ЗАТВЕРДЖУЮ
Ректор Державного вищого навчального закладу «Національний гірничий університет»

_____ Півняк І.Г

“___” _____ 2017 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ВИЩОЇ ОСВІТИ

ГАЛУЗЬ ЗНАНЬ	12 Інформаційні технології
СПЕЦІАЛЬНІСТЬ	125 Кібербезпека
РІВЕНЬ ВИЩОЇ ОСВІТИ	1-й
СТУПІНЬ	бакалавр
ПРОФЕСІЙНА КВАЛІФІКАЦІЯ	фахівець з кібербезпеки

Дніпро
НГУ
2017

Передмова

1. ВНЕСЕНО

кафедрою безпеки інформації та телекомунікацій Державного вищого навчального закладу «Національний гірничий університет»

2. ЗАТВЕРДЖЕНО

наказом ректора від «___» _____ 2017 р. №___.як тимчасовий документ до введення стандартів вищої освіти за спеціальністю.

3. ВВЕДЕНО ВПЕРШЕ

4. РОЗРОБНИКИ

КОРНІЄНКО ВАЛЕРІЙ ІВАНОВИЧ, доктор технічних наук, завідувач кафедри безпеки інформації та телекомунікацій
ГЕРАСІНА ОЛЕКСАНДРА ВОЛОДИМИРІВНА, кандидат технічних наук, доцент кафедри безпеки інформації та телекомунікацій
КАГАДІЙ ТЕТЯНА СТАНІСЛАВІВНА, доктор фізико-математичних наук, професор кафедри безпеки інформації та телекомунікацій
КРУЧІНІН ОЛЕКСАНДР ВОЛОДИМИРОВИЧ, старший викладач кафедри безпеки інформації та телекомунікацій
ТИМОФЄЄВ ДМИТРО СЕРГІЙОВИЧ, старший викладач кафедри безпеки інформації та телекомунікацій

Зав. каф. БІТ Корнієнко В.І.

Голова НМК зі спеціальності 125 Гер Герасіна О.В.

ЗМІСТ

1.	**Вступ**	4
1.1	**Загальні відомості**	4
1.2	**Нормативні посилання**	6
1.3	**Терміни та їх визначення**	6
1.4.	**Позначення**	9
2.	**Компетентності бакалавра кібербезпеки**	9
2.1	**Перелік компетентностей випускника**	9
2.2	**Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання**	10
3	**Вимоги до попереднього рівня освіти здобувачів**	18
4	**Обсяг програми та його розподіл за нормативною та вибірковою частинами**	18
5	**Розподіл змісту вищої освіти та кредитів за видами навчальної діяльності**	18
6	**Результати навчання та вимоги до структури програм дисциплін**	20
7	**Загальні вимоги до засобів діагностики**	20
8	**Структурно-логічна схема**	20
9	**Прикінцеві положення**	22

1. ВСТУП

1.1. Загальні відомості

Наказом МОН України від 06. 11. 2015 № 1151 «Про особливості запровадження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти», вищим начальним закладам запропоновано розробити та запровадити з 1-го вересня 2016 року освітні програми та навчальні плани згідно з вимогами Закону України «Про вищу освіту».

Для створення тимчасової освітньої програми використовувались такі положення Закону України «Про вищу освіту»:

1) за ст. 1, п. 1. 17 - освітня програма (освітньо-професійна, освітньо-наукова) – система освітніх компонентів на відповідному рівні вищої освіти в межах спеціальності, що визначає:

- вимоги до рівня освіти осіб, які можуть розпочати навчання за цією програмою;
- перелік навчальних дисциплін і логічну послідовність їх вивчення;
- кількість кредитів ЄКТС, необхідних для виконання цієї програми;
- очікувані результати навчання, якими повинен оволодіти здобувач відповідного ступеня вищої освіти;

2) за ст. 10, п. 3 - стандарт вищої освіти визначає такі вимоги до освітньої програми:

- обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти;
- перелік компетентностей випускника;
- нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання (сукупність знань, умінь, навичок, інших компетентностей);
- форми атестації здобувачів вищої освіти;
- вимоги до наявності системи внутрішнього забезпечення якості вищої освіти;

3) за ст. 5, п.1 - перший (бакалаврський) рівень передбачає здобуття особою теоретичних знань та практичних умінь і навичок, достатніх для успішного виконання професійних обов’язків за обраною спеціальністю.

4) за ст. 1 п. 1.13 - компетентність визначає здатність особи успішно здійснювати професійну та подальшу навчальну діяльність і є результатом навчання на певному рівні вищої освіти;

5) за ст. 1 п. 1.19 - результати навчання - сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за певною освітньо-професійною, освітньо-науковою програмою, які можна ідентифікувати, кількісно оцінити та виміряти.

