МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека»

Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь вищої освіти	Бакалавр
Спеціальність	125 «Кібербезпека»
Галузь знань	12 Інформаційні технології
Кваліфікація	Бакалавр з кібербезпеки

Затверджено рішенням вченої ради
Протокол від 25 серпня 2020 р. № 1
Голова вченої ради _____ Васильєв А.В.

Суми 2020 р.

Освітня програма обговорена та схвалена на засіданні Ради з якості факультету електроніки та інформаційних технологій.

Протокол № 1 від 27.08.2020 р.

Голова Ради з якості факультету

Ткач О.П.

Освітня програма обговорена та схвалена на засіданні Ради із забезпечення якості освітньої діяльності та якості вищої освіти Сумського державного університету.

Протокол № 1 від 27.08. 2020 р.

Голова Ради з якості Сумського державного університету

Карпуша В.Д.

ПЕРЕДМОВА

Міністерство освіти і науки України. Стандарт вищої освіти. Перший (бакалаврський) рівень вищої освіти. Ступінь «бакалавр». Галузь знань: 12 «Інформаційні технології», спеціальність: 125 «Кібербезпека». Затверджено та введено в дію наказом МОН України від 04.10.2018 р. № 1074.

Розроблено робочою проєктною групою (РПГ) у складі:

Прізвище, ім'я, по батькові		Науковий ступінь, шифр та назва наукової спеціальності	Вчене звання (за кафедрою)	Посада та назва підрозділу (за основним місцем роботи)
Керівник робочої проектної групи (гарант освітньої програми):	1. Шелехов Ігор Володимирович	Кандидат технічних наук. 05.13.07 – Автоматизація процесів керування	Доцент за кафедрою комп'ютерних наук	Доцент кафедри комп'ютерних наук
Члени РПГ:	1. Лавров Євгеній Анатолійович	Доктор технічних наук, 05.02.20 – Ергономіка	Професор за кафедрою кібернетики та інформатики	Професор кафедри комп'ютерних наук
	2. Москаленко В'ячеслав Васильович	Кандидат технічних наук. 05.13.07 – Автоматизація процесів керування	Доцент за кафедрою комп'ютерних наук	Доцент кафедри комп'ютерних наук
	3. Ященко Анна Миколаївна	-	-	Бакалавр, група КБ-81 (3 курс)
	4. Теницька Альона Олексіївна	-	-	Бакалавр, КБ-71 (4 курс)
	5. Чалий Олександр Володимирович	-	-	Завідувач відділу технічної підтримки рішень замовників ТОВ «НЕТКРЕКЕР» м. Суми; керівник навчально-консультативного центру ТОВ «НЕТКРЕКЕР» в СумДУ
	6. Кальченко Вадим Володимирович	-	-	Головний інспектор з захисту інформації Управління державної служби спеціального зв'язку і захисту інформації в Сумській області

Зовнішні рецензенти:

Прізвище, ім’я, по батькові	Науковий ступінь, шифр та назва наукової спеціальності	Вчене звання (за кафедрою)	Посада та назва підрозділу (за основним місцем роботи)
Халімов Геннадій Зайдулович	Доктор технічних наук, 05.13.05 – Комп'ютерні системи та компоненти	Професор кафедри безпеки інформаційних технологій	Завідувач кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, голова спеціалізованої вченої ради К 64.052.05 з захисту зі спеціальністю 05.13.21- «системи захисту інформації», член НМР, член НТР
Косяков Олександр Валерійович	-	-	Начальник відділу протидії кіберзлочинам в Сумській області Департаменту кіберполіції Національної поліції України, майор поліції

Освітня програма обговорена та схвалена на засіданні Експертної ради роботодавців зі спеціальності 122 «Комп’ютерні науки», 125 «Кібербезпека»

Протокол № 3 від 26.08.2020 р.

Голова Експертної ради роботодавців зі спеціальності

Чалий О. В.

