Відомості про самооцінювання освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти

Загальні відомості

Інформація про ЗВО

Реєстраційний номер ЗВО (ВСП ЗВО) у ЄДЕБО	56 ВСП ЗВО - 1430
Повна назва ЗВО	Київський університет імені Бориса Грінченка
Ідентифікаційний код ЗВО	02136554
ПІБ керівника ЗВО	Огнев'юк Віктор Олександрович
Посилання на офіційний веб-сайт ЗВО	http://kubg.edu.ua
ВСП ЗВО	
Повна назва ВСП ЗВО	Університетський коледж Київського університету імені Бориса Грінченка
Ідентифікаційний код ВСП ЗВО	35823141
ПІБ керівника ВСП ЗВО	Братко Марія Василівна
Посилання на офіційний веб-сайт ВСП ЗВО	http://uk.kubg.edu.ua/

Загальна інформація про освітню програму, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	26192
Назва ОП	Безпека інформаційних і комунікаційних систем
Реквізити рішення про ліцензування спеціальності на відповідному рівні вищої освіти	Протокол засідання Ліцензійної комісії МОН України від 18.01.2018 № 81/2; Наказ МОН України від 18.01.2018 № 53-л
Цикл (рівень вищої освіти)	Другий (магістерський) рівень вищої освіти
Галузь знань, спеціальність та (за наявності) спеціалізація	Галузь знань – 12 Інформаційні технології Спеціальність – 125 Кібербезпека
Структурний підрозділ, що забезпечує реалізацію ОП	Кафедра інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	Не надається
Мова (мови) викладання	Українська
ПІБ та посада гаранта ОП	Доктор технічних наук, професор Бурячок Володимир Леонідович, завідувач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка

Загальні відомості про ОП, історію її розроблення та впровадження

Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти (далі – ОПП) розроблена на підставі Закону України «Про вищу освіту» з урахуванням рекомендацій «Магістерської програми нового покоління експертів в інформаційній безпеці», яка в рамках угоди 2013-5084/001-001 про співробітництво між Україною та Євросоюзом за підтримки Європейської комісії: агентства з освіти, культури та аудіовізуальних засобів (Tempus IV) у 2013–2017 роках впроваджувалась у ЗВО України;

ОПП розроблено проєктною групою науково-педагогічних працівників (НПП) у складі керівника групи Бурячка Володимира Леонідовича, доктора технічних наук, професора та членів проектної групи Бессалова Анатолія Володимировича, доктора технічних наук, професора, Толюпи Сергія Васильовича, доктора технічних наук, професора, Абрамова Вадима Олексійовича, кандидата технічних наук, доцента. До розроблення були долучені адміністративний склад Університету, академічна спільнота та роботодавці за фахом.

Як результат, рецензентами ОПП виступили провідні фахівці сфери захисту інформації, а саме: Смірнов Олексій Анатолійович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету (м. Кропивницький) та Татьянін В'ячеслав Вікторович, директор ТОВ «АВТОР» (м. Київ). Відгуки рецензентів позитивні. ОПП затверджено Вченою радою Київського університету імені Бориса Грінченка (протокол від 23.11.2017 № 11) та введено в дію з 01.09.2018 наказом ректора від 24.11.2017 № 762.

На початку 2018 року спеціальність 125 Кібербезпека успішно пройшла ліцензування за першим (бакалаврським) та другим (магістерським) рівнями вищої освіти (Протокол засідання Ліцензійної комісії МОН України від 18.01.2018 № 81/2; наказ МОН України від 18.01.2018 № 53-л), а у першій половині 2019 року за третім (освітньо-науковим) рівнем вищої освіти (Протокол засідання Ліцензійної комісії МОН України від 24.04.2019 № 132; наказ МОН України від 24.04.2019 № 356-л). Ліцензований обсяг за спеціальністю 125 Кібербезпека першого (бакалаврського) рівня вищої освіти – 50 осіб, другого (магістерського) рівня вищої освіти – 25 осіб, третього – 12 осіб (на 4 роки).

У лютому 2018 року наказом ректора Університету від 23.02.2018 № 107 було створено кафедру інформаційної та кібернетичної безпеки.

