**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:** 125 Кібербезпека та захист інформації
**ГАЛУЗЬ ЗНАНЬ:** 12 Інформаційні технології
**ОСВІТНЯ КВАЛІФІКАЦІЯ:** Бакалавр з кібербезпеки та захисту інформації

**РІК ВСТУПУ:** 2023

**ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ**
**Державного біотехнологічного університету**
**протокол № 9 від «16» травня 2023 р.)**
**та вводиться в дію з «01» вересня 2023 р.**

**В. о. ректора**

**_____ /Андрій Кудряшов/**

**Харків – 2023**

# ПЕРЕДМОВА

Освітньо-професійна програма (ОПП) для підготовки здобувачів вищої освіти першого (бакалаврського) рівня за спеціальністю 125 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 кібербезпеки та інформаційних технологій.
3. **Міхнова Олена Дмитрівна**, кандидат технічних наук, доцент кафедри кібербезпеки та інформаційних технологій.
4. **Чалий Ігор Вільович,** кандидат технічних наук, доцент кафедри кібербезпеки та інформаційних технологій.

Освітньо-професійна програма «**Кібербезпека та захист інформації**» підготовки фахівців першого (бакалаврського) рівня вищої освіти за спеціальністю 125 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 125 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 125 Кібербезпека та захист інформації (наказ Міністерства освіти і науки України від 13.01.2022 р. №26).

# 1. Профіль освітньо-професійної програми «Кібербезпека та захист інформації» зі спеціальності 125 Кібербезпека та захист інформації

| 1 - Загальна інформація | |
|---|---|
| **Повна назва закладу вищої освіти та структурного підрозділу** | Державний біотехнологічний університет<br>Факультет кіберпорт, кафедра кібербезпеки та інформаційних технологій. |
| **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<br>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 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 12 Інформаційні технології<br>Спеціальність 125 Кібербезпека та захист інформації.<br>Об’єкти професійної діяльності випускників:<br>- об'єкти інформатизації, включаючи комп’ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології;<br>- технології забезпечення безпеки інформації;<br>- процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту. |

| | |
|---|---|
| | Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Теоретичний зміст предметної області.<br>Знання:<br>- законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;<br>- принципів супроводу систем та комплексів інформаційної та/або кібербезпеки;<br>- теорії, моделей та принципів управління доступом до інформаційних ресурсів;<br>- теорії систем управління інформаційною та/або кібербезпекою;<br>- методів та засобів виявлення, управління та ідентифікації ризиків;<br>- методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації;<br>- методів та засобів технічного та криптографічного захисту інформації;<br>- сучасних інформаційно-комунікаційних технологій;<br>- сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій;<br>- автоматизованих систем проектування.<br>Методи, методики та технології: методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки.<br>Інструменти та обладнання:<br>- системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки;<br>- сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. |
| **Орієнтація освітньої Програми** | Освітньо-професійна |
| **Основний фокус освітньої програми та спеціалізації** | Спеціальна, в галузі 12 «Інформаційні технології», спеціальність 125 Кібербезпека та захист інформації<br>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.<br>З метою підготовки до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації бакалавр з кібербезпеки програма передбачає надання студентам:<br>- системних теоретичних знань в галузі ІТ технологій із поглибленим вивченням спеціалізації безпека інформаційних і комунікаційних систем;<br>- 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.<br>З метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу програма передбачає:<br>- реалізацію процесного підходу при конструюванні змісту профільно-орієнтованих навчальних дисциплін, студентської мобільності, академічної співпраці та молодіжних обмінів;<br>- 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.<br>Фахівці, які здобули освіту 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 125 Кібербезпека та захист інформації має право продовжити навчання для отримання ОС «Магістр» за |

