МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ БІОТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»

РІВЕНЬ ВИЩОЇ ОСВІТИ: Перший (бакалаврський)
СТУПІНЬ ВИЩОЇ ОСВІТИ: Бакалавр
ГАЛУЗЬ ЗНАНЬ: F Інформаційні технології
СПЕЦІАЛЬНІСТЬ: F5 «Кібербезпека та захист інформації»
ОСВІТНЯ КВАЛІФІКАЦІЯ: Бакалавр з кібербезпеки та захисту інформації

РІК ВСТУПУ: 2026

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Державного біотехнологічного університету
Голова вченої ради

_____/ /
(протокол № __ від « » квітня 2026 р.)
та вводиться в дію з «01» вересня 2026 р.

Харків – 2026

ПЕРЕДМОВА

Відповідає Стандарту вищої освіти першого (бакалаврського) рівня галузі знань F «Інформаційні технології», спеціальності F5 «Кібербезпека та захист інформації», затвердженого та введеного в дію наказом Міністерства освіти і науки України від 29.10.2024 р. № 1547.

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 менеджменту, адміністрування та права Кафедра інформаційних технологій, кібернетики та захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Освітня кваліфікація: бакалавр з кібербезпеки та захисту інформації Кваліфікація в дипломі: 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	Акредитується вперше
Цикл/рівень	Перший (бакалаврський) рівень FQ-EHEA – 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 2030 року. Переглядається щорічно
Інтернет-адреса постійного розміщення опису освітньої програми	https://biotechuniv.edu.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 вивчення: − технології кібербезпеки та захисту інформації; − процеси управління кібербезпекою 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 кібербезпеки 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. **Методи, методики та технології:** методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки. **Інструменти та обладнання:** засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проєктування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Орієнтація освітньої програми	Освітньо-професійна. Підготовка фахівців у сфері кібербезпеки та захисту інформації.
Основний фокус освітньої програми	Спеціальна, в галузі F «Інформаційні технології», спеціальність F5 Кібербезпека та захист інформації Ключові слова: інформаційні технології, 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 інформаційно-комунікаційних систем (далі – ІКС) від несанкціонованого доступу, реалізації управління інформаційною та кібернетичною безпекою, 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: - використання курсів мережевої академії Cisco з Networking, Prometheus та інших; - 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); супроводження 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; 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 освіту за освітньою програмою «Кібербезпека та захист інформації», можуть обіймати такі первинні посади: 2139.2 Фахівець сфери захисту інформації; 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології); 2139.2 Фахівець з підтримки інфраструктури кіберзахисту; 2139.2 Фахівець з реагування на інциденти кібербезпеки;

	2139.2 Фахівець з криптографічного захисту інформації; 2139.2 Фахівець з технічного захисту інформації; 2139.2 Фахівець з тестування систем безпеки та захисту інформації; 2139.2 Аудитор інформаційних технологій (з кібербезпеки); 2139.2 Фахівець з оцінки заходів захисту інформації (кібербезпеки).
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.
Академічні права випускників	Концепція освітньої програми підготовки фахівців відповідає освітнім програмам підготовки бакалаврів закордонних університетів «Bachelor of Science in Cybersecurity (Bachelor of Information Security)». 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 Moddle, 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.
Оцінювання	Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль. Екзамени, диференційовані заліки проводяться відповідно до вимог «Положення про організацію освітнього процесу в Державному біотехнологічному університеті » (2025 р). В ДБТУ використовується модульна форма проміжного 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**. Здатність до пошуку, оброблення та системному аналізу інформації. **ЗК***. Формування знань, умінь і навичок, необхідних для виконання конституційного обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України. ЗК* формується вибірковою дисципліною «Теоретична підготовка БЗВП» / «Національно-патріотична та правова підготовка молоді» (згідно з постановою КМУ № 734 від 21 червня 2024 року та наказом ДБТУ від 24 березня 2025 року № 02-02/217).
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, сучасні 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 (комплекси 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	
Результати навчання за спеціальністю (визначені стандартом вищої освіти спеціальності)	**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, згідно з діючим законодавством України (Постанова Кабінету Міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р. № 1187, зі змінами, внесеними згідно з Постановою КМУ № 365 від 24.03.2021. (Додаток 15-16). Склад робочої групи освітньої програми, професорсько викладацький склад, що задіяний до викладання навчальних дисциплін за спеціальністю відповідають Ліцензійним умовам провадження освітньої діяльності на першому (бакалаврському) рівні вищої освіти. До викладання залучаються викладачі-практики, фахівці та співробітники ІТ-компаній, а також закордонні фахівці.
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 інформаційних технологій, кібернетики та захисту інформації функціонують ряд проблемних науково-дослідних та навчальних лабораторій. Матеріально-технічне забезпечення відповідає ліцензійним вимогам, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187, зі змінами, внесеними згідно з Постановою КМУ № 365 від 24.03.2021. (Додаток 15-16), щодо надання освітніх послуг у сфері вищої світи 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. У навчальному процесі застосовується LMS (Learning Management System) Moodle. 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 (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 м^2, яка має 5 читальних залів площею 259 м^2 на 162 посадкових місць та книгосховище площею 649 м^2. 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 стратегію розвитку ДБТУ на 2022-2027 роки, 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.
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