Поля для завантаження загальних документів:

Назва/опис документа(ів)	*Поле для завантаження документів*
* Освітня програма	http://kubg.edu.ua/informatsiya/vstupnikam/napryami-pidgotovki/magistr.html
*Навчальний план за ОП	http://kubg.edu.ua/informatsiya/vstupnikam/napryami-pidgotovki/magistr.html
Рецензії та відгуки роботодавців	Рецензії.pdf

1. Проектування та цілі освітньої програми

Мета ОПП – забезпечити студентам фундаментальну підготовку у вигляді поглиблених теоретичних і практичних знань, умінь та навичок зі спеціальності 125 Кібербезпека, достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузях телекомунікацій та ІТ.

Особливістю ОПП є те, що при її розробці, окрім рекомендацій «Магістерської програми нового покоління експертів в ІБ», проектною групою було враховано:

Стандарт вищої освіти з підготовки бакалаврів зі спеціальності 125 Кібербезпека;

Стратегія розвитку Київського університету імені Бориса Грінченка на 2018 – 2022 роки;

результати прогнозу трансформації компетентностей компанії World Economic Forum;

типовий навчальний план зі спеціальності «Кібербезпека», розроблений у 2017 році робочою групою консорціуму «Партнерство заради миру»;

міжнародні стандарти National Science Education Standards, NRC & NAP та K-4 і 9-12 «Наука і дослідження. Розвиток умінь і знань студентів», а також рекомендації міжнародної ініціативи CDIO Standard 2.1.

Окрім того особливістю ОПП є те, що вона дає можливість вступникам отримати фахову освіту, яка ґрунтується на технологіях активного навчання й унікальній матеріально-технічній базі (таблиця 1 Додатку до цих «Відомостей …») та у поєднанні з можливостями розвитку соціальних навичок є достатньою для ефективного виконання завдань інноваційного характеру в галузі телекомунікацій та ІТ.

Місією Університету є служіння людині, громаді, суспільству, а покликанням університету є сприяння особистісному та професійному розвитку успішної особистості шляхом удосконалення її природних здібностей, розкриття потенціалу та формування життєвих компетентностей. Напрями і завдання, реалізація яких забезпечує втілення місії, задекларовані в Стратегії (програмі) розвитку Київського університету імені Бориса Грінченка на 2018 – 2022 роки (розміщена на офіційному сайті Університету). Стратегія розвитку Університету в свою чергу зорієнтована на зайняття певної конкурентної позиції як на вітчизняному, так і на міжнародному ринках освітніх та інформаційних послуг.

Цілі ОПП вповні корелюються з місією та стратегією Університету, оскільки програма спрямована на забезпеченням студентам ґрунтовної підготовки та високої конкурентоспроможності на ринку праці для ефективного виконання завдань інноваційного характеру обраного ними рівня професійної діяльності в сфері ІТ технологій, відповідає корпоративним цінностям, а також передбачає налагодження зв’язків із закордонними ЗВО з метою отримання студентами подвійних дипломів.

Саме з цією метою до навчального плану з підготовки магістрів включено 7 базових дисциплін з «Магістерської програми нового покоління експертів в інформаційній безпеці» (міжнародний проект ENGENSEC, угода № 2013-5084/001-001).

Здобувачі вищої освіти та випускники програми

Спеціальність 125 Кібербезпека за другим (магістерським) рівнем вищої освіти, як вже зазначалося, пройшла ліцензування у січні 2018 року.

Під час розробки ОПП другого (магістерського) рівня вищої освіти ані здобувачів, ані випускників за спеціальністю 125 Кібербезпека в Університеті не було. Зважаючи на таке члени проектної групи при формуванні цілей та визначенні програмних результатів навчання (ПРН) враховували, зокрема, думку випускників інших ЗВО, а саме Державного університету телекомунікацій, Харківського національного університету радіоелектроніки та Національного університету «Львівська Політехніка», де зазначена вище «Магістерська програма нового покоління експертів в інформаційній безпеці» впроваджувалась протягом 2013 – 2017 років. Інтереси здобувачів вищої освіти в ОПП було враховано в меті навчання – оволодіння поглибленими теоретичними і практичними знаннями, уміннями та навичками, достатніми для ефективного виконання завдань інноваційного характеру сфери ІТ технологій.

Роботодавці

Інтереси роботодавців враховані в аспекті прагнення підготовки фахівців з розвинутими професійними компетентностями, які могли б демонструвати свої знання, уміння і

навички, необхідні для здійснення фахової діяльності у сфері ІТ технологій та ІКБ безпосередньо на робочому місці. З цією метою до формування ОПП було залучено представників роботодавців від ТОВ «АВТОР», НВК «Криптон», ТОВ «СапФоріс», ДП «Українські спеціальні системи», ДП «Державний центр інформаційних ресурсів», тощо. Одним із рецензентів ОПП було обрано досвідченого практика Татьяніна В'ячеслава Вікторовича, директора ТОВ «АВТОР» (м. Київ).