| | |
|---|---|
| | спеціальністю 125 Кібербезпека та захист інформації або інших споріднених спеціальностей.<br>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.<br>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.<br>Екзамени, заліки та диференційовані заліки проводяться відповідно до вимог "Положення про екзамени та заліки в Державному біотехнологічному університеті " (2022 р).<br>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.<br>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.<br>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.<br>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 – Програмні компетентності | |
|---|---|
| **Інтегральна компетентність** | Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в галузі забезпечення інформаційної безпеки та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов. |
| **Загальні компетентності (ЗК)** | **КЗ1**. Здатність застосовувати знання у практичних ситуаціях.<br>**КЗ2**. Знання та розуміння предметної області та розуміння професії.<br>**КЗ3**. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.<br>**КЗ4**. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.<br>**КЗ5**. Здатність до пошуку, оброблення та аналізу інформації.<br>**КЗ6**. 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;<br>**КЗ7**. 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.<br>**КЗ8**. Здатність до абстрактного і системного мислення, аналізу та синтезу. |
| **Фахові компетентності спеціальності (ФК)** | **ФК1**. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.<br>**ФК2**. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.<br>**ФК3**. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.<br>**ФК4**. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.<br>**ФК5**. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.<br>**ФК6**. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.<br>**ФК7**. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) |

| | |
|---|---|
| | **ФК8**. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.<br>**ФК9**. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.<br>**ФК10**. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.<br>**ФК11**. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.<br>**ФК12**. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.<br>**ФК13**. Здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем захисту інформації. |
| **7 - Програмні результати навчання (ПРН)** | |
| | 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;<br>2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;<br>3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;<br>4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;<br>5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;<br>6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;<br>7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки;<br>8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки;<br>9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;<br>10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;<br>11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;<br>12. Розробляти моделі загроз та порушника; |

| | |
|---|---|
| | 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;<br>14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;<br>15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;<br>16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;<br>17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;<br>18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;<br>19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;<br>20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;<br>21. Вирішувати задачі забезпечення та супроводу (в тому числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;<br>22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;<br>23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;<br>24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);<br>25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; |

| | |
|---|---|
| | 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;<br>27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;<br>28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;<br>29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;<br>30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;<br>31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;<br>32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;<br>33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;<br>34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;<br>35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;<br>36. Виявляти небезпечні сигнали технічних засобів;<br>37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;<br>38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;<br>39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах |

| | |
|---|---|
| | додержання режиму секретності із фіксуванням результатів у відповідних документах;<br>40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;<br>41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;<br>42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної, і/або кібербезпеки;<br>43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;<br>44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;<br>45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;<br>46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;<br>47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;<br>48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;<br>49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;<br>50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);<br>51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;<br>52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;<br>53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз;<br>54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.<br>55. Знати і розуміти наукові, математичні і фізичні положення, що лежать в основі функціонування систем захисту інформації.<br>Вміти застосовувати знання для розв’язування задач аналізу та синтезу засобів, характерних для систем захисту інформації. |

| 8 – Ресурсне забезпечення реалізації програми | |
|---|---|
| **Кадрове забезпечення** | Професорсько-викладацький склад, який забезпечує її реалізацію відповідає вимогам, визначеними Ліцензійними умовами провадження освітньої діяльності закладів освіти. Понад 80 % професорсько-викладацького складу, задіяного до викладання циклу дисциплін професійної підготовки, мають відповідні наукові ступені з дисциплін, які викладають. |
| **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 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.<br>Фонди НБ складають: 372523 одиниць друкованих видань та інших носіїв інформації, у т. ч. наукової літератури – 82410, навчальної – 249310, художньої – 40337, виокремлено із загального фонду 483 примірника рідкісних та цінних видань (хронологічні рамки колекції з кінця XVIII по XX ст.).<br>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 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 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: Білоруський агротехнічний університет, Професіонально-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. На факультеті кіберпорт на навчання залучено 2 іноземних студентів на спеціальність 125 Кібербезпека та захист інформації. |
| **Форми атестації здобувачів вищої освіти та вимоги до неї** | Атестація здобувачів першого (бакалаврського) освітньо-професійного рівня за спеціальністю 125 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 125 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. |

