автомобільних систем.

Оцінювання знань студентів на бакалаврській програмі «IT-безпека онлайн» (IT-Sicherheit online) від Берлінської вищої школи техніки (Berliner Hochschule für Technik, BHT) характеризується комплексним підходом. До підсумкових іспитів студенти мають виконати низку попередніх робіт, які мають екзаменаційне значення (Prüfungsrelevante Vorleistungen). До таких форм активності належать домашні завдання (Einsendeaufgabe), групова робота в онлайн-форматі та безпосередня участь у контактних сесіях. Фіналізація навчання відбувається у шостому семестрі шляхом написання та захисту бакалаврської роботи. Висока якість освітнього контенту гарантується на рівні консорціуму: фаховий комітет VFH з IT-безпеки (FAITS) систематично аналізує результати опитувань здобувачів та верифікує методичне забезпечення програми.

Програма «Cyber Security» (B.Sc.) в IU Internationale Hochschule реалізується у форматі дистанційного навчання (Fernstudium), що базується на концепції «Education on Demand». Загальний обсяг програми складає 180 кредитів ECTS, нормативний термін навчання – 6 семестрів (36 місяців). Завдяки

високій гнучкості студенти можуть обирати варіативні моделі часової інтенсивності (Full-time, Part-time I, Part-time II), розтягуючи процес до 48 або 72 місяців без зміни змісту. Важливою особливістю є двомовність програми (доступна англійською та німецькою мовами), а також модульний принцип побудови, де стандартний модуль оцінюється у 5 ECTS. Фіналізація навчання відбувається через написання бакалаврської роботи (Bachelor Thesis, 10 ECTS).

Навчальний план (Curriculum) програми «Cyber Security» (B.Sc.) в IU Internationale Hochschule відрізняється від класичних інженерних програм впровадженням принципу раннього занурення (Early Exposure) та компетентнісного підходу (Competence-Based Learning) [18]. Блок фундаментально-професійної бази (1–2 семестри) вирізняється інтегрованим підходом: замість послідовного вивчення загальної теорії, програма передбачає одночасне опанування спеціалізації та прикладного інструментарію. Студенти вивчають програмування (Introduction to Programming with Python, Object-oriented Programming with Java) та математичний мінімум (Mathematics: Analysis, Statistics). Вже у першому семестрі викладаються спеціалізовані дисципліни: Introduction to Data Protection and IT Security та System Pentesting Basics, що дозволяє виконувати завдання з етичного хакінгу на ранніх етапах. Технологічне ядро (3–4 семестри) формує профіль фахівця, інтегрованого в процеси розробки (Shift Left Security). Ключовими дисциплінами є DevSecOps and Common Software Weaknesses, Cryptography, Host and Software Forensics, а також інфраструктурні модулі (Operating Systems, Introduction to the Internet of Things).

У 4–5 семестрах програма посилює прикладну складову через інтеграцію управлінського та правового компонентів: обов'язкові дисципліни IT Project Management і IT Service Management доповнюються модулем IT Law з акцентом на регуляторні вимоги, зокрема GDPR, що сприяє підготовці випускників до діяльності в бізнес-середовищі. Технологічна актуальність забезпечується курсами Cloud Computing та Artificial Intelligence. Гнучкість траєкторії

забезпечується блоком вибіркових дисциплін (Electives A, B, C) обсягом 30 ECTS (5–6 семестри). Студент обирає спеціалізацію за векторами: Advanced Cyber Security: Cyber Threat Intelligence, Secure Coding, Social Engineering. Future Tech: Blockchain and Quantum Computing, Machine Learning. Business & Management: Leadership 4.0, бізнес-аналітика [19].