Академічна спільнота

При формулюванні цілей, фахових компетентностей та ПРН були враховані інтереси академічної спільноти, насамперед фахівців, які працюють у сфері захисту інформації з Університету Грінченка, Національного авіаційного університету та Державного університету телекомунікацій, а також дослідників з наукових установ МО, СБУ та ДССЗЗІ. Рецензентом від академічної спільноти було обрано Смірнова Олексія Анатолійовича, доктора технічних наук, професора, завідувача кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

Спільними зусиллями, за поданням представників роботодавців та академічної спільноти, було запропоновано додати до ОПП дисципліни, що пов'язані з криптографічним захистом інформації, а саме дисципліну «Математичні методи криптографії» та дисципліну «Методи побудови і аналізу криптосистем». Це дозволило конкретизувати 9-й програмний результат навчання й додати до нього пункт «Вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки».

Документальним підтвердженням такого є протоколи засідань робочих органів Університету, які відповідали за створення/оновлення ОПП – кафедри, вченої ради факультету інформаційних технологій та управління, а також Вченої ради університету.

За результатами аналізу програмних документів, які було враховано при розробці ОПП, а також за цілями і ПРН, які покладено в її основу, програма відповідає:

1) тенденціям зростання як наявних, так і потенційних викликів та загроз у сфері інформаційної та кібербезпеки (ІКБ) як в Україні, так і в усьому світі;

2) запитам щодо підготовки конкурентоспроможних фахівців сфери захисту інформації (ЗІ) для потреб освітніх, наукових і державних установ, структур спеціального призначення, центрів і служб ЗІ підприємств та банківських установ різних форм власності, тощо.

Студенти, що навчаються за ОПП будуть здатні:

виявляти та оцінювати ознаки стороннього кібервпливу, моделювати його можливі ситуації та прогнозувати його можливі наслідки;

організовувати й підтримувати комплекс заходів щодо забезпечення ІКБ з урахуванням імовірних загроз та рівня розвитку технологій захисту інформації;

проводити дослідження у напрямах забезпечення ІКБ національних інтересів України та обґрунтовувати шляхи підвищення їх ефективності;

протидіяти несанкціонованому проникненню протиборчих сторін до власних ІТ систем і мереж, забезпечувати стійкість їх роботи, а також відновлювати їх нормальне функціонування після здійснення кібернападів;

забезпечувати криптозахист власного інформаційного ресурсу тощо.

Підтвердженням такому є структурно-логічна схема навчання, що реалізується в навчальному плані другого рівня вищої освіти та конкретизується в робочих програмах навчальних дисциплін.

Під час формулювання цілей та ПРН програми було враховано *галузевий контекст* у плані визначення загальних пріоритетів сфери ІКБ та ЗІ, бачення процесу підготовки та подальшої діяльності фахівців із захисту ІТ систем та мереж, які знають: існуючі уразливості, методи їх