На підставі цих положень прийнята (за термінологією Закону України «Про вищу освіту») така структура освітньої програми:

- виявлення видів і змісту професійної діяльності бакалавра за обраною спеціальністю (змісту вищої освіти) з урахуванням вимог професійних стандартів або еквівалентної нормативної бази;
- регламентація системи компетентностей бакалавра (змісту вищої освіти) як здатностей для успішного виконання професійних обов’язків за обраною спеціальністю з урахуванням вимог професійних стандартів або еквівалентної нормативної бази та вимог Національної рамки кваліфікацій до рівня освіти;
- розподіл компетентностей та кредитів на їх опанування за видами навчальної діяльності (навчальні дисципліни, практики, індивідуальні завдання);
- визначення результатів навчання (змісту навчання) через декомпозицію та конкретизацію компетентностей і формування системи умінь й відповідних знань у

програмах усіх видів навчальної діяльності здобувача – документах безпосередньої реалізації вищої освіти.

Реалізація компетентнісного підходу до проектування вищої освіти шляхом створення однозначного зв'язку запланованих компетентностей (зовнішніх цілей вищої освіти) і результатів навчання за програмами дисциплін, практик та індивідуальних завдань (реалізація цілей) є вирішальним чинником якості вищої освіти НГУ та створення реальної системи внутрішнього її забезпечення.

Прозорі й зрозумілі структура та зміст освітньої програми актуальні для абітурієнтів, здобувачів, викладачів, роботодавців.

Освітня програма використовується під час :

- акредитації освітньої програми, інспектуванні освітньої діяльності за спеціальністю та спеціалізацією ;
- розроблення навчального плану, програм навчальних дисципліні й практик;
- розроблення засобів діагностики якості вищої освіти;
- визначення змісту навчання в системі перепідготовки та підвищення кваліфікації;
- професійної орієнтації здобувачів фаху.

Освітня програма враховує вимоги Закону України «Про вищу освіту», Національної рамки кваліфікацій і встановлює:

- обсяг та термін навчання бакалаврів;
- загальні компетенції;
- професійні компетентності за спеціальністю та спеціалізаціями;
- перелік та обсяг навчальних дисциплін для опанування компетентностей освітньої програми;
- вимоги до структури навчальних дисциплін.

Освітня програма використовується для:

- складання навчальних планів та робочих навчальних планів;
- формування індивідуальних планів студентів;
- формування програм навчальних дисциплін, практик, змісту індивідуальних завдань;
- визначення інформаційної бази для формування засобів діагностики;
- акредитації освітньої програми;
- зовнішнього контролю якості підготовки фахівців;
- атестації бакалаврів і магістрів спеціальності 125 «Кібербезпека».

Користувачі освітньої програми:

- здобувачі вищої освіти, які навчаються в Державному ВНЗ «НГУ»;
- викладачі Державного ВНЗ «НГУ», які здійснюють підготовку бакалаврів спеціальності 125 «Кібербезпека»;
- Екзаменаційна комісія спеціальності 125 «Кібербезпека»;
- Приймальна комісія Державного ВНЗ «НГУ».

Освітня програма поширюється на кафедри Державного ВНЗ «НГУ», що здійснюють підготовку фахівців ступеня бакалавра спеціальності.

1.2. Нормативні посилання

Освітня програма розроблена на основі таких нормативних документів:

1. Закон України «Про вищу освіту» від 01.07.2014 // Відомості Верховної Ради. – 2014. – № 37, 38.
2. Національна рамка кваліфікацій. Додаток до постанови Кабінету Міністрів України від 23 листопада 2011 р. № 1341.
3. Постанова Кабінету Міністрів України від 26.04.2015 №266 «Перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти».
4. Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти. – К. : Ленвіт, 2006. – 35 с.
5. Наказ МОН 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.

1.3. Терміни та їх визначення

У програмі терміни вживаються в такому значенні*:*

1) *автономність і відповідальність* - здатність самостійно виконувати завдання, розв'язувати задачі і проблеми та відповідати за результати своєї діяльності;

2) *акредитація освітньої програми* – оцінювання освітньої програми та/або освітньої діяльності вищого навчального закладу за цією програмою на предмет відповідності стандарту вищої освіти; спроможності виконати вимоги стандарту та досягти заявлених у програмі результатів навчання; досягнення заявлених у програмі результатів навчання;

3) *атестація* - це встановлення відповідності засвоєних здобувачами вищої освіти рівня та обсягу знань, умінь, інших компетентностей вимогам стандартів вищої освіти;