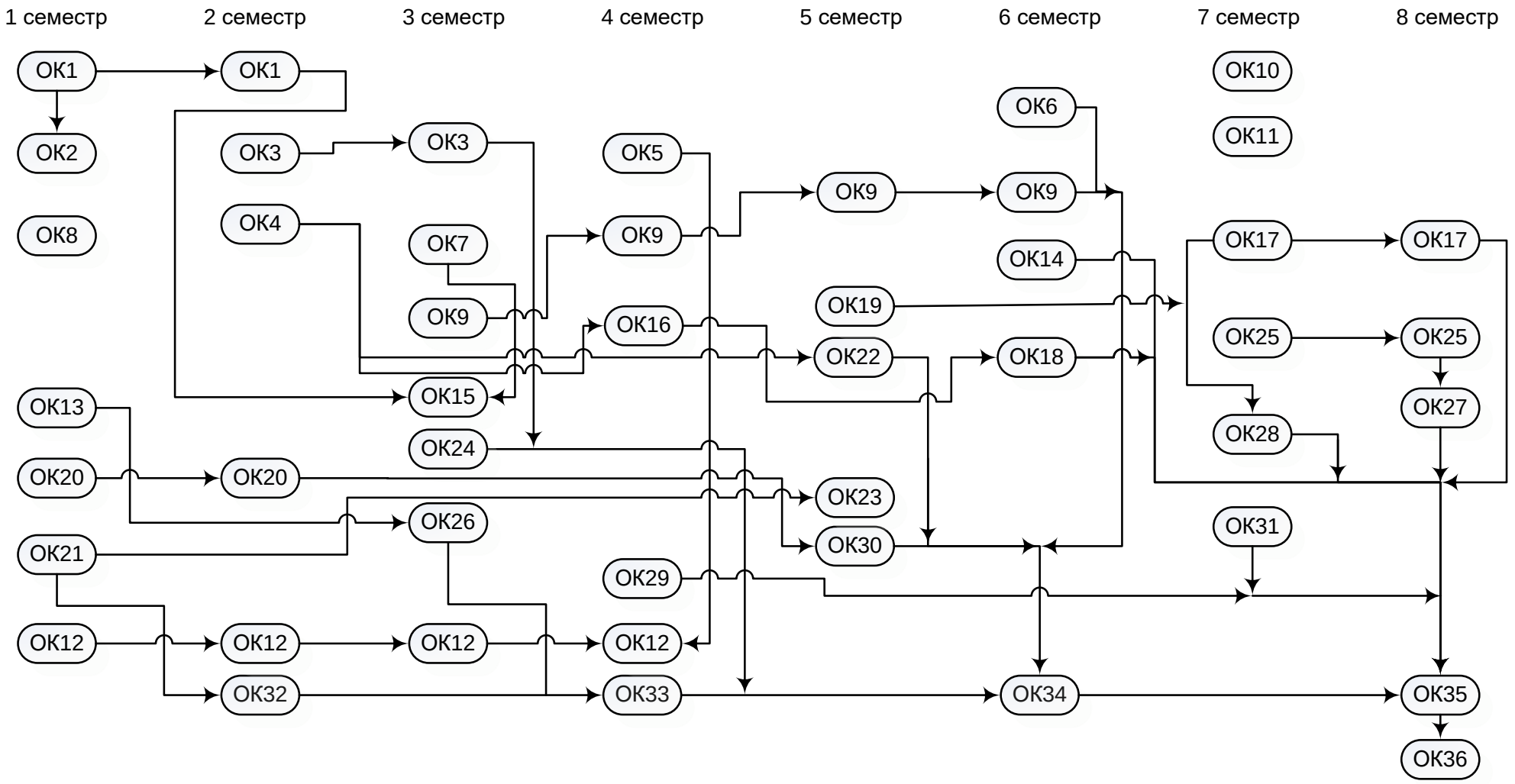
## 2. Перелік компонент освітньо-професійної програми «Кібербезпека та захист інформації» та їх логічна послідовність

