



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ БІОТЕХНОЛОГІЧНИЙ
УНІВЕРСИТЕТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»

РІВЕНЬ ВИЩОЇ ОСВІТИ: Перший (бакалаврський)

СТУПІНЬ ВИЩОЇ ОСВІТИ: Бакалавр

СПЕЦІАЛЬНІСТЬ: F5 “Кібербезпека та захист інформації”

ГАЛУЗЬ ЗНАНЬ: F Інформаційні технології

ОСВІТНЯ КВАЛІФІКАЦІЯ: Бакалавр з кібербезпеки та захисту інформації

РІК ВСТУПУ: 2025

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Державного біотехнологічного
університету
Голова вченої ради

_____/_____
(протокол № __ від « » квітня 2025 р.)
та вводиться в дію з «01» вересня 2025 р.

Харків – 2025

ПЕРЕДМОВА

Освітньо-професійна програма (ОПП) для підготовки здобувачів вищої освіти першого (бакалаврського) рівня за спеціальністю F5 Кібербезпека та захист інформації містить обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти; перелік компетентностей випускника; нормативний зміст підготовки здобувачів вищої освіти, сформульований в термінах результатів навчання; форми атестації здобувачів вищої освіти; вимоги до наявності системи внутрішнього забезпечення якості вищої освіти.

Розроблено проектною групою у складі:

- 1. Піскачова Ірина Вікторівна**, кандидат технічних наук, доцент кафедри автоматизації та комп'ютерно-інтегрованих технологій.
- 2. Левкін Артур Володимирович**, кандидат технічних наук, доцент кафедри інформаційних технологій, кібернетики та захисту інформації.
- 3. Дьоміна Вікторія Михайлівна**, кандидат технічних наук, доцент кафедри інформаційних технологій, кібернетики та захисту інформації.
- 4. Чалий Ігор Вільович**, кандидат технічних наук, доцент кафедри інформаційних технологій, кібернетики та захисту інформації.

- Освітньо-професійна програма «**Кібербезпека та захист інформації**» підготовки фахівців першого (бакалаврського) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації розроблена відповідно до Закону України «Про вищу освіту» від 01.07.2014 р., Постанов Кабінету Міністрів України від 23.11.2011 р. «Про затвердження Національної рамки кваліфікацій» від 30.12.2015 р. № 1187, «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30.12.2015 р., методичних рекомендацій «Розроблення освітніх програм. Методичні рекомендації» (2014 р.), наказом Міністерства освіти і науки України «Про затвердження стандарту вищої освіти за спеціальністю F5 Кібербезпека та захист інформації для першого (бакалаврського) рівня вищої освіти від 04 жовтня 2018 року № 1074, з урахуванням змін у Стандарті вищої освіти зі спеціальності F5 Кібербезпека та захист інформації (наказ Міністерства освіти і науки України від 13.01.2022 р. №26), Наказ № 842 від 13.06.2024 "Про внесення змін до деяких стандартів вищої освіти", наказ Міністерства освіти і науки України від 29.10.2024 р. №1547), та відповідно до змін до Закону України «Про військовий обов'язок і військову службу», від 15 січня 2025 року.

1. Профіль освітньо-професійної програми «Кібербезпека та захист інформації» зі спеціальності

F5 Кібербезпека та захист інформації

1 - Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Державний біотехнологічний університет Факультет кіберпорт, кафедра інформаційних технологій, кібернетики та захисту інформації.
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр, бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Кібербезпека та захист інформації
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	Ліцензується вперше.
Цикл/рівень	Перший (бакалаврський) рівень FQ-ЕНЕА – перший цикл, EQF LLL – 6 рівень, НРК – 6 рівень / Бакалавр
Передумови	Умови вступу визначаються «Правилами прийому до Державного біотехнологічного університету», затвердженими Вченою радою. Наявність повної загальної середньої освіти. Підготовка фахівців з кібербезпеки проводиться за денною і заочною формами навчання
Мова(и) викладання	Українська
Термін дії освітньої Програми	Термін дії освітньо-професійної програми «Кібербезпека та захист інформації» до 2027 року.
Інтернет-адреса постійного розміщення опису освітньої програми	http://btu.kharkov.ua/
2 - Мета освітньо-професійної програми	
Метою освітньо-професійної програми є формування у майбутнього фахівця здатності поєднувати знання, практичні навички, майстерність та інноваційність з відповідальністю під час вирішення проблем інформаційної безпеки в умовах швидкозмінного, багатофункціонального середовища; забезпечення теоретичної та практичної підготовки європейського рівня з метою задоволення ціннісних очікувань стейкхолдерів (зацікавлених сторін) в галузі кібербезпеки; виховання на загальнолюдських цінностях духовно збагаченої, національно свідомої, конкурентоздатної особистості, здатної до творчого розвитку в процесі розв'язання складних спеціалізованих задач із захисту інформації.	
3 - Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань F Інформаційні технології Спеціальність F5 Кібербезпека та захист інформації. Об'єкти професійної діяльності випускників: - об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; - технології забезпечення безпеки інформації; - процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту.