застосування та способи боротьби з ними; спеціальне обладнання для забезпечення мережевої безпеки; методи та способи розробки і тестування ПЗ та протидії злоякісному програмному коду; методи організації захищеної передачі даних у незахищеному середовищі; технологію розслідування інцидентів у відповідності до стандартів безпеки, тощо. Зважаючи на те, що Університет Грінченка є ЗВО комунальної форми власності підготовка студентів за ОПП спеціальності 125 Кібербезпека дозволить суттєво вплинути на вирішення задач захисту інформації як в м.Києві, так і загалом у Київському регіоні (*регіональний контекст*). З цією ж метою Університетом укладено угоди із спеціалізованим комунальним підприємством м. Києва «Київтелесервіс» (угода №152/18-ФІТУ від 05.10.2018 р.) та Департаментом ІКТ виконавчого органу КМДА (угода № УС-269/19 від 27.08.2019 р.). Це дозволило студентами спеціальності 125 Кібербезпека проходити у зазначених та інших профільних підприємствах, установах та організаціях виробничу, науково-дослідну та переддипломну практики, виконувати під керівництвом кваліфікованих співробітників зазначених установ курсові проекти та/або магістерські атестаційні роботи. Це також буде сприяти працевлаштуванню випускників ОПП.
Аналіз інформації щодо ЗВО України, які здійснюють підготовку за спеціальністю 125 Кібербезпека, показав, що серед 49 ліцензованих ЗВО лише 25 (на час розробки ОПП) готують фахівців за другим (магістерським) рівнем. Для аналізу було обрано ОПП, які знаходились у відкритому доступі. Такими ОПП є: «Адміністративний менеджмент в сфері захисту інформації» ХНУРЕ; «Кібербезпека» ТНТУ імені Івана Пулюя; «Кібербезпека» КНУ імені Тараса Шевченка; «Системи технічного захисту інформації» НТУ України «КПІ імені Ігоря Сікорського» тощо. Вивчення проводилось шляхом порівняння цілей, компетентностей і програмних результатів навчання ззазначених ОПП з «Магістерською програмою нового покоління експертів в ІБ» Євросоюзу, яка була впроваджена у ДУТ, ХНУРЕ та НУ «Львівська політехніка». Результати порівняльного аналізу дозволили в ОПП спеціальності 125 Кібербезпека врахувати такі головні аспекти активного навчання, як: індивідуальність завдання (індивідуальний набір навичок і компетентностей абітурієнта); спрямованість не на оцінку, а на результат. Зазначені аспекти було покладено до схеми формування навичок в ОПП «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти, основу якої становлять технології активного навчання (при цьому роботодавець виступає в якості замовника професійних *hard skills* навичок) і критеріїв щодо формування соціальних/універсальних *soft skills* компетентностей, а також у структурно-логічну схему проходження дисциплін.
Стандарт вищої освіти за спеціальністю 125 Кібербезпека галузі знань 12 Інформаційні технології для другого (магістерського) рівня вищої освіти відсутній.
Національна рамка кваліфікацій за 8 кваліфікаційним рівнем освіти передбачає здатність особи розв'язувати складні задачі і проблеми у певній галузі професійної діяльності та/або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог. Вимоги НРК: Знання: спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень Критичне осмислення проблем у галузі та на межі галузей знань. Уміння/навички: спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку

нових знань та процедур здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах; здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності.

Комунікація: зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема, до осіб, які навчаються.

Компетентності та результати навчання за ОПП:

Знання: Загальні компетентності ЗК1 … ЗК3. Результати навчання ПРН1 … ПРН2 Уміння/навички: Фахові компетентності ФК1 … ФК5 Результати навчання ПРН2… ПРН9 Комунікація: Результати навчання ПРН1 … ПРН2.

Таким чином, мета ОПП, а також результати навчання за нею відповідають вимогам щодо рівня, знань, умінь/навичок та засобів комунікацій, визначених Національною рамкою кваліфікацій за 8 кваліфікаційним рівнем освіти.

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?	90 кредитів ЄКТС
Яким є обсяг освітніх компонентів (у кредитах ЄКТС), спрямованих на формування компетентностей, визначених стандартом вищої освіти за відповідною спеціальністю та рівнем вищої освіти (за наявності)?	63 кредити ЄКТС
Який обсяг (у кредитах ЄКТС) відводиться на дисципліни за вибором здобувачів вищої освіти?	27 кредитів ЄКТС

Зміст ОП відповідає предметній області заявленої для неї спеціальності. Це стосується об'єкту, цілей, методів, методик та технологій ОПП. Так, об'єктами професійної діяльності випускників згідно ОПП є: об'єкти інформаційної діяльності (ОІД), комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні та ІТ системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації; процеси управління ІКБ ОІД, що підлягають захисту.

Цілями навчання є підготовка професіоналів, здатних використовувати і впроваджувати технології та застосовувати засоби ІКБ.

Теоретичний зміст предметної діяльності полягає у наданні студентам знань щодо:

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 ІР;

теорії систем управління ІКБ; сучасних ІКТ та їх програмно-апаратного забезпечення;

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;

автоматизованих систем проектування.