### 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 | 9 | Екзамен, Залік |
| ОК2. | Фізика | 4 | Екзамен |
| ОК3. | Програмування | 8 | Екзамен, Екзамен |
| ОК4. | Основи кібербезпеки | 4 | Екзамен |
| ОК5. | Безпека життєдіяльності і ПДР | 3 | Екзамен |
| **1.2 Обов'язкові компоненти ОПП за рішенням вченої ради університету** | | | |
| ОК6. | Українська мова за професійним спрямуванням | 4 | Залік |
| ОК7. | Дискретна математика | 4 | Екзамен |
| ОК8 | Історія української державності | 3 | Екзамен |
| ОК9 | Іноземна мова | 16 | Екзамен (2), Залік (2) |
| ОК10 | Філософія | 4 | Залік |
| ОК11 | Основи економіки та бізнесу | 4 | Залік |
| ОК12 | *Фізичне виховання (за рахунок вільного часу студентів)* | *0* | *Залік* |
| **2. ЦИКЛ СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ** | | | |
| **2.1 Обов'язкові компоненти ОПП** | | | |
| ОК13. | Вступ до фаху кібернетичної безпеки | 4 | Екзамен |
| ОК14. | Теорія ризиків | 6 | Екзамен |
| ОК15. | Теорія ймовірності та математична статистика | 4 | Екзамен |
| ОК16. | Захист програмного забезпечення | 4 | Екзамен |
| ОК17. | Комплексні системи захисту інформації | 6 | Екзамен, Екзамен |
| ОК18. | Організаційне забезпечення захисту інформації | 4 | Екзамен |
| ОК19. | Архітектура комп'ютерних систем | 4 | Екзамен |
| ОК20. | Комп'ютерні системи та мережі, їх безпека | 7 | Екзамен, Залік |
| ОК21. | Інформаційні технології | 4 | Екзамен |
| ОК22. | Криптографічний та стеганографічний захист | 6 | Екзамен |
| ОК23. | Операційні системи та їх безпека | 4 | Екзамен |
| ОК24. | Інженерія програмного забезпечення | 4 | Екзамен |
| ОК25. | Безпека безпровідних, мобільних та хмарних технологій | 7 | Екзамен |
| ОК26. | Теоретичні основи захисту інформації | 4 | Залік |
| ОК27. | Криптоаналіз | 6 | Екзамен |
| ОК28. | Технічний захист інформації | 4 | Екзамен |
| ОК29 | Бази даних та інформаційні системи | 4 | Екзамен, Залік |
| ОК30 | Аналіз шкідливого програмного забезпечення | 3 | Екзамен |
| ОК31. | Аналіз і моніторинг кібернетичної безпеки | 6 | Екзамен |
| ОК32. | Навчальна практика з програмування (комп'ютерна) | 6 | Залік |
| ОК33. | Виробнича практика (з технологій захисту інформації) | 6 | Залік |
| ОК34. | Виробнича практика (інженерна) | 6 | Залік |
| ОК35. | Передатестаційна практика | 6 | Залік |
| ОК36. | Єдиний державний кваліфікаційний іспит | 2 | Екзамен |
| **Загальний обсяг обов'язкових компонентів** | | **180** | |

| | | | |
|---|---|---|---|
| **3. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ**<br><br>*(Перелік вибіркових 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 вибіркових компонентів** | | **60** | |
| **ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ** | | **240** | |

**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 125 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 125 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **КЗ1** | | + | + | + | | | + | | | | | | | + | + | + | + | + | + | + | + | + |
| **КЗ2** | | | + | + | | | | | | | | | + | + | + | + | + | + | + | + | + | + |
| **КЗ3** | | | | | | + | | | + | | | | | | | | | | | | | |
| **КЗ4** | | | + | + | | | | | | | | | + | + | + | + | + | + | + | + | + | + |
| **КЗ5** | | | + | + | | | | | | | | | + | + | + | + | + | + | + | + | + | + |
| **КЗ6** | | | | | | | | + | | + | | | | | | | | | | | | |
| **КЗ7** | | | | | + | | | | | | | + | + | | | | | | | | | |
| **КЗ8** | + | + | + | + | | | + | | | + | + | + | + | + | + | + | + | + | + | + | + | + |
| **ФК1** | | | | + | | | | | | | | | + | | | | | | | | | + |
| **ФК2** | | | | | | | | | | | | | | | | | | | | | + | |
| **ФК3** | | | | | | | | | | | | | | | | | + | | + | | + | |
| **ФК4** | | | | | | | | | | | | | | | | + | + | + | | | | |
| **ФК5** | | | | | | | | | | | | | | + | | + | + | + | | | | + |
| **ФК6** | | | | | | | | | | | | | | | | + | + | | | | | |
| **ФК7** | | | | | | | | | | | | | | + | | + | + | + | | | | + |
| **ФК8** | | | | | | | | | | | | | | | | | | | | | | |
| **ФК9** | | | | | | | | | | | | | | | | | | | | | | |
| **ФК10** | | | | | | | | | | | | | | | | + | | | | | | + |
| **ФК11** | | | | | | | | | | | | | | | | | | | | | | |
| **ФК12** | | | | | | | | | | | | | | + | | | | | | | | |
| **ФК13** | | | + | | | | | | | | | | | | | + | + | | | | | |