	Об'єкти вивчення: — технології кбербезпеки та захисту інформації; — процеси управління кбербезпекою та захистом інформації; — об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кбербезпеки та захисту інформації. Теоретичний зміст предметної області. Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Знання: - законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; - принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; - теорії, моделей та принципів управління доступом до інформаційних ресурсів; - теорії систем управління інформаційною та/або кібербезпекою; - методів та засобів виявлення, управління та ідентифікації ризиків; - методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; - методів та засобів технічного та криптографічного захисту інформації; - сучасних інформаційно-комунікаційних технологій; - сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій. Методи, методики та технології: методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки. Інструменти та обладнання: - системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки; - сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої Програми	Освітньо-професійна
Основний фокус освітньої програми та спеціалізації	Спеціальна, в галузі F «Інформаційні технології», спеціальність F5 Кібербезпека та захист інформації Ключові слова: інформаційна безпека, кібербезпека та захист інформації, захист інформації в комп'ютерних системах.

Особливості програми	Інтегрована підготовка фахівців до створення та використання апаратного і системного програмного забезпечення комп'ютерних систем інформаційної безпеки та кібербезпеки. З метою підготовки до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації бакалавр з кібербезпеки програма передбачає надання студентам: - системних теоретичних знань в галузі ІТ технологій із поглибленим вивченням спеціалізації безпека інформаційних і комунікаційних систем; - сучасних компетентностей та практичних навичок з програмування, розробки та управління базами даних, формування моделей захисту інформації та політик безпеки, технічного і криптографічного захисту інформації, побудови захищених IP і TCP мереж та обслуговування сертифікатів відкритих ключів, побудови комплексних систем захисту інформації (далі – КСЗІ) на об'єктах інформаційної діяльності та захисту автоматизованих систем від несанкціонованого доступу, тестування систем захисту інформаційно-комунікаційних систем (далі – ІКС) на проникнення, реалізації управління інформаційною та кібернетичною безпекою, адміністрування захищених ІКС, проведення їх моніторингу та аудиту тощо. З метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу програма передбачає: - реалізацію процесного підходу при конструюванні змісту профільно-орієнтованих навчальних дисциплін, студентської мобільності, академічної співпраці та молодіжних обмінів; - залучення до викладацької діяльності керівників та професіоналів, які працюють як в системі професійної освіти, так й на виробництві в галузі інформаційних технологій та телекомунікацій, а також представників бізнесу.
4 - Придатність випускників до працевлаштування та подальшого навчання	