Термін перегляду освітньої програми 1 раз на 1 рік

Ця освітня програма не може бути повністю або частково відтворена, тиражована та розповсюджена без дозволу Сумського державного університету.

1. Профіль освітньої програми

1.1 Загальна інформація

Повна офіційна назва вищого навчального закладу	Сумський державний університет
Повна назва структурного підрозділу	Факультет електроніки та інформаційних технологій, кафедра комп'ютерних наук
Ступінь вищої освіти та назва кваліфікації	Бакалавр. Бакалавр з кібербезпеки
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний. Обсяг освітньої програми на базі повної загальної середньої освіти становить 240 кредитів ЄКТС, термін навчання – 3 роки 10 місяців Обсяг освітньої програми на базі ступеня молодшого бакалавра / молодшого спеціаліста споріднених спеціальностей може становити 120 кредитів ЄКТС, термін навчання – 1 рік 10 місяців
Наявність акредитації	-
Цикл/рівень вищої освіти	Перший (бакалаврський) рівень вищої освіти, НРК – 6 рівень, QF-LLL – 6 рівень, FQ-EHEA – перший цикл
Передумови	Наявність середньої освіти, ступеня молодший бакалавр, ОКР молодший спеціаліст
Мова(и) викладання	Українська мова
Термін дії освітньої програми	До 01.07.2025 р.
Інтернет-адреса постійного розміщення опису освітньої програми	https://op.sumdu.edu.ua/#/programm/1735

1.2 Мета освітньої програми

Програма розроблена відповідно до місії університету, спрямована на підготовку фахівців, здатних використовувати та впроваджувати технології інформаційної та / або кібербезпеки, розв'язувати складні спеціалізовані задачі та практичні проблеми з забезпечення інформаційної та / або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

1.3 Характеристика освітньої програми

Предметна область освітньої програми	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 області Знання – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;

	– принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. Інструменти та обладнання: – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Освітньо-професійна програма. Акцент на моделюванні, проектуванні, розробці, інтеграції та супроводженні систем та комплексів інформаційної та/або кібербезпеки на базі сучасних інформаційно-комунікаційних технологій.
Основний фокус освітньої програми та спеціалізації	Загальна освіта в області кібербезпеки. Програма базується на сучасних методах, методиках, інформаційно-комунікаційних технологіях та технологіях забезпечення інформаційної та/або кібербезпеки, орієнтує на подальшу професійну кар'єру в ІТ-сфері. Ключові слова: кібербезпека, інформаційна безпека, криптографічний захист інформації, технічний захист інформації, захист персональних даних, антивірусний захист, захист інформації від несанкціонованого доступу, електронний цифровий підпис, захист від технічних розвідок.
Особливості освітньої програми	Передбачається проходження виробничої та переддипломної практик здобувачів вищої освіти за освітньо-професійною програмою «Кібербезпека» в підрозділах відділу протидії кіберзлочинам в Сумській області Департаменту кіберполіції Національної поліції України.

1.4 Придатність випускників до працевлаштування та подальшого навчання

Придатність до працевлаштування	Адміністратор бази даних (код КП 2131.2) Адміністратор даних (код КП 2131.2) Адміністратор доступу (код КП 2131.2) Аналітик з комп'ютерних комунікацій (код КП 2131.2) Аналітик комп'ютерних систем (код КП 2131.2) Аналітик операційного та прикладного програмного забезпечення (код КП 2131.2) Аналітик програмного забезпечення та мультимедіа (код КП 2131.2) Інспектор з організації захисту секретної інформації(код КП 3439) Фахівець із організації інформаційної безпеки (код КП 3439) Фахівець із організації захисту інформації з обмеженим доступом (код КП 3439) Фахівець з режиму секретності(код КП 3439) Фахівець з розробки та тестування програмного забезпечення (код КП 2131)

Подальше навчання	Можливість продовжити навчання за програмою другого рівня вищої освіти.