| | ОК23 | ОК24 | ОК25 | ОК26 | ОК27 | ОК28 | ОК29 | ОК30 | ОК31 | ОК32 | ОК33 | ОК34 | ОК35 | ОК36 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **К31** | + | + | + | + | + | + | + | + | + | + | + | + | + | + |
| **К32** | + | + | + | + | + | + | + | + | + | + | + | + | + | + |
| **К33** | | | | | | | | | | | | | | |
| **К34** | + | + | + | + | + | + | + | + | + | + | + | + | + | + |
| **К35** | + | + | + | + | + | + | + | + | + | + | + | + | + | + |
| **К36** | | | | | | | | | | | | | | |
| **К37** | | | | | | | | | | | | | | |
| **К38** | + | + | + | + | + | + | + | + | + | + | + | + | + | + |
| **ФК1** | | | | | | | | | | | | | | |
| **ФК2** | | | | + | | | | | | | | | | |
| **ФК3** | | | | | | | | | | | | | | |
| **ФК4** | | | | | | | | | | | | | | |
| **ФК5** | + | | + | | + | + | | + | | | | | | |
| **ФК6** | | | + | | | + | | + | | | | | | |
| **ФК7** | | | + | + | + | + | + | + | + | + | + | + | | |
| **ФК8** | | | + | | | | | + | | | | | | |
| **ФК9** | | | | | | | | | + | + | + | + | | |
| **ФК10** | | | | | | + | | | | + | + | + | | |
| **ФК11** | | | | | | | | | + | | | | | |
| **ФК12** | | | | | | | | | + | | | | | |
| **ФК13** | | + | | | | + | | | | | | | | |

## 5. Матриця забезпечення програмних 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ПРН1** | | | | | | + | | | + | | | | | | | | | | | | | |
| **ПРН2** | | | | | + | | | | | | | | | + | | + | + | + | + | + | + | + |
| **ПРН3** | | | | + | | | | | | | | | | | | + | + | + | + | + | + | + |
| **ПРН4** | | | | | | | | | | | | | | + | | | | | | | | |
| **ПРН5** | | | | | | | | | | | | | | + | + | | | | | | + | + |
| **ПРН6** | | | | | | | | | | | | | | + | + | | | | | | | |
| **ПРН7** | | | | | | | | | | | | | + | | | | | | | | | |
| **ПРН8** | | | | | | | | | | | | | | | | | | | | | | |
| **ПРН9** | | | | | | | | | | | | | | | | | | | | | | |
| **ПРН10** | | | | | | | | | | | | | | | | | | | | + | + | |
| **ПРН11** | | | | | | | | | | | | | | | | | | | | + | + | |
| **ПРН12** | | | | | | | | | | | | | | | | | + | + | | | | |
| **ПРН13** | | | | | | | | | | | | | | | | | | | | + | + | |
| **ПРН14** | | | | | | | | | | | | | | | | + | + | | + | | | |
| **ПРН15** | | | | | | | | | | | | | | | | + | + | | + | + | + | |
| **ПРН16** | | | | | | | | | | | | | | | | | + | | + | + | + | |
| **ПРН17** | | | | | | | | | | | | | | | | + | + | + | + | + | + | + |
| **ПРН18** | | | | | | | | | | | | | | | | + | + | | | | | + |
| **ПРН19** | | | | | | | | | | | | | | | | + | + | | | | | + |
| **ПРН20** | | | | | | | | | | | | | | | | + | + | | | | | + |
| **ПРН21** | | | | | | | | | | | | | | | | | + | + | | | | |
| **ПРН22** | | | | | | | | | | | | | | | | | + | + | | | | |
| **ПРН23** | | | | | | | | | | | | | | | | | + | + | | | | |
| **ПРН24** | | | | | | | | | | | | | | | | | + | + | | | | |