Придатність до працевлаштування	Згідно з чинною редакцією Національного класифікатора України: Класифікатор професій (ДК 003:2010) та International Standard Classification of Occupations 2008 (ISCO-08) випускник з професійною кваліфікацією «Фахівець з організації інформаційної безпеки» може працевлаштуватися на підприємствах і закладах будь-якої форми власності, які працюють в сфері ІТ-технологій, інформаційно-комунікаційного та телекомунікаційного сектора для виконання робіт з адміністрування ОС сімейств Windows/Linux, мережевого обладнання і технологій TCP/IP, DNS, DHCP, SSL/TLS та інш.; застосування засобів антивірусного захисту, програмних, клієнт-серверних та хмарних технологій захисту інформації (систем веб-фільтрації, систем запобігання вторгнень, систем захисту пошти від вірусів і спаму, тощо); створення технічної, проектної та експлуатаційної документації ІКС) та систем захисту інформації (СЗІ); налагодження, експлуатації та проведення аналізу системних процесів функціонування мережевих, клієнт-серверних та хмарних технологій; проведення моніторингу несанкціонованої активності в обчислювальних системах; створення, впровадження та експлуатації КСЗІ а також СЗІ в складі інформаційно-телекомунікаційних (ІТС) та обчислювальних систем; формування політик та процесів у сфері ІТ безпеки, управління доступом до мережевих ресурсів ІТС та ризиками інформаційної безпеки; проведення розслідувань інцидентів та забезпечення аудиту процесів інформаційної безпеки. Фахівці, які здобули освіти за освітньою програмою «Кібербезпека та захист інформації», можуть обіймати такі первинні посади: програміст/тестувальник програмного забезпечення систем ІКБ; адміністратор комп'ютерних систем і мереж; адміністратор інформаційної та кібербезпеки; аудитор безпеки інформаційно-комунікаційних систем; розробник засобів захисту інформації; інженер служби технічного захисту інформації, тощо.
Подальше навчання	Бакалавр зі спеціальності F5 Кібербезпека та захист інформації має право продовжити навчання для отримання ОС «Магістр» за
	спеціальністю F5 Кібербезпека та захист інформації або інших споріднених спеціальностей. Концепція освітньої програми підготовки фахівців відповідає освітнім програмам підготовки бакалаврів закордонних університетів «Bachelor of Science in Computer Engineering». Освітня програма надає можливість продовжувати навчання бакалаврів за кордоном і забезпечує академічну мобільність в межах України.
5 - Викладання та оцінювання	

Викладання та навчання	Студентоцентроване навчання, технологія проблемного і диференційованого навчання, технологія інтенсифікації та індивідуалізації навчання, технологія програмованого навчання, використання інформаційних технологій, технологія розвивального навчання, кредитно-трансферна система організації навчання, електронне навчання в системі e-learn, самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді: лекції, мультимедійної лекції, інтерактивної лекції, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, консультації з викладачами, атестації у формі єдиного державного кваліфікаційного іспиту. (підготовки кваліфікаційної роботи бакалавра (проекту).
Оцінювання	Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль. Екзамени, заліки та диференційовані заліки проводяться відповідно до вимог "Положення про екзамени та заліки в Державному біотехнологічному університеті " (2022 р). В ДБТУ використовується рейтингова форма контролю після закінчення логічно завершеної частини лекційних та практичних занять (модуля) з певної дисципліни. Її результати враховуються під час виставлення підсумкової оцінки. Рейтингове оцінювання знань студентів не скасовує традиційну систему оцінювання, а існує поряд із нею. Воно робить систему оцінювання більш гнучкою, об'єктивною і сприяє систематичній та активній самостійній роботі студентів протягом всього періоду навчання, забезпечує здорову конкуренцію між студентами у навчанні, сприяє виявленню і розвитку творчих здібностей студентів. Рейтинг студента із засвоєння навчальної дисципліни складається з рейтингу з навчальної роботи – 60 балів та рейтингу з атестації – 40 балів. Таким чином, на оцінювання засвоєння змістових модулів, на які поділяється навчальний матеріал дисципліни, передбачається 60 балів. Рейтингові оцінки із змістових модулів, як і рейтинг з атестації, теж обчислюються за 100-бальною шкалою. Письмові екзамени із співбесідою, здача звітів та захист лабораторних/практичних робіт, рефератів в якості самостійної роботи, проведення дискусій, семінарів та модулів. Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.

6 – Перелік компетентностей випускника:	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання в галузі кібербезпеки та захисту інформації.
Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності. ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК4. Здатність спілкуватися іноземною мовою. ЗК5. Здатність вчитися і оволодівати сучасними знаннями. ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ЗК7. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності; ЗК8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. ЗК9. Формування знань, умінь і навичок, необхідних для виконання конституційного обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України. ЗК10. Здатність до пошуку, оброблення та аналізу інформації
Спеціальні (фахові, предметні) компетентності	СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійної діяльності. СК2. Здатність використовувати інформаційні технології, сучасних методи і моделі кібербезпеки та системи захисту інформації. СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики інформаційної кібербезпеки та захисту інформації. СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики інформаційної кібербезпеки й захисту інформації. СК5. Здатність відновлювати функціонування інформаційних, та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплексні нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

	СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою безпеки.
7 - Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання.	
	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому. РН14. Вирішувати задачі управління процесами відновлення

	штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах; РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах. РН22. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Професорсько-викладацький склад, який забезпечує її реалізацію відповідає вимогам, визначеними Ліцензійними умовами провадження освітньої діяльності закладів освіти.