1.5 Викладання, навчання та оцінювання

Викладання та навчання	Студентоцентроване навчання, проблемно-орієнтоване навчання, електронне навчання в системі OCW СумДУ, самонавчання, навчання через лабораторну, виробничу та переддипломну практики, навчання на основі досліджень. Викладання проводиться у вигляді: лекцій, мультимедійних лекцій, інтерактивних лекцій, семінарських, практичних занять, лабораторних робіт. Також передбачена самостійна робота з можливістю консультацій з викладачем, e-learning за окремими освітніми компонентами.
Оцінювання	За освітньою програмою передбачено формативне (письмові та усні коментарі та настанови викладачів в процесі навчання, формування навичок самооцінювання, залучення студентів до оцінювання роботи один одного) та сумативне (письмові іспити з навчальних дисциплін, оцінювання поточної роботи протягом вивчення окремих освітніх компонентів (презентації, тестування), захист звітів з практики, захист курсових робіт (проектів), прилюдний захист кваліфікаційної роботи) оцінювання

1.6 Програмні компетентності (ПК)

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 (ЗК)	**ЗК 1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК 2.** Знання та розуміння предметної області та розуміння професії. **ЗК 3.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **ЗК 4.** Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **ЗК 5.** Здатність до пошуку, оброблення та аналізу інформації. **ЗК 6.** Здатність реалізовувати свої права як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. **ЗК 7.** 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.
Фахові компетентності спеціальності (ФК)	***Фахові компетентності, визначені за спеціальністю*** **ФК 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. **ФК 2.** Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. **ФК 3.** Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. **ФК 4.** Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

	ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. **ФК 6.** Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. **ФК 7.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). **ФК 8.** Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **ФК 9.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. **ФК 10.** Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. **ФК 11.** Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. **ФК 12.** Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

1.7 Програмні результати навчання (ПРН)

Програмні результати навчання, визначені за спеціальністю

ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН 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.

ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

ПРН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

ПРН 12. Розробляти моделі загроз та порушника.

ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності, якості прийнятих рішень.
ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
ПРН 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.
ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
ПРН 21. 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.
ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 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).
ПРН 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.
ПРН 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.
ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 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;
ПРН 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.
ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

ПРН 33. Вирішувати задачі забезпечення неперервності бізнес процесів організації на основі теорії ризиків.
ПРН 34. Брати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
ПРН 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.
ПРН 36. Виявляти небезпечні сигнали технічних засобів.
ПРН 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.
ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
ПРН 44. Вирішувати задачі забезпечення неперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно вітчизняними та міжнародними вимогами і стандартами.
ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
ПРН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

