Міністерство освіти і науки України
Вінницький національний технічний університет

ЗАТВЕРДЖУЮ
Ректор Вінницького національного технічного університету
_____ В. В. Грабко
(підпис)
«___» _____ 2016 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ БАКАЛАВРІВ

за спеціальністю 125 – Кібербезпека
І (бакалаврський) рівень вищої освіти

Назва освітньо-професійної програми «Безпека інформаційних і комунікаційних систем»

(освітньо-професійна програма затверджена Вченою радою
Вінницького національного технічного університету
протокол № 14 від 23.06.2016 р.)

Галузь науки – 12 Інформаційні технології
Кваліфікація – Бакалавр з кібербезпеки

Термін навчання – 3 роки 10 місяців
Форма навчання – денна та заочна

Передмова

1. РОЗРОБЛЕНО у Вінницькому національному технічному університеті кафедрою захисту інформації (ЗІ) .

2. ВНЕСЕНО Вінницьким національним технічним університетом

3. ВВЕДЕНО вперше

4. РОЗРОБНИКИ

1. Лужецький Володимир Андрійович, ВНТУ, д.т.н., професор, завідувач кафедри захисту інформації.

2. Войтович Олеся Петрівна, ВНТУ, к.т.н., доцент, доцент кафедри захисту інформації.

3. Дудатьєв Андрій Веніамінович, ВНТУ, к.т.н., доцент, доцент кафедри захисту інформації.

Зміст

ВСТУП

Освітня програма (далі – ОП) підготовки бакалаврів за спеціальністю 125 «Кібербезпека» розроблена з врахуванням пропозицій Науково-методичної ради Міністерства освіти і науки України, Науково-методичної підкомісії за спеціальністю 125 – «Кібербезпека», галузевих об’єднань роботодавців.

Освітньо-професійна програма (далі ОП) підготовки бакалавра за спеціальністю 125 «Кібербезпека» розроблена на виконання наказу Міністерства освіти і науки України від 06.11.2015 № 1151 «Про особливості запровадження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету міністрів України від 29 квітня 2015 року № 266» з урахуванням вимог статті 10 Закону України «Про вищу освіту».

При розробленні ОП підготовки бакалавра врахована Таблиця відповідності переліку напрямів, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітнім рівнем бакалавр (перелік 2006 р.) та переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти (перелік 2015 р.).

У зв’язку із відсутністю стандартів вищої освіти для спеціальностей за переліком 2015 р., у процесі розроблення ОП використані чинні галузеві стандарти з врахуванням пропозицій Науково-методичної ради Міністерства освіти і науки України, Науково-методичної підкомісії за спеціальністю 125 – «Кібербезпека», галузевих об’єднань роботодавців.

Освітня програма підготовки бакалавра за спеціальністю 125 «Кібербезпека» розроблена колективом професорсько-викладацького складу кафедри захисту інформації факультету інформаційних технологій та комп’ютерної інженерії Вінницького національного технічного університету.

1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь, що присвоюється	Бакалавр
Назва галузі знань	12 Інформаційні технології
Назва спеціальності	125 Кібербезпека
Обмеження щодо форм навчання	Денна, заочна
Кваліфікація освітня, що присвоюється	бакалавр з кібербезпеки
Опис предметної області	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. Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки . Теоретичний зміст предметної діяльності 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 та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації. Методи, методики та технології: Методи, методики та технології забезпечення інформаційної та/ або кібербезпеки Інструменти та обладнання: – системи розробки, забезпечення, моніторингу та контролю інформаційної та/ або кібербезпеки.
Академічні права випускників	Можливість продовжити навчання за освітньо-професійною або освітньо-науковою програмою ступеня магістра

Працевлаштування випускників

У відповідності з чинним Класифікатором професій ДК 003:2010 зі змінами від березня 2016 передбачається функціональна підготовка для роботи за професіями, вказаними за ДК 003:2010, в таблиці:

КОД КП	КОД ЗКППТР	ВИПУСК ДКХП	Професійна назва роботи
3439			Фахівець із організації інформаційної безпеки
3439			Фахівець із організації захисту інформації з обмеженим доступом

2 ОБСЯГ КРЕДИТІВ ЄКТС, НЕОБХІДНИЙ ДЛЯ ЗДОБУТТЯ ВІДПОВІДНОГО СТУПЕНЯ ВИЩОЇ ОСВІТИ

Перший (бакалаврський) рівень вищої освіти відповідає шостому кваліфікаційному рівню Національної рамки кваліфікацій і передбачає здобуття особою теоретичних знань та практичних умінь і навичок, достатніх для успішного виконання професійних обов'язків за обраною спеціальністю.