Критично важливим елементом системи забезпечення якості освіти в IU є стратегічна відмова від домінування тестових методик на користь альтернативних форм контролю, що регламентуються положенням «General Examination Regulations» [21]. Університет впроваджує формат робочого зошита (Workbook), який передбачає поетапне виконання практичних завдань безпосередньо протягом вивчення модуля. Для оцінки аналітичних компетентностей широко застосовується метод ситуаційних вправ (Case Study). Вагоме місце у структурі оцінювання посідає проєктна робота (Project Work), сутність якої полягає у самостійній розробці та документуванні комплексних технічних рішень, як це реалізовано, наприклад, у курсі з хмарних обчислень. Окрім письмових робіт, навчальний план передбачає усні презентації (Oral Assignment) у форматі відеоконференцій, що дозволяє викладачам верифікувати комунікативні навички здобувача та пересвідчитися в автентичності його знань. Що стосується класичних іспитів, то вони проводяться у повністю дистанційному форматі із залученням технологій прокторингу, які гарантують дотримання принципів академічної доброчесності навіть за відсутності фізичної присутності студента в кампусі.

Потрібно зазначити, що у ВНТ (державний сектор університетської освіти) діє жорсткий Numerus Clausus (NC) – конкурсний відбір за середнім балом атестата. Це зумовлено обмеженою пропускною здатністю фінансованої державою системи та фізичним лімітом місць під час обов'язкових очних занять. Такий підхід формує «вхідний фільтр» ще до початку навчання: абітурієнти з нижчим балом змушені або відмовлятися від вступу, або накопичувати так звані

«семестри очікування» (Wartesemester). Додатковим селективним фактором є мовні вимоги: програма викладається німецькою мовою, що вимагає підтвердження рівня C1 (DSH-2 або TestDaF), обмежуючи доступ для іноземних вступників. Натомість в IU (приватний університет) політика «NC-frei» робить вступ максимально доступним. Цифрова модель дозволяє масштабувати набір без жорстких лімітів, а наявність англомовного треку усуває мовні перешкоди. Втім, відсутність адміністративних бар'єрів компенсується іншими чинниками: вартість навчання (від 12 000 євро за курс) стає головним регулятором доступу. Селекція зміщується на етап навчання, де студенти, нездатні до самоорганізації в дистанційному форматі, відсіюються природним шляхом. Крім того, IU активно застосовує механізм вступу без атестата (Abitur) для осіб з професійним досвідом, що реалізує принцип навчання протягом усього життя Lifelong Learning.

Для наочності відмінності між проаналізованими моделями зведено у таблицю 1 (див. Табл.1):

Таблиця 1

Порівняльна характеристика організаційно-методичних засад бакалаврських програм з кібербезпеки в BHT та IU Internationale Hochschule

Критерій порівняння	**Berliner Hochschule für Technik (BHT)**	**IU Internationale Hochschule (IU)**
Тип установи	Державний заклад	Приватний заклад
Формат доступу	Фіксований початок (семестровий), є NC (обмеження на вступ до університету через фіксовану кількість навчальних місць)	Вступ на протязі року (365 днів на рік), без NC
Ступінь віртуалізації	Гібридний (онлайн + обов'язкові візити) 4 очні заняття на семестр (п'ятниця-субота)	100% онлайн (включно з іспитами

ISSN: 2786-9458

Фокус програми	Академічна база + прикладна інженерія	Вузькоспеціалізоване навчання
Вартість	570 €– передплата за медіа за семестр	36 місяців навчання –379 євро на місяць, 48 місяців – 329 євро на місяць, 72 місяці – 249 євро на місяць

Джерело: власна розробка автора

Дослідження виявило концептуальні розбіжності у підходах до формування професійних компетентностей. Модель навчання у BHT реалізує класичний дедуктивний підхід («від теорії до практики»), де перші три семестри присвячено фундаментальній базі (вища математика, фізика, C/C++), а спеціалізація відтермінована до четвертого семестру. Натомість модель IU сповідує принцип «Early Exposure» (раннього занурення у професію): профільні модулі з захисту даних вводяться вже у першому семестрі паралельно з вивченням Python – індустріального стандарту скриптингу, що сприяє швидкій професіоналізації та мотивації студентів.