4) *бакалавр* - це освітній ступінь, що здобувається на першому рівні вищої освіти та присуджується вищим навчальним закладом у результаті успішного виконання здобувачем вищої освіти освітньо-професійної програми, обсяг якої становить 180-240 кредитів ЄКТС. Обсяг освітньо-професійної програми для здобуття ступеня бакалавра на основі ступеня молодшого бакалавра визначається вищим навчальним закладом;

5) *вища освіта* – сукупність систематизованих знань, умінь і практичних навичок, способів мислення, професійних, світоглядних і громадянських якостей, морально-етичних цінностей, інших компетентностей, здобутих у вищому навчальному закладі у відповідній галузі знань за певною кваліфікацією на рівнях вищої освіти, що за складністю є вищими, ніж рівень повної загальної середньої освіти;

6) *вищий навчальний заклад* – окремий вид установи, яка є юридичною особою приватного або публічного права, діє згідно з виданою ліцензією на провадження освітньої діяльності на певних рівнях вищої освіти, проводить наукову, науково-технічну, інноваційну та/або методичну діяльність, забезпечує організацію освітнього процесу і здобуття особами вищої освіти, післядипломної освіти з урахуванням їхніх покликань, інтересів і здібностей;

7) *галузь знань* – основна предметна область освіти і науки, що включає групу споріднених спеціальностей, за якими здійснюється професійна підготовка;

8) *дипломна робота* – це кваліфікаційна робота, що має на меті виконання виробничих завдань, спрямованих на організацію технологічного процесу (технічну підготовку, забезпечення функціонування, контроль) та управління (планування, облік, аналіз, регулювання) організацією та власне технологічним процесом. Програми дипломних робіт зазвичай регламентовано певними професійними функціями й завданнями згідно з освітніми стандартами відповідних рівнів підготовки

9) *дипломний проект* – це кваліфікаційна робота, що присвячена реалізації виробничих завдань, переважна більшість яких віднесена до проектної та проектно-конструкторської професійних функцій. У межах цієї роботи передбачається виконання технічного завдання, ескізного й технічного проектів, робочої, експлуатаційної, ремонтної документації тощо;

10) *дисциплінарні компетентності* – деталізовані програмі компетентності як результат декомпозиції компетентностей фахівця спеціальності (спеціалізації) певного рівня вищої освіти;

11) *Європейська кредитна трансферно-накопичувальна система (ЄКТС)* – система трансферу і накопичення кредитів, що використовується в Європейському просторі вищої освіти з метою надання, визнання, підтвердження кваліфікацій та освітніх компонентів і сприяє академічній мобільності здобувачів вищої освіти. Система ґрунтується на визначенні навчального навантаження здобувача вищої освіти, необхідного для досягнення визначених результатів навчання, та обліковується в кредитах ЄКТС;

12) *засоби діагностики* – документи, що затверджені в установленому порядку, та призначені для встановлення ступеню досягнення запланованого рівня сформованості компетентностей студента при контрольних заходах;

13) *здобувачі вищої освіти* – особи, які навчаються у вищому навчальному закладі на певному рівні вищої освіти з метою здобуття відповідного ступеня і кваліфікації;

14) *змістовий модуль* – сукупність умінь, знань, цінностей, які забезпечують реалізацію певної компетентності;

15) *знання* - осмислена та засвоєна суб'єктом наукова інформація, що є основою його усвідомленої, цілеспрямованої діяльності. Знання поділяються на емпіричні (фактологічні) і теоретичні (концептуальні, методологічні);

16) *інтегральна компетентність* - узагальнений опис кваліфікаційного рівня, який виражає основні компетентностні характеристики рівня щодо навчання та/або професійної діяльності;

17) *інтегрована оцінка* – результат оцінювання конкретизованих завдань різних рівнів з урахуванням коефіцієнта пріоритетності (запланованого рівня сформованості компетентностей);

18) *інформаційне забезпечення навчальної дисципліни* – засоби навчання, у яких системно викладено основи знань з певної дисципліни на рівні сучасних досягнень науки і культури, опора для самоосвіти і самонавчання (підручники; навчальні посібники, навчально-наочні посібники, навчально-методичні посібники, хрестоматії, словники, енциклопедії, довідники тощо);

19) *кваліфікаційний рівень* - структурна одиниця Національної рамки кваліфікацій, що визначається певною сукупністю компетентностей, які є типовими для кваліфікацій даного рівня;

20) *кваліфікація* - офіційний результат оцінювання і визнання, який отримано, коли уповноважений компетентний орган установив, що особа досягла компетентностей (результатів навчання) за заданими стандартами;

21) *компетентність/компетентності* (за НРК) – здатність особи до виконання певного виду діяльності, що виражається через знання, розуміння, уміння, цінності, інші особисті якості;