Дані знання студент отримує шляхом оволодіння методами, методиками та технологіями забезпечення ІКБ, використовуючи системи розробки, забезпечення, моніторингу та контролю ІКБ, а також програмно-апаратне забезпечення ІКТ, розташоване у навчальних лабораторіях Університету:

1) «*Лабораторії комп'ютерних мереж*» (дозволяє на базовому наборі обладнання Standard Core за програмою компанії Cisco Systems отримувати професійні знання в галузі

мережевих технологій та компетентності в технологіях мережевої безпеки);

2) «*Лабораторії Антивірусного захисту інформації*» (дозволяє на обладнанні та за програмами компанії ESET, опановувати технології виявлення, попередження та/або захисту від цільових APT-атак в режимі реального часу, реагувати на інциденти, швидко аналізуючи та виправляючи будь-яку проблему безпеки в мережі);

3) «*Лабораторії безпеки інформаційних активів*» (дозволяє на обладнанні компанії Dell, IBM, D-Link, MicroSoft опановувати технології виявлення кібератак й протидії ним, захисту інформації в хмарних сховищах даних, моделювання процесів підтримки рівня захищеності інформаційних активів, ліквідації наслідків застосування кіберзброї та відновлення нормальних режимів функціонування мереж управління об'єктами інформаційної і кіберінфраструктури);

4) «*Лабораторії систем технічного та криптографічного захисту інформації*» (дозволяє на обладнанні та за програмами компаній РІАС, АВТОПРОМ, КРИПТОН, АВТОР, ТОВ «ІІТ», ТОВ «ТЗІ» опановувати технології впровадження та забезпечення функціонування КСЗІ на ОІД, а також протидії НСД до ресурсів і процесів в ІТС, розробки і застосування криптомеханізмів ІКБ, обслуговування сертифікатів відкритих ключів).

Право та порядок формування індивідуальної освітньої траєторії здобувачами вищої освіти забезпечується такими нормативними документами університету: Стратегія (програма) розвитку Київського університету імені Бориса Грінченка на 2018 – 2022 роки, Положення про організацію освітнього процесу в Київському університеті імені Бориса Грінченка п. 7.2, Положення про порядок та умови здійснення вибору навчальних дисциплін, Положення про порядок реалізації права на академічну мобільність учасників освітнього процесу Київського університету імені Бориса Грінченка.

Відповідно до нормативних документів студенти мають право на:

- вибір навчальних дисциплін в обсязі, що становить не менше як 25% загальної кількості кредитів ЄКТС, передбачених відповідною освітньою програмою;
- навчання одночасно за декількома освітніми програмами, зокрема в інших ЗВО;
- обрання для вивчення додаткових навчальних дисциплін (понад встановлені 60 кредитів на рік);
- академічну мобільність;
- можливість пропонувати власні теми індивідуальних навчально-дослідних завдань, курсових, дипломних, магістерських робіт;
- можливість пропонувати бази для проходження виробничої практики.

Надання кваліфікованих консультацій щодо формування індивідуальної освітньої траєкторії та її реалізації покладається на гарантів освітніх програм, завідувачів випускових кафедр, заступників керівників структурних підрозділів.

Виконання індивідуальних освітніх траєкторій фіксується в індивідуальних навчальних планах студентів.

В Університеті порядок вибору студентами навчальних дисциплін унормовано Положенням про організацію освітнього процесу в Київському університеті імені Бориса Грінченка та Положенням про порядок та умови здійснення вибору навчальних дисциплін.

Студенту, відповідно до Положень, пропонується реалізувати своє право шляхом вибору дисциплін із переліку (каталогу курсів) чи вибору спеціалізованого блоку дисциплін.

Перелік вибіркових навчальних дисциплін формується робочими групами. Наказ на створення робочих груп та призначення їх голів видається кожного навчального року. Визначені робочою групою вибіркові навчальні дисципліни рекомендуються вченою радою факультету та затверджуються Вченою радою університету. Заходи щодо інформування студентів про можливість вибору навчальних дисциплін та сам їх вибір здійснюються у навчальному році, що передує року, в якому заплановане вивчення обраних дисциплін.

Формування варіативної складової індивідуального плану магістра здійснює випускова

кафедра разом зі студентом протягом перших двох тижнів навчання за обраною програмою.

Результати здійснення здобувачами вищої освіти вільного вибору навчальних дисциплін заслуховуються на Вченій раді університету, а заяви студентів з підсумками їх вибору зберігаються упродовж всього терміну навчання студента за певним освітнім рівнем. Обрані студентом дисципліни є складовою його індивідуального навчального плану.

В ОПП практична підготовка, що включає виробничу (ЗК1, ЗК2, ЗК3, ФК1, ФК2, ФК3), науково-дослідну (ЗК1, ЗК2, ЗК3, ФК1) та переддипломну практики (ЗК1, ЗК2, ЗК3, ФК1, ФК2, ФК3, ФК4, ФК5) формує і забезпечує як загальні, так і фахові компетентності випускника.