| | ОК1 | ОК2 | ОК3 | ОК4 | ОК5 | ОК6 | ОК7 | ОК8 | ОК9 | ОК10 | ОК11 | ОК12 | ОК13 | ОК14 | ОК15 | ОК16 | ОК17 | ОК18 | ОК19 | ОК20 | ОК21 | ОК22 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ПРН25** | | | | | | | | | | | | | | | | | + | + | | | | |
| **ПРН26** | | | | | | | | | | | | | | | | | + | + | | + | + | |
| **ПРН27** | | | | | | | | | | | | | | | | | | | | + | + | |
| **ПРН28** | | | | | | | | | | | | | | | | | | | | | | |
| **ПРН29** | | | | | | | | | | | | | | + | | | + | | | | | + |
| **ПРН30** | | | | | | | | | | | | | | + | | | + | | | | | |
| **ПРН31** | | | | | | | | | | | | | + | | | + | + | + | | | | + |
| **ПРН32** | | | | | | | | | | | | | | | | | + | + | | | | |
| **ПРН33** | | | | | | | | | | | | | | + | | | | | | | | |
| **ПРН34** | | | | | | | | | | | | | | | | | | + | | | | |
| **ПРН35** | | | | | | | | | | | | | | | | | + | + | | | | |
| **ПРН36** | | | | | | | | | | | | | | | | | | | | | | |
| **ПРН37** | | | | | | | | | | | | | | | | | | | | | | |
| **ПРН38** | | | | | | | | | | | | | | | | | | | | | | |
| **ПРН39** | | | | | | | | | | | | | | | | | | | | | | |
| **ПРН40** | | | | | | | | | | | | | | | | | | | | | | |
| **ПРН41** | | | | | | | | | | | | | | | | | | + | | | | |
| **ПРН42** | | | | | | | | | | | | | | | | | | + | | | | |
| **ПРН43** | | | | + | + | | | | | | | | + | | | | | | | | | |
| **ПРН44** | | | | + | + | | | | | | | | | + | | | + | | | | | |
| **ПРН45** | | | | | | | | | | | | | | + | | | | + | | | | |
| **ПРН46** | | | | | | | | | | | | | | + | | | | | | | | |
| **ПРН47** | | | | | | | | | | | | | | | | | + | | | | | + |
| **ПРН48** | | | | | | | | | | | | | | | | | | | | | | |
| **ПРН49** | | | | | | | | | | | | | | | | | | | | | | |

| | ОК1 | ОК2 | ОК3 | ОК4 | ОК5 | ОК6 | ОК7 | ОК8 | ОК9 | ОК10 | ОК11 | ОК12 | ОК13 | ОК14 | ОК15 | ОК16 | ОК17 | ОК18 | ОК19 | ОК20 | ОК21 | ОК22 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ПРН50** | | | | | | | | | | | | | | | | | | | | | | |
| **ПРН51** | | | | | | | | | | | | | | | | | + | | | | | |
| **ПРН52** | | | | | | | | | | | | | | | | | | | | | | |
| **ПРН53** | | | + | | | | | | | | | | | | | | | | | | | |
| **ПРН54** | | | | | + | | | | | | | | | | | | | | | | | |
| **ПРН55** | + | + | | + | | | + | | | | | | | + | + | | | | | | | |