22) *комунікація* - взаємозв'язок суб'єктів з метою передавання інформації, узгодження дій, спільної діяльності;

23) *кредит Європейської кредитної трансферно-накопичувальної системи* (далі – кредит ЄКТС) – одиниця вимірювання обсягу навчального навантаження здобувача вищої освіти, необхідного для досягнення визначених (очікуваних) результатів навчання. Обсяг одного кредиту ЄКТС становить 30 годин. Навантаження одного навчального року за денною формою навчання становить, як правило, 60 кредитів ЄКТС;

24) *курсова робота* – індивідуальне завдання, виконання якого спрямовано на організацію технологічного процесу (наприклад. технічну підготовку, забезпечення функціонування, контроль) та управління ним (планування, облік, аналіз, регулювання);

25) *курсовий проект* – індивідуальне завдання виконання якого відноситься здебільшого до проектної та проектно-конструкторської діяльності. Цей вид навчальної роботи може включати елементи технічного завдання, ескізні та технічні проекти, розроблення робочої, експлуатаційної, ремонтної документації тощо. Виконання курсового проекту регламентується відповідними стандартами;

26) *магістр* - це освітній ступінь, що здобувається на другому рівні вищої освіти та присуджується вищим навчальним закладом у результаті успішного виконання здобувачем вищої освіти відповідної освітньої програми. Ступінь магістра здобувається за освітньо-

професійною або за освітньо-науковою програмою. Обсяг освітньо-професійної програми підготовки магістра становить 90-120 кредитів ЄКТС, обсяг освітньо-наукової програми - 120 кредитів ЄКТС. Освітньо-наукова програма магістра обов'язково включає дослідницьку (наукову) компоненту обсягом не менше 30 відсотків;

27) *методичне забезпечення навчальної дисципліни* – рекомендації до супроводження навчальної діяльності студента за всіма видами навчальних занять, що містить, у тому числі інформацію щодо засобів та процедури контрольних заходів, їх форми та змісту, методів розв'язання вправ, джерел інформації;

28) *модульний контроль* – оцінювання ступеню досягнення студентом запланованого рівня сформованості компетентностей за видами навчальних занять;

29) *молодший бакалавр* - це освітньо-професійний ступінь, що здобувається на початковому рівні (короткому циклі) вищої освіти і присуджується вищим навчальним закладом у результаті успішного виконання здобувачем вищої освіти освітньої-професійної програми, обсяг якої становить 90-120 кредитів ЄКТС;

30) *навчальна дисципліна* – сукупність модулів, що підлягає підсумковому контролю;

31) *навчальний елемент* – мінімальна навчальна інформація самостійного смислового значення (поняття, явища, відношення, алгоритми);

32) *об'єкт діагностики* – компетентності, опанування яких забезпечуються навчальною дисципліною;

33) *об'єкт діяльності* – процеси, явища, технології або (та) матеріальні об'єкти на які спрямована діяльність фахівця (суб'єкта діяльності). Незалежно від фізичної природи об'єкт діяльності має певний період (цикл) існування, який передбачає етапи: проектування (розроблення), протягом якого вирішуються питання щодо забезпечення певних його якостей та властивостей; створення (виробництва, впровадження); експлуатації, протягом якої об'єкт використовується за призначенням; відновлення (ремонту, удосконалення), яке пов'язане з відновленням властивостей якості, підвищенням ефективності тощо; утилізації та ліквідації.

34) *освітній процес* – це інтелектуальна, творча діяльність у сфері вищої освіти і науки, що провадиться у вищому навчальному закладі (науковій установі) через систему науково-методичних і педагогічних заходів та спрямована на передачу, засвоєння, примноження і використання знань, умінь та інших компетентностей у осіб, які навчаються, а також на формування гармонійно розвиненої особистості.

35) *освітня (освітньо-професійна чи освітньо-наукова) програма* – система освітніх компонентів на відповідному рівні вищої освіти в межах спеціальності, що визначає вимоги до рівня освіти осіб, які можуть розпочати навчання за цією програмою, перелік навчальних дисциплін і логічну послідовність їх вивчення, кількість кредитів ЄКТС, необхідних для виконання цієї програми, а також очікувані результати навчання (компетентності), якими повинен оволодіти здобувач відповідного ступеня вищої освіти;

36) *освітня діяльність* – діяльність вищих навчальних закладів, що провадиться з метою забезпечення здобуття вищої, післядипломної освіти і задоволення інших освітніх потреб здобувачів вищої освіти та інших осіб;

37) *підсумковий контроль* – комплексне оцінювання запланованого рівня сформованості дисциплінарних компетентностей;