Основні підсумки зазначених видів практики:

виробничої – студенти закріплюють та поглиблюють теоретичні знання у сфері захисту інформації, формують професійні уміння та навички, що сприятимуть прийняттю самостійних рішень у реальних виробничих умовах, шляхом виконання окремих завдань і функцій, властивих майбутній професії;

науково-дослідної – студенти набувають досвід самостійної науково-дослідної роботи та опрацьовують методики її проведення, поглиблюють теоретичні знання у сфері захисту інформації, накопичують фактичний матеріал та отримують наукові результати, які будуть використані при написанні магістерської роботи;

переддипломної – студенти вдосконалюють набуті ними теоретичні знання, практичні уміння та навички в сфері захисту інформації та готують до захисту магістерську роботу.

Програма практики розробляється випусковою кафедрою з врахуванням побажань від баз практики, з якими укладені договори.

Крім проходження зазначених видів практик студенти набувають практичних навичок під час практичних та лабораторних занять у Центрах «Дослідження технологій захисту інформаційних ресурсів» та «Дослідження технологій функціонування і захисту ІКС та мереж», які створені на Факультеті інформаційних технологій та управління.

Освітні компоненти, що наповнюють програму підготовки магістрів з кібербезпеки, дозволяють здобувачам оволодіти комплексом соціальних/універсальних (soft skills) навичок, притаманних сучасному фахівцю. Починаючи з оволодіння здібностями креативного мислення, управління інформацією, уміння формувати власну думку та приймати рішення і завершуючи здібностями емоційного інтелекту, а також уміннями працювати в команді та вести переговори, ОПП дозволяє забезпечити формування у студентів комплексу soft skills для застосування у професійній діяльності. Цьому сприяє:

1) вивчення студентами таких дисциплін як іноземна мова професійного спрямування, організація науки і наукових досліджень та прикладна загальна теорія систем безпеки, в ході чого вони вчаться аналізувати, верифікувати, оцінювати повноту та достовірність інформації, за необхідності її доповнювати й синтезувати відсутню, продукувати нові ідеї, формувати власну думку та приймати рішення;

2) проходження студентами виробничої та науково-дослідної практик, під час яких вони вчаться налагоджувати співробітництво з колегами, проявляти лідерські якості, працювати в критичних умовах та логічно і системно мислити;

3) участь студентів у системі студентського самоврядування, у заходах мистецького спрямування, тощо, під час чого вони вчаться аналізувати явища, ситуації та проблеми, враховуючи різні параметри, фактори і причини, здійснювати новаторську діяльність, вести міжособистісне спілкування.

Професійний стандарт за спеціальністю 125 Кібербезпека галузі знань 12 Інформаційні технології для другого (магістерського) рівня вищої освіти відсутній. Професійна кваліфікація не надається.

Питання співвіднесення обсягу окремих освітніх компонентів ОПП (у кредитах ЄКТС) із фактичним навантаженням здобувачів вищої освіти (включно із самостійною роботою) регламентується Положенням про організацію освітнього процесу. Найменування освітніх компонент ОПП, їх обсяг, час викладання, форма контролю унормовані потребами ринку праці. Контактні (аудиторні) години освітніх компонентів відповідають «Магістерській програмі нового покоління експертів в інформаційній безпеці» (EACEA, Tempus IV, угода 2013-5084/001-001 про співробітництво між Україною та Євросоюзом). За необхідності, співвідношення між обсягами окремих освітніх компонентів можуть бути скореговані робочим навчальним планом. Враховуючи таке, а також вимоги ЄКТС та досвід впровадження кредитно-модульної системи в ряді Європейських країн, проєктною групою при формуванні ОПП було отримано такий розподіл залікових кредитів за циклами навчальних дисциплін: загальноосвітні: 5 (нормативна); 0 (вибіркова); фундаментальні: 8 (нормативна); 7 (вибіркова); проф.підготовка: 44 (нормативна); 20 (вибіркова); атестація: 6 (нормативна); 0 (вибіркова). За результатами опитування груп здобувачів вищої освіти, що навчаються за ОПП, було з'ясовано: обсяг навантаження є незавищеним; час, що виділений на самостійну роботу, є оптимальним.
Дуальна модель навчання реалізується в Університеті в модифікованому вигляді: організація освітнього процесу для першого рівня підготовки має практико-орієнтований характер і організовується за схемою «аудиторія – центри компетентностей – бази практик». Діяльність (робота) студентів в Центрах компетентностей спрямована на отримання вмінь і практичних навичок при формуванні (розширенні та/або поглибленні) спеціальних (фахових, предметних) компетентностей. Дуальна форма здобуття освіти в Університеті за ОПП «БІКС» другого (магістерського) рівня не здійснюється. Її планується реалізувати в рамках тристоронньої угоди № УС-269/19 від 27.08.2019 року між Університетом, Департаментом ІКТ виконавчого органу Київської міської ради (КМДА) та громадською організацією «СМАРТ СИТИ Хаб», а також в рамках угод про співробітництво з іншими потенційними роботодавцями як від КМДА, зокрема СКП «Київтелесервіс» (угода №152/18-ФІТУ від 15.10.2018 року), так і з низкою інших державних і приватних організацій (установ) України. Це передбачає проходження студентами різних видів практик у зазначених підприємствах, установах та організаціях, виконання студентами під керівництвом профільних фахівців магістерських робіт, а також розширює можливості працевлаштування випускників.