| | ОК23 | ОК24 | ОК25 | ОК26 | ОК27 | ОК28 | ОК29 | ОК30 | ОК31 | ОК32 | ОК33 | ОК34 | ОК35 | ОК36 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ПРН1** | | | | | | | | | | | | | | |
| **ПРН2** | + | | | | + | + | | + | + | | | | | |
| **ПРН3** | + | | + | + | + | + | + | + | + | + | + | + | + | + |
| **ПРН4** | | | | | | | | | + | | | | | |
| **ПРН5** | | | | | + | | | | | | | | | |
| **ПРН6** | | | | | | | | | | | | | | |
| **ПРН7** | | | | | | | | | | | | | | |
| **ПРН8** | | | | | + | | | | | | | | | |
| **ПРН9** | | | | | + | | | | | | | | | |
| **ПРН10** | | | | | | | | | | | | | | |
| **ПРН11** | | | | | | | | | | | | | | |
| **ПРН12** | | | + | + | | | | | | | | | | |
| **ПРН13** | | | | | | | | | | | | | | |
| **ПРН14** | | | | | | + | | | | | | | | |
| **ПРН15** | | | | | | | | | | | | | | |
| **ПРН16** | | | | | | | | | | + | + | + | | |
| **ПРН17** | + | | + | + | + | + | + | + | + | | | | | |
| **ПРН18** | + | | + | | | | | + | | | | | | |
| **ПРН19** | + | | + | | | | | + | | | | | | |
| **ПРН20** | + | | + | | | | | + | | | | | | |
| **ПРН21** | | | | | | | | | | | | | | |
| **ПРН22** | | | | | | | | | | | | | | |

| | ОК23 | ОК24 | ОК25 | ОК26 | ОК27 | ОК28 | ОК29 | ОК30 | ОК31 | ОК32 | ОК33 | ОК34 | ОК35 | ОК36 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ПРН23** | | | | | | | | | | | | | | |
| **ПРН24** | | | | | | | | | | | | | | |
| **ПРН25** | | | | | | | | | | | | | | |
| **ПРН26** | | | | | | | | | | | | | | |
| **ПРН27** | | | | | | + | | | | | | | | |
| **ПРН28** | | | | | | | | | + | + | + | + | | |
| **ПРН29** | | | | | | | | + | + | | | | | |
| **ПРН30** | | | | | | | | + | + | | | | | |
| **ПРН31** | + | | + | + | + | | | + | | | | | | |
| **ПРН32** | | | + | + | | + | + | + | | | | | | |
| **ПРН33** | | | | | | | | | | | | | | |
| **ПРН34** | | | | | | | | | | | + | + | | |
| **ПРН35** | | | | | | | | | | | | | | |
| **ПРН36** | | | | | | + | | | | | | | | |
| **ПРН37** | | | | | | + | | | | | | | | |
| **ПРН38** | | | | | | + | | | + | | | | | |
| **ПРН39** | | | | | | | | | + | | | | | |
| **ПРН40** | | | | | | + | | | + | | | | | |
| **ПРН41** | | | | | | | + | | | | | | | |
| **ПРН42** | | | | | | | | | + | | | | | |
| **ПРН43** | | | | | | | | | | | | | | |
| **ПРН44** | | | | | | | | | | | | | | |
| **ПРН45** | | | | | | | | | | | | | | |
| **ПРН46** | | | | | | | + | | | | | | | |
| **ПРН47** | | | | | | | | | | | | | | |
| **ПРН48** | | | | | | | | + | | | | | | |
| **ПРН49** | | | | | | | | | + | | + | + | | |
| **ПРН50** | | | | | | + | | | | | | | | |
| **ПРН51** | | | | | | + | | | + | | | | | |
| **ПРН52** | | | | | | | | | + | | | | | |
| **ПРН53** | | + | | | | | | | | + | | | | |
| **ПРН54** | | | | | | | | | | | | | | |
| **ПРН55** | | | | | | | | | | | | | | |

## 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, 2021. – 53 с. [Режим доступу: https://btu.kharkov.ua/pro-universitet/publichna-informatsiya/normatyvna-baza/];
8. . Положення про організацію освітнього процесу з використанням дистанційних технологій, Харків, 2022. – 13 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 125 «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