38) *поточний контроль* – оцінювання засвоєння студентом навчального матеріалу під час проведення аудиторного навчального заняття (опитування студентів на лекціях, перевірка та прийом звітів з виконання лабораторних робіт, тестування тощо);

39) *програма дисципліни* – нормативний документ, що визначає зміст навчальної дисципліни відповідно до освітньої програми, розробляється кафедрою, яка закріплена наказом ректора для викладання дисципліни;

40) *результати навчання* (Закон України «Про вищу освіту») – сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за певною освітньо-професійною, освітньо-науковою програмою, які можна ідентифікувати, кількісно оцінити та виміряти;

41) *результати навчання* (Національна рамка кваліфікацій) – компетентності (знання, розуміння, уміння, цінності, інші особисті якості), які набуває та/або здатна продемонструвати особа після завершення навчання;

42) *рівень сформованості дисциплінарної компетентності* – частка правильних відповідей або виконаних суттєвих операцій від загальної кількості запитань або суттєвих операцій еталону рішень;

43) *робоча програма дисципліни* – нормативний документ, що розроблений на основі програми дисципліни відповідно до річного навчального плану (містить розподіл загального часу на засвоєння окремих навчальних елементів і модулів за видами навчальних занять та формами навчання);

44) *самостійна робота* – діяльність студента з вивчення навчальних елементів та змістових модулів, опанування запланованих компетентностей, виконання індивідуальних завдань, підготовки до контрольних заходів;

45) *спеціалізація* – складова спеціальності, що визначається вищим навчальним закладом та передбачає профільну спеціалізовану освітньо-професійну чи освітньо-наукову програму підготовки здобувачів вищої та післядипломної освіти;

46) *спеціальність* – складова галузі знань, за якою здійснюється професійна підготовка;

47) *стандарт вищої освіти* – це сукупність вимог до змісту та результатів освітньої діяльності вищих навчальних закладів і наукових установ за кожним рівнем вищої освіти в межах кожної спеціальності;

48) *стандарт освітньої діяльності* – це сукупність мінімальних вимог до кадрового, навчально-методичного, матеріально-технічного та інформаційного забезпечення освітнього процесу вищого навчального закладу й наукової установи;

49) *уміння* - здатність застосовувати знання для виконання завдань та розв'язання задач і проблем. Уміння поділяються на когнітивні (інтелектуально-творчі) та практичні (на основі майстерності з використанням методів, матеріалів, інструкцій та інструментів).

50) *якість вищої освіти* – рівень здобутих особою знань, умінь, навичок, інших компетентностей, що відображає її компетентність відповідно до стандартів вищої освіти.

1.4. Позначення

НРК – Національна рамка кваліфікацій;
КЗ – загальні компетентності;
КФ – фахові компетентності.

2. КОМПЕТЕНТНОСТІ БАКАЛАВРА КІБЕРБЕЗПЕКИ

2.1 Перелік компетентностей випускника

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
	КЗ 2. Знання та розуміння предметної області та розуміння професії.
	КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово
	КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням
	КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.
Фахові компетентності	КФ 1. 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.
	КФ 2. Здатність до використання інформаційно-комунікаційних

	технологій, сучасних методів і моделей інформаційної безпеки.
	КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
	КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики безпеки.
	КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки.
	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 впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
	КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку
	КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою.
	КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
	КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем.
	КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам .

2.2 Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання

Кінцеві, підсумкові та інтегративні результати навчання, що визначають нормативний зміст підготовки і корелюються з визначеним вище переліком загальних і спеціальних компетентностей, подано нижче.

Результати навчання
- застосовувати знання державної та 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;
- 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;

- критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
- діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, 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 тому 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 системи 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.

Фахові компетентності	Результати навчання
КФ 1. 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.	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки	- здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; - розробляти та аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; - застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем; - здійснювати захист ресурсів і процесів в ІТС на основі моделей безпеки (кінцевих автоматів, управління потоками, *Bell-LaPadula, Biba, Clark-Wilson*, та інші), а також встановлених режимів безпечного функціонування ІТС; - виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим

	вимогам інформаційної і\або кібербезпеки в ІТС.
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту (КЗЗ) інформації в інформаційно-телекомунікаційних (автоматизованих) системах	- забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - виконувати розробку експлуатаційної документації на КЗЗ.
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики безпеки	- вирішувати задачі супроводу (в тому числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - 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); - вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в ІТС.
КФ 5 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки.	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної і кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних

	(автоматизованих) системах; - проектувати та реалізувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; - вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.	- вирішувати задачі управління процесами забезпечення неперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів; - вирішувати задачі корекції цілей, стратегій, планів забезпечення неперервності бізнесу після здійснення кібератак, збоїв та відмов різних класів. - створювати і впроваджувати плани процесу забезпечення неперервності бізнесу; - виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання.
КФ7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - здійснювати оцінку рівня захищеності інформації що обробляється в ІТС використовувати інструментальні засоби оцінювання наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих); - вирішувати задачі експертизи, випробування КСЗІ.
КФ 8. Здатність здійснювати процедури управління	- вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування

інцидентами, проводити розслідування, надавати їм оцінку.	на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - проводити розслідування інцидентів інформаційної безпеки та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної безпеки та/або кібербезпеки; - забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації.
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою.	- забезпечувати неперервність бізнес процесів організації на базі системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів; - забезпечувати функціонування системи управління інформаційною та\або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки.
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	- аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації; - аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації; - виявляти небезпечні сигнали технічних засобів; - вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами; - визначати ефективність захисту інформації від витоку технічними каналами 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 системи технічного захисту інформації; – обґрунтовувати можливість створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; – впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами.
КФ 11. Здатність виконувати моніторинг ресурсів і процесів функціонування, інформаційно-телекомунікаційних	- забезпечувати процеси моніторингу доступу до ресурсів і процесів ІТС; - забезпечувати конфігурування та функціонування систем моніторингу ресурсів та

(автоматизованих) систем.	процесів в ІТС;
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам .	- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних та автоматизованих системах; - аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в ІТС; - аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

3. ВИМОГИ ДО ПОПЕРЕДНЬОГО РІВНЯ ОСВІТИ ЗДОБУВАЧІВ

Особа має право здобувати ступінь бакалавра за умови наявності в неї повної загальної середньої освіти.

4. ОБСЯГ ПРОГРАМИ ТА ЙОГО РОЗПОДІЛ ЗА НОРМАТИВНОЮ ТА ВИБІРКОВОЮ ЧАСТИНАМИ

Обсяг освітньо-професійної програми становить 240 кредитів ЄКТС. Нормативна частина програми становить 175 кредити ЄКТС (73 %). Обсяг вибіркової частини – 65 кредитів ЄКТС (27%).

5. РОЗПОДІЛ ЗМІСТУ ВИЩОЇ ОСВІТИ ТА КРЕДИТІВ ЗА ВИДАМИ НАВЧАЛЬНОЇ ДІЯЛЬНОСТІ

№	Вид навчальної діяльності	Компе-тенції	обсяг, *кред.*
1. НОРМАТИВНА ЧАСТИНА			**175**
1.1 Цикл загальної підготовки			**25**
З1	Українська мова (за професійним спрямуванням)	КЗ 3	3
З2	Філософія	КЗ 4	3
З3	Іноземна мова професійного спрямування (англійська/німецька/французька)	КЗ 3	6
З4	Історія українського суспільства	КЗ 2	3
З5	Світова та українська культура	КЗ 1	3
З6	Фізична культура і спорт	КЗ 1	3
З7	Цивільна безпека	КЗ 4	4
1.2 Цикл професійної підготовки			**150**
1.2.1 Базові дисципліни за галуззю знань			**27**
Б1	Вища математика	КФ2, КФ 10	12
Б2	Фізика	КФ5, КФ 10	8
Б3	Теорія ймовірностей та математична статистика	КФ2, КФ 8, КФ 9, КФ 10	4
Б4	Економіка і управління підприємством	КФ 12	3
1.2.2 Фахові дисципліни за спеціальністю			**93**
Ф1	Спеціальні розділи з математики	КФ 2, КФ5, КФ 10	6