Для здобуття ступеня бакалавра на основі ступеня молодшого бакалавра або освітньо-кваліфікаційного рівня молодшого спеціаліста ВНЗ має право скорочувати обсяг освітньої програми. При цьому програма має забезпечувати

набуття визначених цим стандартом результатів навчання, а її загальний обсяг має бути не меншим, ніж 120 кредитів.

3 ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ БАКАЛАВРА

Для успішного виконання професійних обов'язків за обраною спеціальністю у процесі навчання у бакалавра повинні бути сформовані загальні та професійні компетентності.

Згідно із Законом України «Про вищу освіту», компетентність – це динамічна комбінація знань, вмінь і практичних навичок, способів мислення, професійних, світоглядних і громадянських якостей, морально-етичних цінностей, яка визначає здатність особи успішно здійснювати професійну та подальшу навчальну діяльність і є результатом навчання на певному рівні вищої освіти. Особливістю компетентностей є те, що вони набуваються поступово, формуються цілою низкою навчальних дисциплін або модулів на різних етапах даної програми і, які мають описані нижче функціональні призначення.

3.1. Інтегральні компетенції

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки, що характеризується комплексністю та неповною визначеністю умов.

3.2. Загальні компетентності

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
КЗ 2. Знання та розуміння предметної області та розуміння професії.
КЗ 3. Здатність спілкуватися рідною та іноземною мовою як усно, так і письмово
КЗ 4. Вміння виявляти, ставити та вирішувати проблеми.
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ 6. Навички міжособистісної взаємодії.
КЗ 7. Прагнення до збереження навколишнього середовища
КЗ 8. Здатність діяти соціально відповідально та громадянсько свідомо.
КЗ 9. Здатність вчитися і бути сучасно навченим.
КЗ 10. Здатність приймати обґрунтовані рішення.
КЗ 11. Здатність до адаптації та дії в новій ситуації.
КЗ 12. Дотримання та пропагування здорового способу життя.
КЗ 13. Здатність бути критичним та самокритичним

3.3. Фахові компетентності

КФ 1. Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності.
КФ 2. Здатність до використання інформаційних і комунікаційних технологій з метою пошуку нової інформації, створення баз даних, аналізу розподілених інформаційно-комунікаційних систем, каналів зв'язку, систем управління

процесами, баз даних, оперативного планування роботи систем на основі аналізу інформаційних потоків та їх оптимізації.
КФ 3. Здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної та кібербезпеки
КФ 4. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки.
КФ 5. Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
КФ 7. Здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС
КФ 8. Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення з забезпечення кібербезпеки
КФ 9. Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою
КФ 10. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку
КФ 11. Здатність здійснювати управління ризиками інформаційної та кібербезпеки
КФ 12. Здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій
КФ 13. Здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники
КФ 14. Розуміння дії економічних законів в різних економічних моделях розвитку та здатність до аналізу і моніторингу економічної діяльності різних підприємств та організацій
КЗ 15. Здатність здійснювати професійну діяльність згідно з вимогами санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки

4 НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ, СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ

4.1. Результати навчання за загальними компетентностями:

- застосовувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки;
- проектувати майбутню професійну діяльність з урахуванням її значущості для громадянина та держави,а також напрямків розвитку інформаційної та кібербезпеки;
- застосовувати знання державної та однієї з іноземних мов з метою забезпечення ефективності професійної комунікації;

- організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблему професійній діяльності, оцінювати їхню ефективність;

- використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

- дотримуватись норм міжособистісного спілкування у професійній взаємодії;

- прогнозувати наслідки результатів діяльності людини з метою збереження навколишнього середовища;

- використовувати історичну спадщину та культурні традиції свого народу для професійного зростання, саморозвитку, самовдосконалення;

- вдосконалювати професійний та особистісний розвиток протягом усього життя;

- 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;

- адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

- демонструвати та пропагуватиздоровий спосіб життя;

- критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності

4.2. Результати навчання за фаховими компетентностями:

- діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних, в галузі інформаційної та /або кібербезпеки;

- готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

- впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

- виконувати аналіз та декомпозицію ІТС;

- виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;

- розробляти моделі загроз та порушника;

- аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних;

- вирішувати завдання захисту програм та інформації, що обробляється в ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень;

- реалізовувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативно-правових документів;

- 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 ;

- використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
- застосовувати теорії та методи захисту для забезпечення безпеки інформації в ІТС;
- забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС ;
- вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в ІТС згідно встановленої політики інформаційної і\або кібербезпеки;
- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
- 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..
- впроваджувати заходи та забезпечувати реалізацію процесів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
- вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
- аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;
- виконувати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в ІТС та ефективності використання КЗЗ в умовах реалізації загроз різних класів.
- здійснювати оцінювання можливості несанкціонованого доступу до елементів ІТС.;
- застосовувати теорії та методи захисту для забезпечення безпеки елементів ІТС
- вирішувати задачі управління процесами відновлення штатного функціонування ІТС з використанням процедур резервування згідно встановленої політики безпеки;
- вирішувати задачі забезпечення неперервності бізнес процесів організації;

- приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

- 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;

- виявляти небезпечні сигнали технічних засобів;

- вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації;

- інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів щодо технічного захисту інформації;

- проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах

- забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур

- впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;

- застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів

- вирішувати задачі забезпечення неперервності бізнес процесів організації на основі встановленої системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів;

- застосовувати політики, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

- здійснювати аналіз ризиків обробки інформації в ІТС;

- вирішувати задачі захисту інформації, що обробляється в ІТС з використанням сучасних методів та засобів криптографічного захисту інформації;

- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в ІТС.

- забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в ІТС;

- забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);

- забезпечувати конфігурування та роботоспроможність систем виявлення вторгнень в ІТС;

- використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;

- вирішувати задачі аналізу програмного коду на наявність можливих вразливостей;

- вирішувати задачі забезпечення неперервності бізнес процесів організації;

- володіння техніками і методами організації і менеджменту виробничих колективів

- дотримуватись вимог санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки при здійсненні професійної діяльності

5 НОРМАТИВНІЙ ЗМІСТ ПІДГОТОВКИ БАКАЛАВРА

Обсяг освітньої програми бакалавра:

- на базі повної загальної середньої освіти з терміном навчання 11 років – 240 кредитів ЄКТС;
- на базі повної загальної середньої освіти з терміном навчання 12 років – 180-240 кредитів ЄКТС;
- на базі ступеня молодшого бакалавра (ОКР молодший спеціаліст) – 120 кредитів ЄКТС.

ВНЗ має право скорочувати обсяг освітньої програми. При цьому програма має забезпечувати набуття визначених результатів навчання, а її загальний обсяг має бути не меншим, ніж 120 кредитів.

Мінімум 75% обсягу освітньої програми має бути спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю 125 «Кібербезпека».

Освітня програма підготовки бакалавра передбачає такі цикли підготовки:

- цикл загальної підготовки,
- цикл фахової підготовки.

6 ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ СТУПЕНЯ БАКАЛАВРА

Згідно із Законом України «Про вищу освіту», здобуття вищої освіти на кожному рівні передбачає успішне виконання особою відповідної освітньої програми, що є підставою для присудження відповідного ступеня вищої освіти.

Підсумкова атестація осіб, які здобувають ступінь бакалавра, здійснюється екзаменаційною комісією, до складу якої можуть включатися представники роботодавців та їх об’єднань, в терміни, передбачені навчальним планом згідно із Положенням про порядок створення, організацію і роботу екзаменаційної комісії у ВНТУ. Положення регламентує:

- завдання екзаменаційної комісії;
- склад та розклад роботи екзаменаційної комісії;
- процедуру роботи екзаменаційної комісії;
- підбиття підсумків роботи екзаменаційної комісії щодо атестації здобувачів вищої освіти.

Результати атестації визначаються оцінками за національною шкалою «відмінно», «добре», «задовільно», «незадовільно».

Форма випускової атестації – атестація здійснюється у формі публічного захисту кваліфікаційної роботи на відкритому засіданні екзаменаційної комісії.

Вимоги до випускової кваліфікаційної роботи

Кваліфікаційна робота має передбачати дослідження та розв’язання спеціалізованого завдання або практичної задачі в галузі інформаційної та/або кібербезпеки.