Матеріально-технічне забезпечення	Навчально-лабораторна база структурних підрозділів ДБТУ дозволяє організовувати та проводити заняття з усіх навчальних дисциплін на задовільному рівні. Для проведення лекційних занять використовуються мультимедійні проектори, навчальні лабораторії обладнані необхідними приладами та інструментами. Кафедри мають усе необхідне обладнання і прилади для проведення занять. На випусковій кафедрі кібербезпеки та інформаційних технологій функціонують ряд проблемних науково-дослідних, навчально-наукових, навчально-виробничих та навчальних лабораторій: «САПР засобів автоматизації», комп'ютерного моделювання, інтегрованих комп'ютерних технологій, «Проектування цифрових пристроїв на ПЛІС», методології та організація наукових досліджень. Матеріально-технічне забезпечення відповідає ліцензійним вимогам, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187, щодо надання освітніх послуг у сфері вищої освіти і є достатнім для забезпечення якості освітнього процесу, зокрема: навчальні приміщення; комп'ютерні класи; спеціалізовані лабораторії; спортивний зал, спортивні майданчики; бібліотека, читальний зал; мультимедійне обладнання; приміщення для науково-педагогічних працівників; гуртожитки; пункти харчування та ін.
Інформаційне та навчально-методичне забезпечення	Офіційний веб-сайт містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Всі зареєстровані в університеті користувачі мають необмежений доступ до мережі Інтернет. Фонди НБ складають: 1489002 одиниць друкованих видань та інших носіїв інформації, у т. ч. наукової літератури – 515464, навчальної – 756951, художньої – 160110, виокремлено із загального фонду 23311 примірника рідкісних та цінних видань (хронологічні рамки колекції з кінця XVIII по XX ст.). Формування фонду забезпечується документами та інформацією навчальної, виховної та наукової діяльності. Електронний каталог налічує більше 240 тис. записів в т. ч. 1420 повних текстів навчальних і навчально-методичних видань: репозитарій включає 9 основних колекцій, загальна кількість представлених документів – більше 13 тис повних текстів; «Веб-портфоліо науковця» електронний ресурс – система демонстрації наукометричних показників вчених ДБТУ, який базується на базах даних ПЗ ІРБІС і оболонці, написаній за допомогою фреймворка YII2 (містить 456 персональних сторінок науковців з інтерактивними посиланнями на профілі науковців в ORCID, Web of Science, Scopus, Google Scholar, Укрпатент, також представлено повний перелік публікацій науковців з посиланням на повний текст) «Літопис ДБТУ » багатосторінковий гіпертекстовий електронний ресурс містить публікації про ДБТУ всього 1050 документів. власний веб-сайт НБ з можливістю його мобільної WEB-присутності, має більше 2 450 проіндексованих сторінок: Загальна площа наукової бібліотеки – 1055 м², яка має 5 читальних залів площею 259 м² на 162 посадкових місць та книгосховище площею 649 м². Використання можливостей сучасних технологій у мережі Інтернет дозволяє суттєво підвищити рівень сервісу для

	віддалених користувачів, діє локальна комп'ютерна мережа, є вільна зона Wi-Fi.
9 - Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між ДБТУ та закладами вищої освіти України.
Міжнародна кредитна мобільність	Міжнародна діяльність університету визначена програмою сталого розвитку до 2025 року, яка передбачає розвиток інтеграційних процесів з міжнародними освітянськими структурами, зокрема: підвищення академічної мобільності викладачів і студентів, входження науковців університету до спільних європейських наукових програм тощо. Університет уклав договори про співпрацю з такими закордонними навчальними закладами: Професійно-технічний інститут провінції Шенсі, Литовський аграрний університет, Державний університет сільського господарства Молдови, Університет в Аалені, Університет в Клеве, Аграрний університет у Варшаві, Аграрний університет у Кракові, Державний університет Люблінська Політехніка, Державний природничий університет, Університет агрономії та ветеринарної медицини, Аграрний університет штату Огайо, Туркменський сільськогосподарський університет, Аграрний університет імені Святого Іштвана, Інститут відкритого суспільства.
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти може проводитися на загальних умовах з додатковою мовною підготовкою.
Форми атестації здобувачів вищої освіти та вимоги до неї	Атестація здобувачів першого (бакалаврського) освітньо-професійного рівня за спеціальністю F5 Кібербезпека та захист інформації здійснюється у формі єдиного державного кваліфікаційного іспиту та завершується видачею документа встановленого зразка про присудження йому ступеня бакалавра з присвоєнням кваліфікації «бакалавр з кібербезпеки та захисту інформації». Атестація здійснюється відповідно до Програми єдиного державного кваліфікаційного іспиту зі спеціальності F5 Кібербезпека та захист інформації на першому (бакалаврському) рівні вищої освіти. Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом вищої освіти та освітньою програмою.