3. Доступ до освітньої програми та визнання результатів навчання

Наведіть посилання на веб-сторінку, яка містить інформацію про правила прийому на навчання та вимоги до вступників ОП	*http://kubg.edu.ua/informatsiya/vstupnikam/pravyla-pryiomu-2019.html*
Конкурсний відбір щодо вступу на навчаня за ОПП проводиться відповідно до «Правил прийому до Київського університету імені Бориса Грінченка», які розробляються, затверджуються та оприлюднюються у встановленому порядку. При вступі абітурієнти здають єдине вступне випробування з іноземної мови та фахове вступне випробування. Вступати на ОПП можуть особи, які мають диплом бакалавра, спеціаліста та/або магістра, здобуті як за спеціальністю 125 Кібербезпека, так і з інших спеціальностей, в т.ч. споріднених. Особи, які мають попередню освіту не за спеціальністю, складають в Університеті додаткове фахове випробування. Вимоги до вступних випробувань зазначаються в програмах вступних випробувань, які щорічно оновлюються та оприлюднюються на сайті університету у розділі «Вступникам».	

Перелік особливих досягнень вступника, що можуть враховуватись при обрахунку рейтингового показника, подано в Додатку 10 «Правил прийому до Київського університету імені Бориса Грінченка».

Усі питання, пов'язані з прийомом до Університету, вирішуються Приймальною комісією на її засіданнях. Рішення Приймальної комісії оприлюднюються на офіційному веб-сайті (www.kubg.edu.ua) в день прийняття або не пізніше наступного дня після прийняття відповідного рішення.

Визнання результатів навчання, отриманих в інших ЗВО, регулюються «Правилами прийому на навчання», «Положенням про організацію освітнього процесу в Київському університеті імені Бориса Грінченка» та «Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу Київського університету імені Бориса Грінченка». Документи розміщені на сайті Університету.

Зарахування кредитів, які були встановлені під час навчання на інших освітніх програмах, здійснюється за рішенням завідувача випускової кафедри на підставі документів про раніше здобуту освіту (додаток до диплома, академічна довідка, свідоцтво про підвищення кваліфікації, сертифікати та інші види документів), витягу з навчальної картки/академічної довідки у разі одночасного навчання за декількома програмами. Максимально дозволений обсяг академічної різниці при поновленні. переведенні або зарахуванні на старші курси встановлений у п. 11.1 «Положення про організацію освітнього процесу…».

За час реалізації ОПП випадків визнання результатів навчання, отриманих в інших ЗВО, не було.

Порядок визнання результатів навчання, отриманих у неформальній освіті регулюється «Положенням про організацію освітнього процесу в Київському університеті імені Бориса Грінченка» (розділ Х) та Положенням про порядок та умови здійснення вибору навчальних дисциплін студентами Університету Грінченка. Доступність документів щодо визнання результатів навчання, отриманих у неформальній освіті, забезпечується шляхом їх оприлюднення на офіційному веб-сайті Університету.