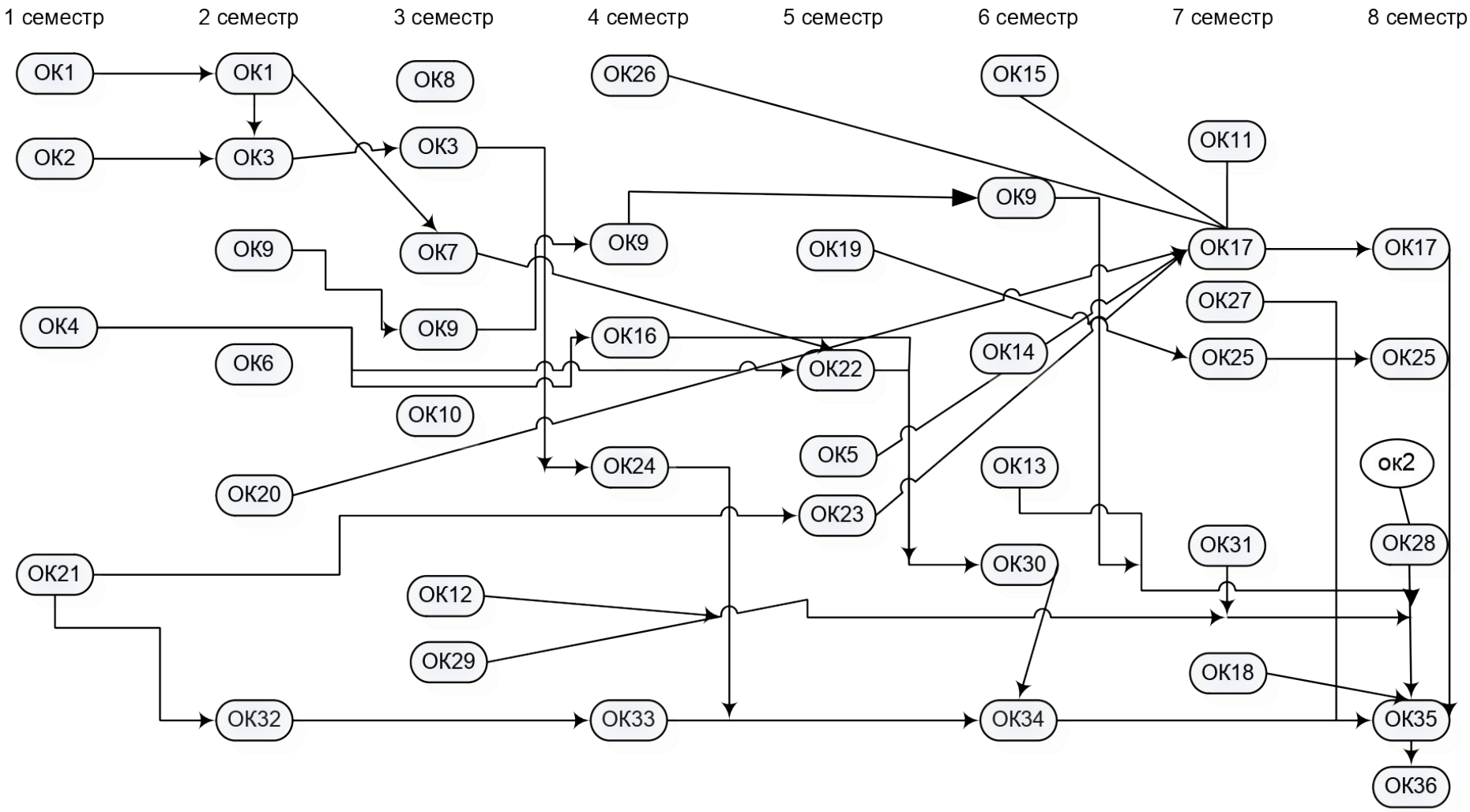
2.1. Перелік обов'язкових компонент ОПП

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			
ОК1	Вища математика	8	Залік , Екзамен,
ОК2	Фізика	4	Екзамен
ОК3	Програмування	8	Екзамен, Екзамен
ОК4	Вступ до фаху та академічна доброчесність	4	Екзамен
ОК7	Математичні основи криптології	4	Екзамен
ОК11	Основи економіки та бізнесу	4	Залік
1.2 Обов'язкові компоненти ОПП за рішенням вченої ради університету			
ОК6	Українська мова (за професійним спрямуванням)	4	Залік
ОК8	Історія української державності та громадянське суспільство	4	Екзамен
ОК9	Іноземна мова	15	Екзамен (1), Залік (2)
ОК10	Філософія	4	Екзамен
2. ЦИКЛ СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
2.1 Обов'язкові компоненти ОПП			
ОК5	Системний аналіз в інформаційній безпеці	4	Залік
ОК12	Теорія інформації і кодування	4	Залік
ОК13	Державні та міжнародні стандарти та практики в галузі кібербезпеки	4	Екзамен
ОК14	Теорія ризиків в кібербезпеці	4	Екзамен
ОК15	Інформаційна безпека держави	4	Залік
ОК16	Захист програмного забезпечення	4	Екзамен
ОК17	Комплексні системи захисту інформації	6	Залік, Екзамен