1.8 Ресурсне забезпечення реалізації програми

Кадрове забезпечення	Основний склад викладачів освітньої програми складається з професорсько-викладацького складу кафедри комп'ютерних наук факультету електроніки та інформаційних технологій. Також до викладання окремих курсів відповідно до їх компетенції та досвіду залучений професорсько-викладацький склад інших кафедр, зокрема кафедри іноземних мов факультету іноземної філології та соціальних комунікацій. Лектори, які викладають у рамках програми, є активними вченими, представниками національних та міжнародних професійних асоціацій «назви асоціацій», які публікують праці у вітчизняній і зарубіжній науковій пресі, мають відповідну професійну компетентність і досвід в галузі викладання, наукових досліджень і педагогічної діяльності. Практико-орієнтований характер освітньої програми передбачає широку участь фахівців-практиків, що відповідають напряму програми, а також залучення до викладання компетентних експертів високого рівня, включаючи представників професійних спілок та асоціацій «назви професійних спілок та асоціацій», що підсилює синергетичний зв'язок теоретичної та практичної підготовки. Гарант, група забезпечення, робоча проєктна група та викладацький склад, який забезпечує її реалізацію, відповідає вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності закладів освіти
Матеріально-технічне забезпечення	Навчальний процес за освітньою програмою проводиться в аудиторіях та лабораторіях, обладнаних аудіовізуальною апаратурою і необхідними технічними засобами. Навчальні заняття проводяться у 11 комп'ютерних класах, оснащених ліцензійними операційними системами від Microsoft та пакетами прикладного програмного забезпечення від Microsoft, Intel, Delcam, Siemens, Symantec, ESET, McAfee тощо. Лабораторія систем технічного захисту інформації дозволяє здобувачам набути практичного досвіту у застосуванні спеціалізованого обладнання інтелектуальних систем безпеки: приладами звукової та візуальної сигналізації, охоронної сигналізації, відеоспостереження; систем контролю та керування доступом з використанням біометричних зчитувачів, безконтактних зчитувачів ID-карт, токенів та електронних ключів тощо. Матеріально-технічна база IT-підприємств «Netcracker», «Brocoders», «Apptimized» та ін., якими було обладнано 5 навчально-методичних центрів на кафедрі, дозволяє ознайомитися з теоретичними і практичними аспектами розробки та впровадження сучасних інформаційно-телекомунікаційних систем та їх компонентів, що забезпечують інформаційну та/або кібербезпеку.
Інформаційне та навчально-методичне забезпечення	Студенти, що навчаються за цією освітньо-професійною програмою, та викладачі можуть використовувати бібліотечно-інформаційний корпус, міжвузівську наукову бібліотеку, окремі бібліотеки та бібліотечні пункти при навчально-наукових структурних підрозділах університету. Також діють віртуальні електронні читальні зали. Інформаційні ресурси бібліотеки СумДУ за освітньо-професійною програмою «Кібербезпека» формуються відповідно до предметної області та сучасних тенденцій наукових досліджень у галузі інформаційних технологій. Студенти можуть отримати доступ до всіх друкованих видань різними мовами, включаючи монографії, навчальні посібники, підручники, словники тощо. При цьому вони можуть переглядати літературу з використанням традиційних засобів пошуку в бібліотеці або використовувати доступ до

	Інтернету та бази даних. Доступ до всіх бібліотечних баз надається у внутрішній мережі університету. Студенти також використовують методичний матеріал, підготовлений викладачами: підручники, презентації за лекціями, конспекти лекцій, методичні вказівки до практичних, лабораторних, семінарських занять, індивідуальних завдань тощо. Методичний матеріал може надаватись як у друкованому вигляді, так і в електронній формі. Для дистанційного доступу до навчально-методичних матеріалів розроблено платформу OCW (ocw.sumdu.edu.ua), а для реалізації змішаного навчання в умовах карантину MIX (mix.sumdu.edu.ua) (платформи дозволяють об'єднати матеріали з дистанційних курсів, конструктор Lectur`ED з можливістю колективної роботи над електронними навчальними ресурсами, матеріали електронного каталогу бібліотеки, репозитарію та посилання на зовнішні навчальні ресурси). Методичний матеріал періодично оновлюється та адаптується до цілей освітньо-професійної програми.