7 ХАРАКТЕРИСТИКА СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ПІДГОТОВКИ БАКАЛАВРА

У Вінницькому національному технічному університеті функціонує система забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

- визначення принципів та процедур забезпечення якості вищої освіти;
- здійснення моніторингу та періодичного перегляду освітніх програм;
- щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті ВНТУ, на інформаційних стендах та в будь-який інший спосіб;
- забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;
- забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі, самостійної роботи студентів;
- забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;
- забезпечення публічності інформації;
- забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників вищих навчальних закладів і здобувачів вищої освіти;
- інших процедур і заходів.

7.1. Принципи та процедури забезпечення якості вищої освіти

Систему забезпечення якості вищої освіти (система внутрішнього забезпечення якості) розроблена згідно із принципами:

- відповідності європейським та національним стандартам якості вищої освіти;
- автономії вищого навчального закладу, який несе відповідальність за забезпечення якості освітньої діяльності та якості вищої освіти;
- органічне поєднання в освітньому процесі освітньої, наукової та інноваційної діяльності;
- відкритості та доступності інформації на всіх етапах забезпечення якості;
- безперервності освіти, яка відкриває можливість для постійного поглиблення загальноосвітньої та фахової підготовки,
- нероздільності навчання і виховання, що полягає в їх органічному поєднанні;
- варіативності освіти, що передбачає запровадження варіативного компоненту змісту освіти, диференціацію та індивідуалізацію освітнього процесу.

Система забезпечення якості вищої освіти (система внутрішнього забезпечення якості) передбачає процедури:

- здійснення на високому рівні освітньої діяльності, яка відповідає стандартам якості вищої освіти, забезпечує здобуття особами ступеню бакалавра за спеціальністю 125 «Кібербезпека»;

- створення необхідних умов для реалізації учасників освітнього процесу їхніх здібностей і талантів;
- збереження естетичних норм життя, культурних, наукових цінностей і досягнень суспільства;
- провадження наукової, творчої, мистецької, культурно-виховної діяльності, забезпечення культурного та духовного розвитку;
- налагодження міжнародних зв'язків в галузі освіти, науки;
- вивчення попиту на спеціальність 125 «Кібербезпека» на ринку праці та сприяння працевлаштуванню випускників;
- формування інноваційного освітньо-виховного середовища;
- впровадження новітніх технологій для підвищення якості вищої освіти,
- оприлюднення на офіційному веб-сайті, на інформаційних стендах та в будь-який інший спосіб інформації про реалізацію своїх прав і виконання зобов'язань;
- участь у національних та міжнародних рейтингових дослідженнях вищих навчальних закладів.

7.2. Моніторинг та періодичний перегляд освітніх програм

Забезпечення високої якості професійної підготовки бакалаврів спеціальності 125 «Кібербезпека» передбачає здійснення процедур затвердження, періодичного перегляду та моніторингу освітньої програми.

Навчальні програми з дисциплін розроблені випусковою кафедрою захисту інформації ВНТУ згідно чинних вимог.

У ВНТУ здійснюється робота над вдосконаленням та адаптацією освітньої програми, підвищенням якості вищої освіти відповідно до сучасних вимог та потреб суспільства.

7.3. Оцінювання здобувачів вищої освіти

Для оцінювання рівня знань, умінь, компетентностей, навичок, професійних, світоглядних та інших особистих якостей здобувачів ступеню бакалавра використовуються засоби діагностики якості вищої освіти під час проведення атестації. Вимоги до засобів діагностики при проведенні атестації здобувачів вищої освіти орієнтуються на рівень сформованості професійних компетентностей, що визначені у освітній програмі.

Формами проміжної атестації фахівців спеціальності 125 «Кібербезпека» є залік, виконання індивідуальних завдань, екзамен, захист випускової роботи.

Оцінювання здобувачів ступеню бакалавра відбувається згідно Порядку оцінювання знань здобувачів вищої освіти у Вінницькому національному технічному університеті. Кредитно-модульна система використовується з метою покращення функціональних характеристик освітнього процесу, а саме: підвищення зацікавленості здобувачів вищої освіти до освітнього процесу, стимулювання їх систематичної та самостійної роботи, підвищення об'єктивності оцінки знань та вмінь, відповідальність за результати навчання. Дана система формується на засадах накопичення кредитів за різноманітну навчальну діяльність студента за певний період навчання.