Ф2	Технологія програмування	КФ 1, КФ 3, КФ 5	11
Ф3	Основи електроніки	КФ 10	3
Ф4	Кіберзахист	КФ 2, КФ 3, КФ 6, КФ 7	12
Ф5	Інженерно-комп'ютерна графіка	КФ 1	4
Ф6	Інформаційні технології	КФ 2, КФ 6, КФ 11	4
Ф7	Мережеві технології і протоколи	КФ 2, КФ 6	9
Ф8	Комплексні системи захисту інформації	КФ 1, КФ 3, КФ 5, КФ 7, КФ 12	9
Ф9	Архітектура інформаційно-обчислювальних систем	КФ 2, КФ 6	4
Ф10	Операційні системи	КФ 2, КФ 6, КФ 11	7
Ф11	Основи теорії кіл, сигнали та процеси в електроніці	КФ 10, КФ 11	4
Ф12	Прикладна криптологія	КФ5, КФ 10	9
Ф13	Основи забезпечення безпеки інформації	КФ 1, КФ 2, КФ 4, КФ 12	5
Ф14	Іноземна мова для професійного спілкування	КЗ 3	6
1.2.3 Практична підготовка та дипломування за спеціальністю			**30**
П1	Практика навчальна комп'ютерна	КЗ 1,КЗ 2, КЗ 5, КФ 2, КФ 3	6
П2	Практика технологічна	КЗ 1, КЗ 2, КЗ 3, КФ2-КФ10	6
П3	Виробнича практика	КЗ 1, КЗ 2, КЗ 3, КФ1-КФ12	6
П4	Переддипломна практика	КЗ 1, КЗ 2, КЗ 3, КФ1-КФ12	3
П5	Дипломування	КЗ 1, КЗ 3, КФ1-КФ12	9
2. ВИБІРКОВА ЧАСТИНА			**65**
2.1 Дисципліни спеціалізації «Кібербезпека»			**53**
С1.1	Теорія ризиків	КФ6, КФ 9	4
С1.2	Технічні системи охорони об’єктів	КФ 1, КФ 10	5
С1.3	Бази даних	КФ 2, КФ 5	6
С1.4	Мікропроцесорні системи	КФ2, КФ 3, КФ 6	6
С1.5	Організаційне забезпечення захисту інформації та спеціального діловодства	КФ 1, КФ 3, КФ 4, КФ 6	4
С1.6	Системи технічного захисту інформації	КФ 1, КФ 10	6
С1.7	Теорія інформації та кодування	КФ 2, КФ 3	4
С1.8	Аналіз безпеки програмного забезпечення	КФ 2, КФ 12	3
С1.9	Нормативно-правове забезпечення інформаційної безпеки	КФ 1, КФ 3, КФ 9	3

С1.10	Кібер-операції	КФ 8, КФ 12	3
С1.11	Економічна безпека	КФ 6, КФ 8, КФ 9	4
С1.12	Управління інформаційною безпекою	КФ 1, КФ 3, КФ 4, КФ 5, КФ 9	5
2.2 Дисципліни спеціалізації «Безпека інформаційних і комунікаційних систем»			**53**
С2.1	Теорія ризиків	КФ6, КФ 9	4
С2.2	Цифрова обробка сигналів	КФ 1, КФ 10	5
С2.3	Організація баз даних та знань	КФ 2, КФ 5	6
С2.4	Спеціальні мікропроцесори	КФ2, КФ 3, КФ 6	6
С2.5	Організація спеціального діловодства	КФ 1, КФ 3, КФ 4, КФ 6	4
С2.6	Відкриті комп'ютерні системи та мережі	КФ 1, КФ 10	6
С2.7	Теорія інформації та кодування	КФ 2, КФ 3	4
С2.8	Система охорони державної таємниці	КФ 2, КФ 12	3
С2.9	Нормативно-правове забезпечення інформаційної безпеки	КФ 2, КФ 6	3
С2.10	Основи теорії систем	КФ 8, КФ 12	3
С2.11	Захист економічної інформації	КФ 6, КФ 8, КФ 9	4
С2.12	Управління інформаційною безпекою	КФ 1, КФ 3, КФ 4, КФ 5, КФ 9	5
2.3 Цикл загальної підготовки. Дисципліни за вибором студента			**12**
В1	Дисципліна вільного вибору №1	КЗ 1, КЗ 2, КЗ 4, КЗ 5	3
В2	Дисципліна вільного вибору №2		3
В3	Дисципліна вільного вибору №3		3
В4	Дисципліна вільного вибору №4		3
Разом за нормативною та вибірковою частинами			**240**

6. РЕЗУЛЬТАТИ НАВЧАННЯ ТА ВИМОГИ ДО СТРУКТУРИ ПРОГРАМ ДИСЦИПЛІН

Уміння бакалавра визначаються за видами навчальної діяльності як конкретизація загальних і професійних компетентностей в програмах навчальних дисциплін, практик, індивідуальних завдань і застосовуються як критерії відбору необхідних і достатніх знань (змістових модулів), які можна ідентифікувати, кількісно оцінити та виміряти.

Зв'язок освітньої програми з програмами підготовки за видами навчальної діяльності забезпечує якість вищої освіти на стадії проектування.

Програма дисципліни має визначати також загальний час на засвоєння, форму підсумкового контролю, перелік базових дисциплін, вимоги до інформаційно-методичного забезпечення, вимоги до засобів діагностики та критеріїв оцінювання, вимоги до структури робочої програми дисципліни.

7. ЗАГАЛЬНІ ВИМОГИ ДО ЗАСОБІВ ДІАГНОСТИКИ

Інформаційною базою для створення засобів діагностики підсумкового контролю за видами навчальної діяльності мають бути дисциплінарні уміння та відповідні знання.

Випускна атестація здійснюється оцінюванням ступеню сформованості компетентностей. Форма атестації – публічний захист дипломної роботи.