Відмінності у навчальних планах формують різні кваліфікаційні траєкторії. Акцент BHT на низькорівневій архітектурі та математичній криптографії спрямований на підготовку системних архітекторів та інженерів-дослідників. Програма IU, інтегруючи управлінський та правовий блоки (IT Service Management, IT Law), готує DevSecOps-фахівців для корпоративного сектору, здатних вбудовувати безпеку в бізнес-процеси. Методологія контролю якості також відображає різний баланс між безпекою та гнучкістю. BHT дотримується підходу «верифікації знань» через очні письмові іспити (Klausuren), що гарантує високу академічну доброчесність, але обмежує мобільність. IU реалізує компетентнісний підхід («демонстрація навичок»), широко застосовуючи асинхронні форми оцінювання (Workbook, Case Studies, проєкти) та онлайн-іспити з прокторингом, що забезпечує гнучкість дистанційного навчання без втрати якості контролю.

Висновки. Німецький досвід демонструє ефективне співіснування двох відмінних парадигм цифрової освіти. Державна модель (BHT) зберігає академічний консерватизм, базуючись на гібридному форматі (Blended Learning) та жорсткій селекції вступників (Numerus Clausus), що забезпечує підготовку фундаментальних інженерів-дослідників. Приватна модель (IU) реалізує гнучку концепцію «освіти за вимогою» (Education on Demand), орієнтовану на швидку професіоналізацію та підготовку практиків (DevSecOps) без адміністративних бар'єрів на вході (NC-frei). Порівняльний аналіз виявив зміну педагогічного дизайну від дедуктивного підходу в державному секторі (спочатку теорія, потім практика) до індуктивного принципу Early Exposure у приватному (раннє занурення у спеціальність). Це доводить, що для IT-спеціальностей ефективними є обидві траєкторії, проте вони задовольняють різні сегменти ринку праці. Враховуючи виклики воєнного стану та необхідність повоєнної цифрової відбудови, імплементація німецького досвіду в освітній простір України є доцільною за такими напрямами: створення університетських консорціумів, нормативна реформа дистанційної освіти, впровадження віртуальних полігонів (Cyber Ranges). В умовах обмеженого доступу до фізичних лабораторій критично важливим є перехід до хмарних середовищ для відпрацювання навичок (за прикладом віртуальних лабораторій IU). Це дозволить студентам з будь-якої точки світу отримувати практичний досвід налаштування мереж та захисту інфраструктури.

Список використаних джерел

1. Амеліна С., Тарасенко Р. Дуальна форма навчання: досвід німецьких закладів вищої освіти. *Humanitarian Studios: Pedagogics, Psychology, Philosophy*. 2024. Вип. 15, № 2. С. 8–14.

2. Биков В. Відкрита освіта: організаційно-педагогічні засади : монографія. Київ : Атіка, 2012. 684 с.

3. Кухаренко В., Березенська С., Бугайчук К. Теорія та практика змішаного навчання / за ред. В. Кухаренка. Харків : Міськдрук, 2016. 284 с.

4. Пилипенко О. Професійна підготовка фахівців ветеринарного профілю у вищих навчальних закладах Німеччини : автореф. дис. … канд. пед. наук. Київ : Нац. ун-т біоресурсів і природокористування України, 2018. 23 с.

5. Alammari A., Sohaib O., Younes S. Developing and evaluating cybersecurity competencies for students in computing programs. *PeerJ Computer Science*. 2022. Vol. 8. P. e827–e828.

6. Berliner Hochschule für Technik (BHT). IT-Sicherheit (Online), Bachelor (B.Sc.). URL: https://studiengang.bht-berlin.de/it-sicherheit (дата звернення: 21.01.2026).

7. Beuth-Hochschule für Technik Berlin. Studien- und Prüfungsordnung für den Bachelorstudiengang IT-Sicherheit online (IT Security online) des Fachbereichs VI der Beuth-Hochschule für Technik Berlin. *Amtliche Mitteilung*. 2021. Jahrg. 42, Nr. 12. P. 1–11.

8. Blazic B. Changing the landscape of cybersecurity education in the EU: will the new approach produce the required cybersecurity skills? *Education and Information Technologies*. 2022. Vol. 27. P. 3011–3036.