Контроль за якістю знань відбувається згідно із Тимчасовим положенням про

кредитно-модульну систему організації навчального процесу у ВНТУ. Положення унормовує організацію поточного та підсумкового семестрового контролю знань та вмінь студентів, проведення практик і атестації та регламентує критерії оцінювання знань і вмінь студентів згідно зі шкалою оцінювання відповідності підсумкових оцінок у балах (100-бальна шкала, національна шкала та шкала ECTS).

7.4. Підвищення кваліфікації педагогічних і науково-педагогічних працівників

Підвищення кваліфікації науково-педагогічних і педагогічних працівників здійснюється згідно із Положенням про підвищення кваліфікації, стажування та атестацію науково-педагогічних працівників ВНТУ, яке передбачає підвищення кваліфікації та стажування науково-педагогічних і педагогічних працівників не рідше одного разу на п’ять років.

Результати підвищення кваліфікації та проходження стажування враховуються під час проведення атестації науково-педагогічних і педагогічних працівників та під час обрання на посаду за конкурсом чи укладання трудового договору з науково-педагогічним працівником.

Підвищення рівня наукової та педагогічної підготовки працівників ВНЗ може здійснюватися у таких формах:

- написання та захист кандидатських, докторських дисертацій;
- навчання в аспірантурі, докторантурі;
- проходження курсів підвищення кваліфікації;
- публікація наукових, методичних і творчих робіт;
- участь у наукових конференціях (виступи з доповідями, публікація тез, обговорення їх на засіданнях кафедр);
- участь у науково-теоретичних та науково-практичних семінарах та форумах з актуальних проблем сучасного стану освіти;
- участь у роботі журі конкурсів;
- участь у роботі виконавсько-педагогічних семінарів, курсів майстерності (проведення відкритих занять, керівництво секціями).

Підвищення кваліфікації здійснюється згідно з планом, який складається на календарний рік та затверджується проректором з навчальної роботи.

Система оцінювання роботи науково-педагогічних і педагогічних працівників проводиться відповідно до Положення про рейтингове оцінювання діяльності науково-педагогічних і педагогічних працівників ВНТУ.

Усі види роботи та відведені на них години відображені у індивідуальному плані роботи науково-педагогічного працівника на навчальний рік, який складається перед початком кожного навчального року.

Оцінювання професійної діяльності науково-педагогічних і педагогічних працівників проводиться наприкінці кожного навчального року.

Інформація щодо результатів оцінювання роботи науково-педагогічних і педагогічних працівників використовується під час розподілу навчального навантаження на новий навчальний рік, під час участі в конкурсі на заміщення вакантних посад, прийняття рішення щодо продовження (визначення терміну)

трудових відносин, для матеріального і морального стимулювання. Результати оцінювання науково-педагогічних і педагогічних працівників оприлюднюється на офіційному веб-сайті ВНТУ наприкінці навчального року.

7.5. Наявність необхідних ресурсів для організації освітнього процесу

ВНТУ гарантує, що наявні ресурси, які забезпечують освітній процес, є достатніми і відповідають змісту освітньої програми підготовки зі спеціальності 125 «Кібербезпека».

До кожної навчальної дисципліни розроблені навчальні програми, робочі навчальні програми, плани семінарських, практичних занять, завдання для самостійної підготовки студентів, методичні вказівки до семінарських та практичних занять, методичне забезпечення контролю знань студентів (контроль поточних та залишкових знань), методичні матеріали для студентів з питань самостійного опрацювання фахової літератури, критерії оцінювання знань і вмінь студентів, методичне забезпечення атестації.

Інформаційне забезпечення складають бібліотечні фонди, можливість роботи у мережі Інтернет, робота власного сайту тощо.

Бібліотека ВНТУ має приміщення для розташування книгосховищ, каталогів, абонементи, читальні зали, які обладнані комп'ютерами, що дає можливість користуватися мережею Інтернет.

У ВНТУ функціонують навчальні лабораторії, обладнані комп'ютерами, на яких встановлено ліцензійне програмне забезпечення. Студенти мають доступ до мережі Інтернет.