1.9 Академічна мобільність

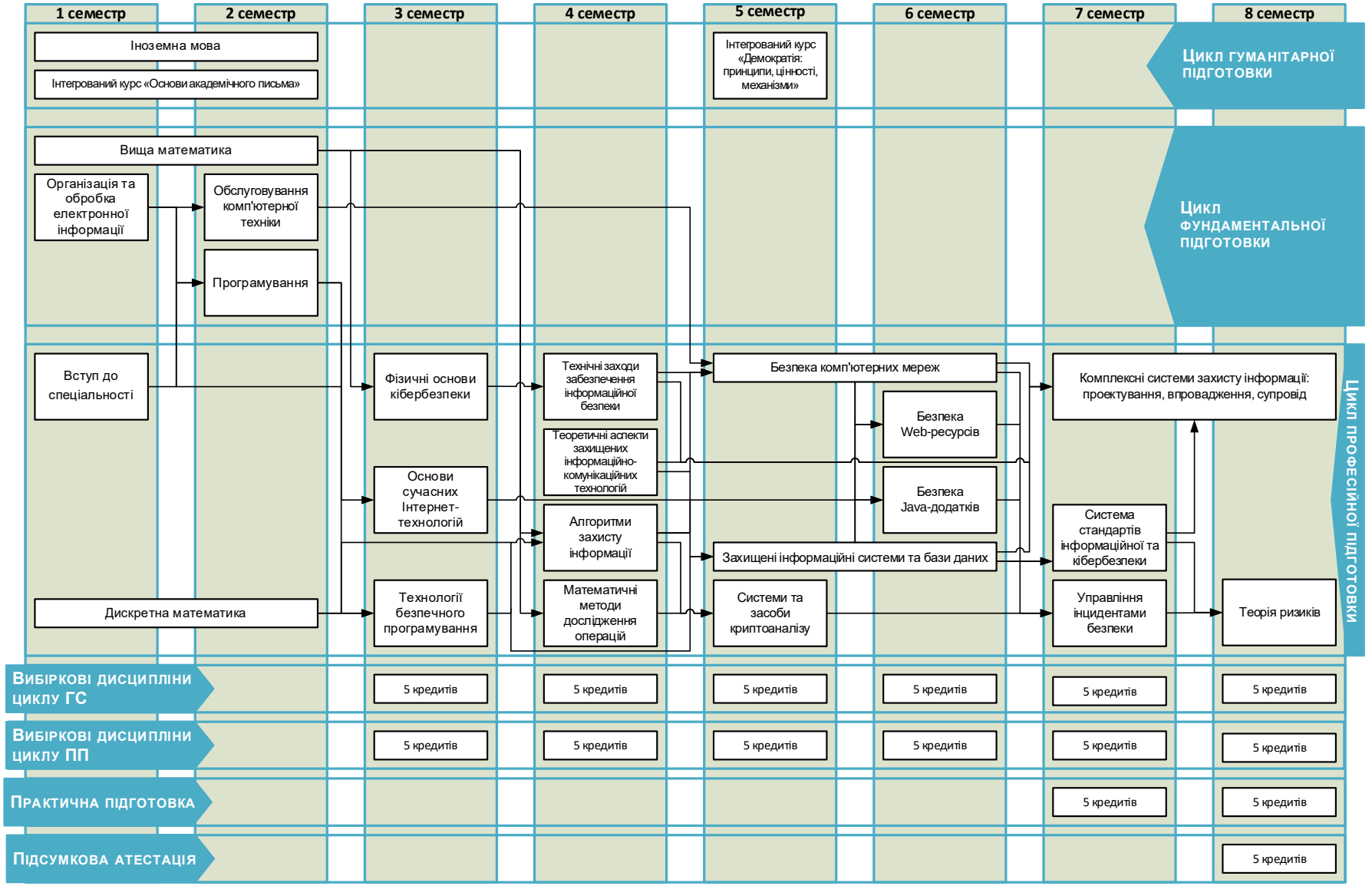
Внутрішня академічна мобільність	На основі двосторонніх договорів між Сумським державним університетом та закладами вищої освіти України
Міжнародна академічна мобільність	Згідно з Положення про академічну мобільність здобувачів вищої освіти (затвердженим наказом ректора №0521-I від 10.07.2018 р. – http://bit.do/feXDu) в рамках урядових стипендіальних програм та на основі двосторонніх договорів між Сумським державним університетом та закордонними закладами вищої освіти, в т.ч.: • з Білоруським державним технологічним університетом (Білорусь) – угода від 01.09.2016 р.; • з Університетом Савой Монблан (Франція) – угода від 20.02.2017 р.; • з Університетом ім. Адама Міцкевича (Польща) – угода від 14.06.17 р.; з Інститутом мистецтва, дизайну та технологій (Ірландія) – угода від 20.09.2018 р.
Навчання іноземних здобувачів вищої освіти	Можливе після проходження первинної акредитації освітньо-професійної програми в 2020-2021 навчальному році.