ОК18	Організаційне забезпечення захисту інформації	4	Екзамен
ОК19	Архітектура комп'ютерних систем	4	Екзамен
ОК20	Комп'ютерні системи та мережі, їх безпека	5	Екзамен
ОК21	Інформаційні технології	6	Екзамен
ОК22	Основи криптографічного та стеганографічного захисту	6	Екзамен
ОК23	Операційні системи та їх безпека	4	Екзамен
ОК24	Інженерія програмного забезпечення	4	Екзамен
ОК25	Безпека безпровідних, мобільних та хмарних технологій	7	Залік, Екзамен
ОК26	Теоретичні основи захисту інформації	3	Екзамен
ОК27	Сучасні методи та засоби збереження, маскування та відновлення даних в сфері інформаційних технологій	4	Екзамен
ОК28	Технічний захист інформації	6	Екзамен
ОК29	Бази даних та інформаційні системи	4	Залік
ОК30	Аналіз шкідливого програмного забезпечення	4	Екзамен
ОК31	Аналіз і моніторинг кібернетичної безпеки	6	Екзамен
ОК32	Навчальна практика (комп'ютерна)	6	Залік
ОК33	Навчальна практика (з технологій захисту інформації)	6	Залік
ОК34	Виробнича практика	6	Залік
ОК35	Передатестаційна практика	4	Залік
ОК36	Єдиний державний кваліфікаційний іспит	2	Екзамен
Загальний обсяг обов'язкових компонентів		**180**	

3. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ *(Перелік вибіркових навчальних дисциплін Освітньої програми міститься у Додатку до ОП)*			
ВНД-1	Вибіркова навчальна дисципліна	3	Залік
ВНД-2	Вибіркова навчальна дисципліна	3	Залік
ВНД-3	Вибіркова навчальна дисципліна	3	Залік
ВНД-4	Вибіркова навчальна дисципліна	3	Залік
ВНД-5	Вибіркова навчальна дисципліна	3	Залік
ВНД-6	Вибіркова навчальна дисципліна	3	Залік
ВНД-7	Вибіркова навчальна дисципліна	3	Залік
ВНД-8	Вибіркова навчальна дисципліна	3	Залік
ВНД-9	Вибіркова навчальна дисципліна	3	Залік
ВНД-10	Вибіркова навчальна дисципліна	3	Залік
ВНД-11	Вибіркова навчальна дисципліна	3	Залік
ВНД-12	Вибіркова навчальна дисципліна	3	Залік
ВНД-13	Вибіркова навчальна дисципліна	3	Залік
ВНД-14	Вибіркова навчальна дисципліна	3	Залік
ВНД-15	Вибіркова навчальна дисципліна	3	Залік
ВНД-16	Вибіркова навчальна дисципліна	3	Залік
ВНД-17	Вибіркова навчальна дисципліна	3	Залік
ВНД-18	Вибіркова навчальна дисципліна	3	Залік
ВНД-19	Вибіркова навчальна дисципліна	3	Залік
ВНД-20	Вибіркова навчальна дисципліна	3	Залік
Загальний обсяг вибіркових компонентів		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

ОКА - Фізичне виховання - позакредитна дисципліна.

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



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	ОК5	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					+																+	
СК1				+									+					+				
СК2			+				+							+		+	+		+	+	+	
СК3											+		+				+	+				
СК4																+	+	+	+	+		
СК5														+		+	+	+				
СК6																+	+	+				
СК7														+	+		+	+				
СК8							+													+		+
СК9																	+			+		
СК10																						+

	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36
ЗК1	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК2	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК3														
ЗК4												+	+	
ЗК5	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК6														
ЗК7														
ЗК8														
ЗК9				+										
СК1										+	+	+	+	
СК2	+			+						+	+	+	+	
СК3	+	+	+									+	+	+
СК4	+	+	+	+	+	+	+	+	+	+		+	+	+
СК5	+		+		+	+		+					+	+
СК6			+			+		+					+	+
СК7	+		+	+	+	+			+				+	+
СК8				+				+					+	+
СК9					+	+					+	+	+	+
СК10								+	+			+	+	+

5. Матриця забезпечення результатів навчання відповідними компонентами освітньої програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22
РН1						+		+														
РН2									+													
РН3				+						+	+		+					+				
РН4			+	+							+		+	+		+	+	+	+	+	+	+
РН5			+		+					+				+	+	+	+	+	+	+	+	+
РН6			+	+						+				+	+	+	+	+	+	+	+	
РН7	+		+				+					+		+	+		+			+		+
РН8	+	+	+	+			+							+		+	+			+		
РН9				+									+				+	+				
РН10					+																+	
РН11											+							+				
РН12							+											+		+		
РН13															+	+	+	+	+	+		
РН14																		+	+	+		
РН15					+									+	+	+	+			+		
РН16																		+	+			
РН17											+			+			+	+				
РН18																						+
РН19																						+
РН20																	+					
РН21														+			+		+	+		
РН22				+	+								+					+				

	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36
РН1														
РН2														
РН3														
РН4	+	+	+	+	+	+	+	+	+	+	+	+	+	+
РН5	+	+	+	+	+	+	+	+	+	+	+	+	+	+
РН6	+	+	+	+	+	+	+	+	+	+	+	+	+	+
РН7	+	+	+	+	+	+	+	+	+	+	+	+	+	+
РН8				+	+						+	+	+	+
РН9						+								
РН10				+										
РН11											+	+	+	+
РН12	+										+	+	+	+
РН13	+	+	+		+	+	+	+			+	+	+	+
РН14					+			+	+			+	+	
РН15	+		+			+		+	+			+	+	+
РН16												+	+	+
РН17												+	+	+
РН18												+	+	+
РН19												+	+	+
РН20						+						+	+	+
РН21	+		+			+						+	+	+
РН22										+	+			

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/l 187-2015-n/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, 2025. – 57 с. [Режим доступу: https://btu.kharkov.ua/pro-universitet/publichna-informatsiya/normatyvna-baza/];

8. Положення про організацію освітнього процесу з використанням дистанційних технологій, Харків, 2025. – 12 с. [https://btu.kharkov.ua/pro-universitet/publichna-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: РВВ ДБТУ, 2021 р. – 26 с. http://btu.kharkov.ua/wp-content/uploads/2021/11/POLOZHENNYA-PRO-SYSTEMU-VNUTRISHNOGO-ZABEZPECHENNYA-YAKOSTI-VYSHHOYI-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. Проєкт 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-standartiv-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