2. Перелік компонент освітньо-професійної програми «Кібербезпека та захист інформації» та їх логічна послідовність

2.1. Перелік обов'язкових компонент ОПП

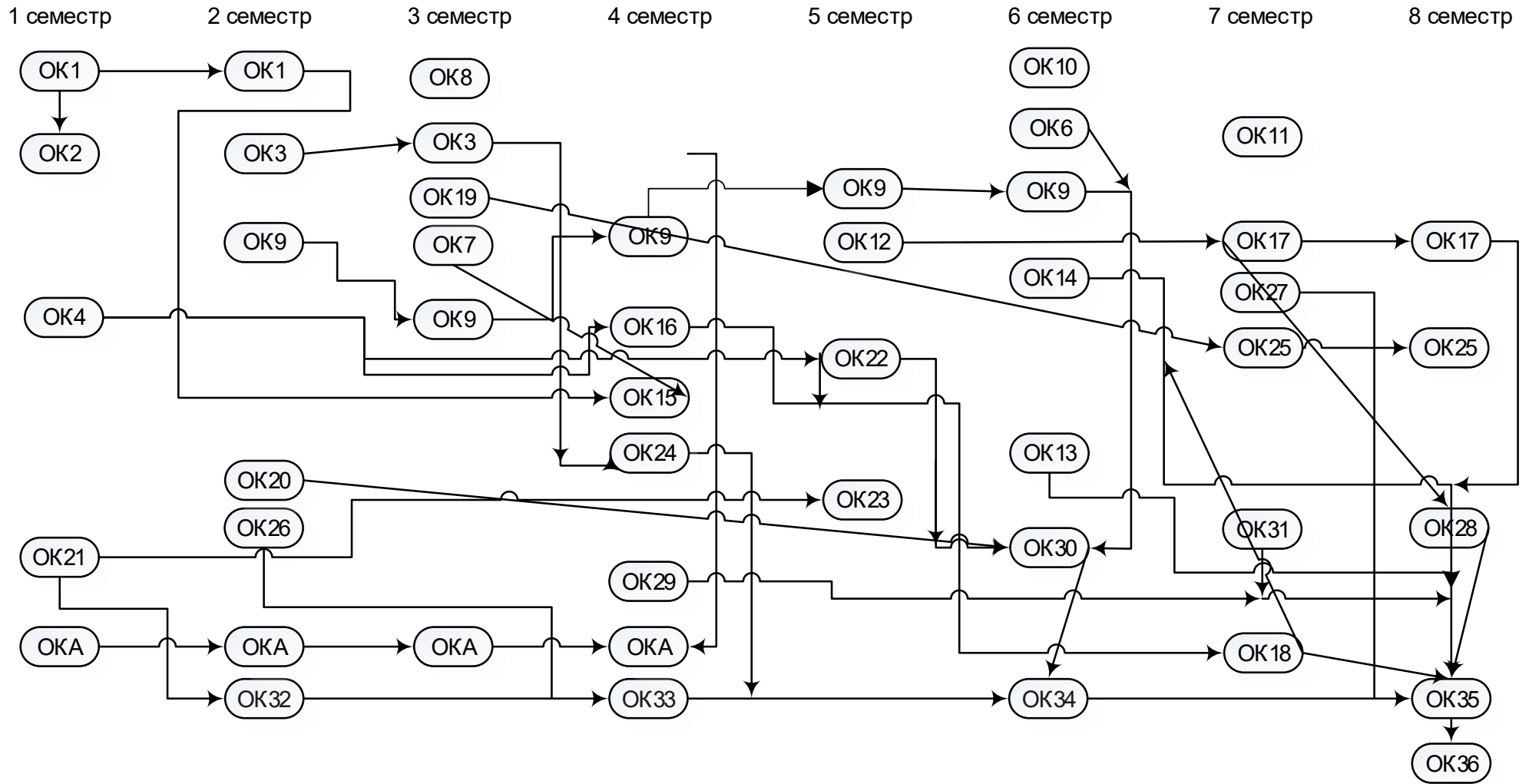
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового Контролю
1	2	3	4
1. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
1.1 Обов'язкові компоненти ОПП. 24			
OK1.	Вища математика	8	Залік , Екзамен,
OK2.	Фізика	4	Екзамен
OK3.	Програмування	8	Екзамен, Екзамен
OK4.	Вступ до фаху та академічна доброчесність	4	Екзамен
1.2 Обов'язкові компоненти ОПП за рішенням вченої ради університету 39			
OK6.	Українська мова за професійним спрямуванням	4	Залік
OK7.	Дискретна математика	4	Екзамен
OK8	Історія української державності	4	Екзамен
OK9	Іноземна мова	15	Екзамен (2), Залік (2)
OK10	Філософія	4	Екзамен
OK11	Основи економіки та бізнесу	4	Залік
2. ЦИКЛ СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
2.1 Обов'язкові компоненти ОПП 117			
OK12	Теорія інформації і кодування	4	Залік
OK13	Державні та міжнародні стандарти та практики в галузі кібербезпеки	4	Екзамен
OK14	Теорія ризиків	4	Екзамен
OK15	Мережева академія Cisco. Спецкурси	4	Залік
OK16	Захист програмного забезпечення	4	Екзамен
OK17	Комплексні системи захисту інформації	7	Екзамен,
OK18	Організаційне забезпечення захисту інформації	6	Екзамен
OK19	Архітектура комп'ютерних систем	4	Екзамен
OK20	Комп'ютерні системи та мережі, їх безпека	5	Екзамен
OK21	Інформаційні технології	6	Екзамен
OK22	Прикладна криптологія та стеганографічний захист	6	Екзамен
OK23	Операційні системи та їх безпека	6	Екзамен
OK24	Інженерія програмного забезпечення	4	Екзамен
OK25	Безпека безпроводних, мобільних та хмарних технологій	6	Залік, Екзамен
OK26	Теоретичні основи захисту інформації	3	Залік
OK27	Сучасні методи та засоби збереження, маскування та відновлення даних в сфері інформаційних технологій	4	Екзамен
OK28	Технічний захист інформації	6	Екзамен
OK29	Бази даних та інформаційні системи	4	Екзамен, Залік
OK30	Аналіз шкідливого програмного забезпечення	4	Екзамен
OK31	Аналіз і моніторинг кібернетичної безпеки	6	Екзамен
OK32	Навчальна практика (комп'ютерна)	6	Залік
OK33	Навчальна практика (з технологій захисту інформації)	6	Залік
OK34	Виробнича практика	6	Залік
OK35	Передатестаційна практика	4	Залік
OK36	Єдиний державний кваліфікаційний іспит	2	Екзамен
ОКА	Фізичне виховання (за рахунок вільного часу студентів)	0	Залік
Загальний обсяг обов'язкових компонентів		180	

3. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ

(Перелік вибіркового навчальних дисциплін Освітньої програми міститься у Додатку до ОП)

ВНД-1	Вибіркова навчальна дисципліна I семестру	3	Залік
ВНД-2	Вибіркова навчальна дисципліна I семестру	3	Залік
ВНД-3	Вибіркова навчальна дисципліна II семестру	3	Залік
ВНД-4	Вибіркова навчальна дисципліна II семестру	3	Залік
ВНД-5	Вибіркова навчальна дисципліна II семестру	3	Залік
ВНД-6	Вибіркова навчальна дисципліна III семестру	3	Залік
ВНД-7	Вибіркова навчальна дисципліна III семестру	3	Залік
ВНД-8	Вибіркова навчальна дисципліна IV семестру	3	Залік
ВНД-9	Вибіркова навчальна дисципліна IV семестру	3	Залік
ВНД-10	Вибіркова навчальна дисципліна IV семестру	3	Залік
ВНД-11	Вибіркова навчальна дисципліна V семестру	3	Залік
ВНД-12	Вибіркова навчальна дисципліна V семестру	3	Залік
ВНД-13	Вибіркова навчальна дисципліна V семестру	3	Залік
ВНД-14	Вибіркова навчальна дисципліна VI семестру	3	Залік
ВНД-15	Вибіркова навчальна дисципліна VI семестру	3	Залік
ВНД-16	Вибіркова навчальна дисципліна VII семестру	3	Залік
ВНД-17	Вибіркова навчальна дисципліна VII семестру	3	Залік
ВНД-18	Вибіркова навчальна дисципліна VIII семестру	3	Залік
ВНД-19	Вибіркова навчальна дисципліна VIII семестру	3	Залік
ВНД-20	Вибіркова навчальна дисципліна VIII семестру	3	Залік
Загальний обсяг вибіркового компонентів		60	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