7.6. Публічність інформації про освітні програми, ступені вищої освіти та кваліфікації

Діяльність і рішення ВНТУ у сфері вищої освіти обов'язково оприлюднюється на офіційному веб-сайті та у засобах інформації, на інформаційних стендах та у інші способи.

ВНТУ має веб-сайт, на якому розміщується інформація про освітню, науково-методичну, концертно-виконавську, організаційну та виховну діяльність. Надається інформація про ступені вищої освіти та кваліфікації, за якими відбувається навчання, забезпеченість освітніми програмами.

7.7. Запобігання та виявлення академічного плагіату

Основною функцією системи запобігання та виявлення академічного плагіату є підвищення якості навчання, розвиток навичок коректної роботи із джерелами інформації, необхідність самостійності та індивідуальності створення авторського твору. Метою впровадження системи запобігання та виявлення плагіату є формування вимог дотримання наукової етики, підвищення відповідальності науково-педагогічних, педагогічних працівників та здобувачів вищої освіти за виявлення плагіату у їхніх роботах.

Перевірка робіт студентів та науково-педагогічних і педагогічних працівників на унікальність та наявність у них плагіату у ВНТУ здійснюється за допомогою програм, які знаходяться у мережі Інтернет (ATutor, Antiplagiat, Anti-Plagiarism).

Перед перевіркою і допуском до доповіді чи захисту студентських навчальних робіт викладач попередньо перевіряє оригінальність електронних версій текстових документів цих робіт.

7.8. Підходи до навчання та викладання

Навчання студентів зі спеціальності 125 «Кібербезпека» здійснюється за навчальним планом освітнього рівня «бакалавр», що відповідає чинним вимогам Закону України «Про вищу освіту» і сучасним тенденціям розвитку освітнього процесу в Україні.

Даний план ґрунтується на науковій базі, новітніх теоретичних розробках та технологіях, вітчизняному й зарубіжному досвіді та спрямований на підготовку фахівців, які відповідають потребам ринку праці, насамперед, в регіональному масштабі.

Організація навчального процесу здійснюється відповідно до розкладу занять та графіка консультацій, які розробляються з урахуванням різноманітності академічного навантаження студентів, науково-педагогічних працівників, аудиторного фонду університету.

Наскрізний контроль навчальної роботи студентів передбачає:

– вхідний контроль знань студентів з дисциплін, які будуть вивчатися та які пов’язані між собою структурно-логічною схемою освітнього процесу зі спеціальності 125 «Кібербезпека»;

– поточний контроль знань, спрямований на визначення системності у вивченні студентами окремих тематик в рамках кожної з дисциплін протягом семестру і застосовується як засіб визначення рівня засвоєння компетенцій;

– модульний (міжсесійний) контроль, під час якого знання студентів оцінюються узагальненою оцінкою, що відповідає певній кількості балів, набраних під час оцінювання набутих компетенцій студентами з окремих модулів дисциплін, що викладаються;

– сесійний контроль, який відбувається у вигляді іспиту або диференційованого або недиференційованого заліку й може проводитись письмово чи комбіновано (усно-письмово). Зміст та структура білетів/завдань має комплексний характер та варіативність. Загальна оцінка з дисципліни виставляється з урахуванням оцінки модульного та поточного контролів, а також оцінки за іспит або залік;

– контрольна перевірка залишкових знань проводиться після здачі іспиту/заліку з визначених дисциплін у наступному семестрі або навчальному році.

Основними формами навчання та викладання є лекції, практичні заняття, семінари, лабораторні роботи в малих групах, самостійна робота з використанням підручників, навчальних посібників, методичних розробок та конспектів, консультації із викладачами, різноманітні активні методи навчання (ситуаційні вправи, ділові ігри, дискусії, виїзні заняття на діючих підприємствах).

Додатково застосовуються й розвиваються дистанційні форми навчання з окремих дисциплін.

Активно застосовується комп’ютерне забезпечення усіх видів занять.

Індивідуальна робота студентів згідно навчального плану спеціальності 125 «Кібербезпека» реалізується через форму виконання курсових проектів і робіт, розрахунково-графічних та розрахункових робіт, підготовку тематичних презентаційних програм.

Практична підготовка студентів здійснюється у лабораторіях, на навчальних полігонах університету та в лабораторіях, а також на виробництвах провідних виробничих підприємствах регіону.