2. Перелік компонентів освітньої програми та їх логічна послідовність

2.1. Перелік компонентів освітньої програми

Код компонента	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти			
Цикл загальної підготовки			
ОК 1.	Іноземна мова	5	залік
ОК 2.	Інтегрований курс «Основи академічного письма»	5	іспит / залік
ОК 3.	Інтегрований курс «Демократія: принципи, цінності, механізми»	5	залік
ОК 4.	Вища математика	20	іспит
ОК 5.	Організація та обробка електронної інформації	5	залік
ОК 6.	Обслуговування комп'ютерної техніки	5	залік
ОК 7.	Програмування	5	іспит
Цикл фахової підготовки			
ОК 8.	Вступ до спеціальності	5	залік
ОК 9.	Дискретна математика	10	іспит / залік
ОК 10.	Основи сучасних Інтернет-технологій	5	залік
ОК 11.	Фізичні основи кібербезпеки	10	іспит
ОК 12.	Технології безпечного програмування	5	іспит
ОК 13.	Теоретичні аспекти захищених інформаційно-комунікаційних технологій	5	іспит
ОК 14.	Алгоритми захисту інформації	5	залік
ОК 15.	Технічні заходи забезпечення інформаційної безпеки	5	іспит
ОК 16.	Математичні методи дослідження операцій	5	іспит
ОК 17.	Системи та засоби криптоаналізу	5	іспит
ОК 18.	Безпека комп'ютерних мереж	10	іспит / залік
ОК 19.	Захищені інформаційні системи та бази даних	10	іспит / залік
ОК 20.	Безпека Web-ресурсів	5	іспит
ОК 21.	Безпека Java-додатків	5	залік
ОК 22.	Система стандартів інформаційної та кібербезпеки	5	іспит
ОК 23.	Комплексні системи захисту інформації: проектування, впровадження, супровід	10	іспит
ОК 24.	Управління інцидентами безпеки	5	залік
ОК 25.	Теорія ризиків	5	залік
Практична підготовка			
ОК 26.	Практика виробнича	5	залік
ОК 27.	Практика переддипломна	5	залік
Атестація			
ОК 28.	Кваліфікаційна робота бакалавра	5	захист
Загальний обсяг обов'язкових компонентів:		**180 кредитів (900 годин)**	
Вибіркові компоненти			
Загальний обсяг вибіркових компонентів:		**60 (300 годин)**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240200 годин)**	

2.2. Структурно-логічна схема освітньої програми



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Кібербезпека» зі спеціальності «125 – Кібербезпека» проводиться у формі публічного захисту (демонстрації) кваліфікаційної роботи бакалавра, і завершується видачею документу державного зразка про присудження ступеня бакалавра із присвоєнням кваліфікації «бакалавр з кібербезпеки». Атестація здійснюється відкрито і публічно.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

Позначки програмних компетент-ностей та освітніх компонентів	ЗК 1	ЗК 2	ЗК 3	ЗК 4	ЗК 5	ЗК 6	ЗК 7	ФК 1	ФК 2	ФК 3	ФК 4	ФК 5	ФК 6	ФК 7	ФК 8	ФК 9	ФК 10	ФК 11	ФК 12
ОК 1			×																
ОК 2			×				×												
ОК 3						×	×												
ОК 4	×				×				×										
ОК 5					×				×			×				×			
ОК 6	×								×			×	×						×
ОК 7	×	×			×														
ОК 8		×						×	×										×
ОК 9																×	×		
ОК 10									×			×		×		×		×	
ОК 11	×	×			×				×		×		×						
ОК 12								×	×								×		×
ОК 13									×			×							×
ОК 14				×				×				×					×		
ОК 15											×	×					×	×	
ОК 16				×	×										×				
ОК 17																×	×		
ОК 18										×	×	×		×			×	×	×
ОК 19									×		×	×					×		
ОК 20										×			×						×
ОК 21									×			×							×
ОК 22								×						×				×	×
ОК 23								×				×		×					×
ОК 24													×		×			×	
ОК 25								×			×					×			×
ОК 26	×			×							×	×				×		×	
ОК 27		×			×									×	×		×		×
ОК 28			×			×	×	×	×	×			×						