9. Catal C., Ozcan A., Donmez E., Kasif A. Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies*. 2023. Vol. 28. P. 1809–1831.

10. Daniels J. *Mega-universities and knowledge media*. London : Kogan Page, 1996. 212 p.

11. de Oliveira Neto J., dos Santos E. Analysis of the methods and research topics in a sample of the Brazilian distance education publications, 1992 to 2007. *American Journal of Distance Education*. 2010. Vol. 24, No. 3. P. 119–134.

12. Duale Hochschule Baden-Württemberg (DHBW). Ravensburg. Studienangebot Bachelor: Informatik. URL:

https://www.ravensburg.dhbw.de/studienangebot/bachelor-studiengaenge/informatik (дата звернення: 21.01.2026).

13. Ekqvist J., Kämppi P., Rajamäki J. Cybersecurity education in Finnish universities of applied sciences: Workforce alignment. *Proceedings of the 24th European Conference on Cyber Warfare and Security (ECCWS 2025)*. 2025. P. 735–744.

14. Fachhochschule des Mittelstands (FHM). Cyber / Computer Security (B.Sc.), Vollzeit. URL: https://www.fh-mittelstand.de/studiengang/cyber-computer-security/vollzeit/ (дата звернення: 21.01.2026).

15. Gaebel M., Kupriyanova V., Morais R., Colucci E. *E-learning in European higher education institutions*. Belgium : European University Association, 2014. 92 p.

16. Gesetz zum Schutz der Teilnehmer am Fernunterricht (FernUSG). 1976. URL: https://www.gesetze-im-internet.de/fernusg/ (дата звернення: 22.01.2026).

17. Hochschulverbund VFH. Hochschulen im VFH-Verbund: Ein starkes Netzwerk für Online-Studium, Weiterbildung und Innovation. URL: https://www.vfh.de/hochschulen-im-vfh-verbund/ (дата звернення: 22.01.2026).

18. IU Internationale Hochschule. Cyber Security (Bachelor): сторінка програми. URL: https://www.iu.de/bachelor/cyber-security/ (дата звернення: 21.01.2026).

19. IU Internationale Hochschule. Cyber Security (Fernstudium), 180 ECTS (EN). URL: https://www.iu.de/bachelor/cyber-security/fernstudium/180-ects-en/ (дата звернення: 21.01.2026).

20. Karinsalo A., Saharinen K., Päijänen J., Salonen J. Pedagogical and Self-Reflecting Approach to Improving the Learning Within a Cyber Exercise. *Proceedings of the 20th European Conference on Cyber Warfare and Security (ECCWS 2021)*. 2021. Vol. 21, No. 1. P. 105–114.

21. *Modulhandbuch Bachelor of Science: Bachelor Cyber Security (FS-BACSD-01): Fernstudium*. Erfurt : IU Internationale Hochschule, 2025. 24 p.

22. Nadeem A. Cybersecurity as a crosscutting concept across an undergrad computer science curriculum: An experience report. *Proceedings of the 55th ACM Technical Symposium on Computer Science Education*. 2024. Vol. 1. P. 916–922.

23. Saharinen K., Backlund J., Nevala J. Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework. *ICETC ’20: Proceedings of the 12th International Conference on Education Technology and Computers*. 2020. P. 170–176.

24. Sobiesk E., Blair J., Conti G., Lanham M., Taylor H. Cyber Education: A Multi-Level, Multi-Discipline Approach. *SIGITE ’15: 16th Annual Conference on Information Technology Education*. Chicago, IL, 2015. P. 43–47.

25. Towhidi G., Pridmore J. Aligning cybersecurity in higher education with industry needs. *Journal of Information Systems Education*. 2023. Vol. 34, No. 1. P. 70–83.

26. Zawacki-Richter O., Kondakci Y., Bedenlier S., Alturki U., Aldraiweesh A., Püplichhuysen D. The development of distance education systems in Turkey, the Russian Federation and Saudi Arabia. *European Journal of Open, Distance and E-Learning*. 2015. Vol. 18, No. 2. P. 113–128.