8. СТРУКТУРНО-ЛОГІЧНА СХЕМА

Послідовність навчальної діяльності здобувача за денною формою навчання:

1-й семестр

№	Вид навчальної діяльності	обсяг, *кред.*
1	Іноземна мова професійного спрямування (англійська/німецька/французька)	3
2	Фізична культура і спорт	2
3	Фізика	5
4	Вища математика	5
5	Українська мова (за професійним спрямуванням) 1 чверть	3
6	Технологія програмування	8
7	Інформаційні технології	4
	Всього за 1-й семестр	30

2-й семестр

№	Вид навчальної діяльності	обсяг, *кред.*
1	Фізична культура і спорт	1
2	Іноземна мова професійного спрямування (англійська/німецька/французька)	3
3	Фізика	3
4	Вища математика	3
5	Технологія програмування	3
6	Інженерно-комп'ютерна графіка	4
7	Архітектура інформаційно-обчислювальних систем	4
8	Практика навчальна комп’ютерна	6
9	Історія українського суспільства (3 чверть)	3
	Всього за 2-й семестр	30

3-й семестр

№	Вид навчальної діяльності	обсяг, кред.
1	Спеціальні розділи з математики	6
2	Вища математика	4
3	Операційні системи	7
4	Основи теорії кіл, сигнали та процеси в електроніці	4
5	Іноземна мова для професійного спілкування (2 чверть)	1
6	Основи забезпечення безпеки інформації	5
7	Світова та українська культура (1 чверть)	3
	Всього за 3-й семестр	30

4-й семестр

№	Вид навчальної діяльності	обсяг, *кред.*
1	Філософія (3 чверть)	3
2	Теорія ймовірностей та математична статистика	4

3	Практика технологічна (4 чверть)	6
4	Основи електроніки	3
5	Мережеві технології і протоколи	9
6	Іноземна мова для професійного спілкування	5
	Всього за 4-й семестр	30

5-й семестр

№	Вид навчальної діяльності	обсяг, *кред.*
1	Теорія ризиків	4
2	Прикладна криптологія	4
3	Дисципліна вільного вибору №1	3
4	Бази даних (спеціалізація за п. 2.1) Організація баз даних та знань (спеціалізація за п. 2.2)	6
5	Мікропроцесорні системи (спеціалізація за п. 2.1) Спеціальні мікропроцесори (спеціалізація за п. 2.2)	6
6	Теорія інформації та кодування	4
7	Нормативно-правове забезпечення інформаційної безпеки	3
	Всього за 5-й семестр	30

6-й семестр

№	Вид навчальної діяльності	обсяг, *кред.*
1	Прикладна криптологія	5
2	Організаційне забезпечення захисту інформації та спеціального діловодства (спеціалізація за п. 2.1) Організація спеціального діловодства (спеціалізація за п. 2.2)	4
3	Системи технічного захисту інформації (спеціалізація за п. 2.1) Відкриті комп'ютерні системи та мережі (спеціалізація за п. 2.2)	6
4	Аналіз безпеки програмного забезпечення (спеціалізація за п. 2.1) Система охорони державної таємниці (спеціалізація за п. 2.2)	3
5	Кібер-операції (спеціалізація за п. 2.1) Основи теорії систем (спеціалізація за п. 2.2)	3
6	Дисципліна вільного вибору № 2	3
7	Виробнича практика (4 чверть)	6
	Всього за 6-й семестр	30

7-й семестр

№	Вид навчальної діяльності	обсяг, *кред.*
1	Кіберзахист	9
2	Технічні системи охорони об'єктів (спеціалізація за п. 2.1) Цифрова обробка сигналів (спеціалізація за п. 2.2)	5
3	Цивільна безпека	4
4	Управління інформаційною безпекою	5
5	Дисципліна вільного вибору №3	3
6	Економічна безпека (спеціалізація за п. 2.1)	4

	Захист економічної інформації (спеціалізація за п. 2.2)	
	Всього за 7-й семестр	30

8-й семестр

№	Вид навчальної діяльності	**обсяг,** *кред.*
1	Дисципліна вільного вибору №4	3
2	Переддипломна практика	3
3	Кіберзахист	3
4	Комплексні системи захисту інформації	9
5	Дипломування	9
6	Економіка і управління підприємством	3
	Всього за 8-й семестр	30

9. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

9.1. Освітня програма оприлюднюється на сайті університету до початку прийому на навчання до університету відповідно до Правил прийому.

9.2. Відповідальність за впровадження освітньої програми та забезпечення якості вищої освіти несуть завідувачі випускових кафедр за спеціальністю та завідувачі випускових кафедр за спеціалізаціями.