Основними перспективами розвитку підходів до навчання, викладання та оцінювання рівня підготовки бакалаврів зі спеціальності 125 «Кібербезпека» є індивідуалізація навчання з виділенням таких напрямків:

– активне залучення студентів до наукової роботи кафедри та індивідуальної роботи в окремих наукових гуртках у різних напрямках під керівництвом викладачів випускової кафедри;

– участь у наукових семінарах, конференціях, олімпіадах, підготовка доповідей та наукових статей, починаючи з 1-2 курсу;

– комп'ютерна підготовка фахівців протягом всього періоду навчання, виконання завдань на практичних заняттях, індивідуальних завдань з курсового проектування за допомогою комп'ютерних технологій;

Для забезпечення відповідності набутих бакалаврами компетентностей і результатів навчання кваліфікації, що здобувається, в освітній процес впроваджуються такі форми навчання:

– реальне проектування в рамках курсових і випускових робіт (проектів), розробка зразків нової техніки та технологій, програмних засобів в галузі інформаційної та кібербезпеки;

– вивчення досвіду організації систем інформаційної та кібербезпеки на підприємствах регіону;

– направлення студентів на виробничі практики (після 3 і 4 курсу) на підприємства та в організації за місцем подальшої роботи.

Бакалавр зі спеціальності 125 «Кібербезпека» має право продовжити навчання з метою отримання вищих кваліфікаційних рівнів і наукових ступенів другого (магістерського), третього (освітньо-наукового) та наукового рівня вищої освіти.

В рамках освітнього процесу підготовки бакалаврів зі спеціальності 125 «Кібербезпека» передбачена система комплексної діагностики знань студентів, за якою виставлення загальної оцінки з дисципліни здійснюється з урахуванням оцінок, що отримані при здачі іспиту (заліку) та результатів поточного, модульного контролю знань студентів й оцінювання індивідуальних форм навчальної діяльності кожного студента протягом семестру (навчального року). Таким чином загальна оцінка визначається на підставі оцінювання усіх видів завдань, визначених робочою навчальною програмою кожної з дисциплін навчального плану. Така система стимулює систематичну самостійну роботу студентів, підвищує об'єктивність оцінки їх знань, виявляє й розвиває творчі здібності, створює здорову конкуренцію у навчанні.

В рамках освітнього процесу діє система рейтингової оцінки результатів діяльності студентів, метою якої є досягнення високого рівня знань, оволодіння

основами майбутньої спеціальності, дотримання здорового способу життя, активної життєвої позиції, забезпечує комплексну оцінку досягнень студентів у навчальній, науково-дослідній, громадській діяльності, культурно-масовій та спортивній роботі. Вона визначається за семестр, навчальний рік, весь період навчання наростаючим підсумком.

7.9. Розроблення системи оцінювання якості освітньої програми з метою її удосконалення

Реалізація освітньої програми зі спеціальності 125 «Кібербезпека» здійснюється в рамках діючої Європейської кредитно-трансферної системи (ЄКТС), яка розроблена для забезпечення мобільності студентів, спрощує розуміння і порівняння навчальних програм та досягнень студентів як між вітчизняними так й іноземними навчальними закладами.

Враховуючи положення системи ЄКТС, усі програми навчальних дисциплін й практик виражені в академічних кредитах.

Кредити ЄКТС відображають загальне навантаження студента при вивченні певного курсу або певної його частини (модулю). Вони також визначають, яку частину загального річного навчального навантаження займає даний курс (або модуль курсу) у ВНЗ, що визначає кредити.

Оскільки система ЄКТС базується на принципах взаємної довіри учасників освітнього процесу, то вона передбачає виконання правил застосування всіх її складових: кредитів ЄКТС; шкали оцінювання; угоди про навчання; інформаційних пакетів; академічної довідки оцінювання знань студента (додатка до диплому).

Шкала оцінювання використовується для спрощення переведення оцінок, отриманих за системою ЄКТС, національною системою і 100-бальною шкалою.

8 АКАДЕМІЧНА МОБІЛЬНІСТЬ

Індивідуальна академічна мобільність реалізується у рамках міжуніверситетських договорів про встановлення науково-освітянських відносин для задоволення потреб розвитку освіти і науки.

Допускається перезарахування кредитів, отриманих у інших навчальних закладах України, за умови відповідності їх набутим компетентностям.

Навчання іноземних здобувачів вищої освіти здійснюється на загальних умовах з додатковою мовною підготовкою.