2.2. Структурно-логічна схема підготовки фахівців (на базі обов'язкових компонентів ОПІ)



3. Форми атестації здобувачів вищої освіти

Атестація здобувачів першого (бакалаврського) освітньо-професійного рівня за спеціальністю F5 Кібербезпека та захист інформації здійснюється у формі єдиного державного кваліфікаційного іспиту та завершується видачею документа встановленого зразка про присудження йому ступеня бакалавра з присвоєнням кваліфікації «бакалавр з кібербезпеки та захисту інформації». Атестація здійснюється відповідно до Програми єдиного державного кваліфікаційного іспиту зі спеціальності F5 Кібербезпека та захист інформації на першому (бакалаврському) рівні вищої освіти. Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом вищої освіти та освітньою програмою.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми «Кібербезпека та захист інформації»

	ОК1	ОК2	ОК3	ОК4	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22
ЗК1		+	+	+				+		+		+	+	+	+	+	+	+	+	+	+
ЗК2			+	+							+	+	+	+	+	+	+	+	+	+	+
ЗК3					+		+														
ЗК4				+				+													
ЗК5	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК6				+			+		+			+					+				
ЗК7				+			+	+	+	+		+					+				
ЗК8				+			+		+	+		+					+				
ЗК9				+			+		+			+					+				
ЗК10				+				+	+			+					+				
СК1				+								+					+				
СК2											+		+	+	+	+		+	+	+	
СК3										+		+				+	+				
СК4															+	+	+	+	+	+	
СК5													+	+	+	+	+				
СК6				+											+	+	+				
СК7													+		+	+	+				
СК8																			+		+
СК9				+												+			+		
СК10				+											+						+

	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	OK33	OK34	OK35	OK36	OKA
3K1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
3K2	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
3K3															
3K4												+	+		
3K5	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
3K6															+
3K7															
3K8															+
3K9															+
3K10										+	+	+	+		
CK1										+	+	+	+		
CK2	+			+						+	+	+	+		
CK3	+	+	+									+	+	+	
CK4	+	+	+	+	+	+	+	+	+	+		+	+	+	
CK5	+		+		+	+		+					+	+	
CK6			+			+		+					+	+	
CK7	+		+	+	+	+			+				+	+	
CK8				+				+					+	+	
CK9					+	+					+	+	+	+	
CK10								+	+			+	+	+	

5. Матриця забезпечення результатів навчання відповідними компонентами освітньої програми

	ОК1	ОК2	ОК3	ОК4	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22
PH1					+		+														
PH2								+													
PH3				+					+	+		+					+				
PH4			+	+					+	+		+	+	+	+	+	+	+	+	+	+
PH5			+	+					+				+	+	+	+	+	+	+	+	+
PH6			+	+					+				+	+	+	+	+	+	+	+	
PH7	+	+	+	+		+					+		+	+		+			+	+	+
PH8	+	+	+	+		+					+		+		+	+			+		
PH9				+								+				+	+				
PH10	+																			+	
PH11										+		+					+				
PH12																	+		+		
PH13													+	+	+	+	+	+	+		
PH14																	+	+	+		
PH15				+									+	+	+	+			+		
PH16				+													+	+			
PH17										+			+			+	+				
PH18																					+
PH19												+									+
PH20																+					
PH21				+									+			+		+	+		
PH22				+								+					+				

	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	OK33	OK34	OK35	OK36	OKA
PH1															
PH2															
PH3															
PH4	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
PH5	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
PH6	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
PH7	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
PH8				+	+						+	+	+	+	
PH9						+									
PH10				+											
PH11											+	+	+	+	
PH12	+										+	+	+	+	
PH13	+	+	+		+	+	+	+			+	+	+	+	
PH14					+			+	+			+	+		
PH15	+		+			+		+	+			+	+	+	
PH16												+	+	+	
PH17												+	+	+	
PH18												+	+	+	
PH19												+	+	+	
PH20						+						+	+	+	
PH21	+		+			+						+	+	+	
PH22										+	+				