5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми

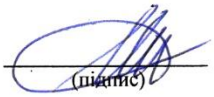
Позначки програмних результатів навчання та освітніх компонентів	ПРН 1	ПРН 2	ПРН 3	ПРН 4	ПРН 5	ПРН 6	ПРН 7	ПРН 8	ПРН 9	ПРН 10	ПРН 11	ПРН 12	ПРН 13	ПРН 14	ПРН 15	ПРН 16	ПРН 17	ПРН 18	ПРН 19	ПРН 20	ПРН 21	ПРН 22	ПРН 23	ПРН 24	ПРН 25	ПРН 26	ПРН 27	ПРН 28	ПРН 29	ПРН 30	ПРН 31	ПРН 32	ПРН 33	ПРН 34	ПРН 35	ПРН 36	ПРН 37	ПРН 38	ПРН 39	ПРН 40	ПРН 41	ПРН 42	ПРН 43	ПРН 44	ПРН 45	ПРН 46	ПРН 47	ПРН 48	ПРН 49	ПРН 50	ПРН 51	ПРН 52	ПРН 53	ПРН 54
ОК 1	×																																																				
ОК 2	×																																																				
ОК 3	×																																																			×
ОК 4			×	×																																×	×														
ОК 5		×	×		×	×	×							×	×			×	×																																		
ОК 6		×	×		×	×					×			×	×						×	×									×																					
ОК 7		×	×	×	×	×																																														
ОК 8		×	×			×	×								×																																				×	×
ОК 9		×	×	×	×					×	×		×				×		×		×			×			×				×			×											×	×		×				
ОК 10														×	×	×			×							×	×				×																×		×				
ОК 11			×	×	×	×									×		×																																				
ОК 12			×	×										×	×												×			×																					×	
ОК 13						×				×			×						×		×	×		×			×				×																×						
ОК 14														×					×												×																		×	×				
ОК 15																						×			×										×	×	×	×	×								×	×				
ОК 16		×	×	×		×								×																												×				×							
ОК 17														×					×												×																		×	×				
ОК 18				×										×	×		×	×		×			×			×		×	×	×										×									×	×	×		
ОК 19						×									×			×	×				×	×	×				×																								
ОК 20							×		×				×							×			×					×	×							×																	×	
ОК 21		×	×	×	×	×								×	×						×			×					×		×																					×	
ОК 22							×	×	×																									×							×												
ОК 23		×	×	×			×		×			×				×																	×	×			×	×	×			×				×						
ОК 24											×								×																					×	×							×				
ОК 25		×	×	×			×		×						×														×	×			×							×	×	×								
ОК 26					×				×				×		×		×	×		×				×	×				×			×		×		×				×						×	×			
ОК 27				×			×					×		×		×					×		×			×				×			×		×		×			×	×				×			×			
ОК 28		×	×			×		×		×	×								×			×					×	×			×		×							×						×	×	×			×	×

Завідувач кафедри із спеціальної (фахової) підготовки комп'ютерних наук
(назва кафедри)


(підпис)

Довбиш А.С.
(прізвище та ініціали)

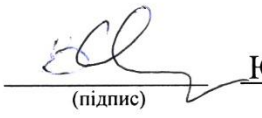
Керівник робочої проектної групи (гарант освітньої програми)


(підпис)

Шелехов І.В.
(прізвище та ініціали)

ПОГОДЖЕНО:

Начальник організаційно-методичного управління


(підпис)

Юскаєв В.Б.
(прізвище та ініціали)