6. Перелік нормативних документів

1. Закон України від 01.07.2014 р. № 1556-VII «Про вищу освіту» [Режим доступу: <http://zakon4.rada.gov.ua/laws/show/1556-18>];
2. Закон України від 05.09.2017 р. «Про освіту» - [Режим доступу: <http://zakon5.rada.gov.ua/laws/show/2145-19>] ;
3. Постанова Кабінету Міністрів України «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29.04.2015 р. №266 [Режим доступу: <http://zakon4.rada.gov.ua/laws/show/266-2015-п>] ;
4. Постанова Кабінету Міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30.12.2015 р. № 1187 [Режим доступу: <http://zakon4.rada.gov.Ua/laws/show/1187-2015-п/page>]
5. Постанова Кабінету Міністрів України «Про затвердження Національної рамки кваліфікацій» від 23.11.2011 р. №1341 [Режим доступу: <http://zakon4.rada.gov.ua/laws/show/1341-2011-п>];
6. Національний класифікатор України: «Класифікатор професій» ДК 003: 2010ДК 003:2010 [Режим доступу: <http://www.dk003.com>];
7. Положення про організацію освітнього процесу в Державному біотехнологічному університеті, Харків, 2021. – 53 с. [Режим доступу: <https://btu.kharkov.ua/pro-universitet/publicna-informatsiya/normatyvna-baza/>];
8. Положення про організацію освітнього процесу з використанням дистанційних технологій, Харків, 2022. – 13 с. [<https://btu.kharkov.ua/pro-universitet/publicna-informatsiya/normatyvna-baza/>];
9. Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG) [Режим доступу: https://osvita.kpi.ua/files/downloads/Standart_EPVO.pdf];
10. Постанова Кабінету Міністрів України «Про атестацію здобувачів ступеня фахової передвищої освіти та ступенів вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях у формі єдиного державного кваліфікаційного іспиту» від 19 травня 2021 р. № 497;
11. Наказ Міністерства освіти і науки України від 13 січня 2022 р. № 26 «Про внесення змін до деяких стандартів вищої освіти»;
12. Наказ Міністерства освіти і науки України «Про затвердження стандарту вищої освіти за спеціальністю F5 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти» від 04 жовтня 2018 р., № 1074;
13. Положення про внутрішню систему забезпечення якості вищої освіти в Державному біотехнологічному університеті. Методична розробка / Ю. О. Васильєва, А. І. Дидикіна, О. В. Коляда // Державний біотехнологічний університет. – Харків: РВБ ДБТУ, 2021 р. – 26 с. <http://btu.kharkov.ua/wp-content/uploads/2021/11/POLOZHENNYA-PRO-SYSTEMU-VNUTRISHNOGO-ZABEZPECHENNYA-YAKOSTI-VYSHNOYI-OSVITY-V-DBTU.pdf>

14. Положення про освітні програми Державного біотехнологічного університету. / О.І. Алфьоров, Ю.О. Васильєва, С.А. Знайдюк, О.В. Коляда, А.І. Дидикіна // Державний біотехнологічний університет. – Харків: РВВ ДБТУ, 2021 р. – 29 с.
<http://btu.kharkov.ua/wp-content/uploads/2021/11/POLOZHENNYA-PRO-OSVITNI-PROGRAMY.pdf>
15. Проект Закону України «Про застосування англійської мови в Україні» <https://itd.rada.gov.ua/billInfo/Bills/pubFile/1854364>
16. Загальноєвропейські рекомендації з мовної освіти.
17. Наказ МОН України № 842 від 13.06.2024 "Про внесення змін до деяких стандартів вищої освіти"
<https://mon.gov.ua/npa/pro-vnesennia-zmin-do-deiakykh-standativ-vyshchoi-osvity842>
18. Наказ МОН України № 1547 від 29.10.2024 "Про внесення змін до стандарту вищої освіти зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти"
19. Постанова КМУ № 734 від 21 червня 2024 року «Порядок проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських». <https://zakon.rada.gov.ua/laws/show/734-2024-%D0%BF#Text>