Зокрема, в межах частини дисциплін вільного вибору студенту можуть зараховуватись кредити і результати навчання, які він здобув під час навчання на відкритих навчальних он-лайн курсах (МООС, зокрема Prometeus, Cursera, Edex, CHAN Academy) з отриманням відповідних сертифікатів. Для розгляду зазначеного питання студент подає до навчальної частини заяву разом із документом, що підтверджує факт і результати навчання. Курси перезараховуються за умови відповідності їх змісту фаховому спрямуванню, мають обсяги, порівняні з обсягами вибіркових навчальних дисциплін та опановані під час навчання студента за відповідною ОПП. Рішення про зарахування кредитів і результатів навчання, отриманих в неформальній освіті, приймається випусковою кафедрою.

За бажанням студента, додатково вивчені дисципліни (модулі) можуть бути включені до його індивідуального навчального плану.

За ОПП «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти конкретних прикладів застосування процедури визнання результатів навчання, отриманих у неформальній освіті, не було.

4. Навчання і викладання за освітньою програмою

Згідно з «Положенням про організацію освітнього процесу в Київському університеті імені Бориса Грінченка» освітній процес здійснюється за такими формами: навчальні заняття; самостійна робота; практична підготовка; контрольні заходи. Основні види

навчальних занять: лекція; семінарське, практичне, лабораторне та індивідуальне заняття; консультація. У навчанні студентів перевага надається активним та інтерактивним формам занять на засадах партнерської взаємодії, що сприяє формуванню навичок критичного мислення та активної пізнавальної діяльності. В освітньому процесі за ОПП використовуються всі зазначені форми і види навчальних занять, але перевага надається практикоорієнтованим формам (практичні та лабораторні заняття). При проведенні проміжного контролю переважно використовуються усне опитування, колоквіум, письмове або комп'ютерне тестування, що має на меті перевірку рівня підготовленості студентів з конкретної теми або циклу. Формами семестрового контролю є заліки, іспити та захист курсової роботи. Іспити проходять у вигляді письмового тестування. Методи та прийоми навчання добираються викладачем самостійно і прописуються у робочій програмі навчальної дисципліни. Форма робочої програми передбачає кореляцію результатів навчання за дисципліною з програмними результатами навчання. Форми і види навчальних занять, а також методи навчання та викладання, що обираються викладачем, сприяють досягненню програмних результатів навчання.
Реалізація студентоцентрованого підходу в освітньому процесі Університету на найближчу перспективу висвітлена, зокрема, у п.3 «Стратегії (програмі) розвитку Київського університету імені Бориса Грінченка на 2018 – 2022 роки» та «Положенні про організацію освітнього процесу…». Студентоцентрованість навчання розуміється передусім як здатність Університету підготувати сучасного і конкурентоспроможного на ринку праці фахівця, з широким доступом до працевлаштування. Вибір форм і методів навчання та викладання в Університеті ґрунтується на інтерактивній взаємодії між учасниками освітнього процесу, орієнтації на результат і спільну відповідальність за нього, використанні нових інноваційних методів та/або підходів до навчання. Форми і методи навчання обираються НПП відповідно до змісту освітніх компонентів, тож їх студентоцентрованість полягає передусім у кращих практиках викладання, максимальній сформованості компетентностей та досягненню зазначених ПРН. В Університеті вже тривалий час реалізується система визначення рівня задоволеності здобувачів освіти методами навчання і викладання на ОПП. Рівень задоволеності визначається шляхом анонімного електронного анкетування, яке має назву «Викладач очима студентів». Анкета складена на компетентнісних засадах і дозволяє визначити рівень задоволеності здобувачів роботою кожного НПП. Останнє анкетування було проведено у грудні 2018 року. Результати такого опитування обговорюються на засіданнях вчених рад факультету та університету.
Згідно з «Положенням про організацію освітнього процесу…» під академічною свободою в Університеті розуміють самостійність і незалежність учасників освітнього процесу в ході провадження педагогічної, науково-педагогічної, наукової та/або інноваційної діяльності, що здійснюється на принципах свободи слова і творчості, поширення знань та інформації, проведення наукових досліджень і використання їх результатів. Різноманітність форм, методів та засобів навчання і викладання, що відображено в робочих програмах навчальних дисциплін (РПНД), можливість вибору місця проведення навчального заняття (аудиторія, Центр компетентностей, виробництво), вільний доступ до інформаційних та бібліотечних ресурсів, широкий спектр баз підвищення кваліфікації та стажування для викладачів, тощо – є яскравим підтвердженням дотримання академічних свобод в Університеті. При викладанні окремих освітніх компонентів ОПП, студентам надається можливість розглянути професійні проблеми під різними кутами зору. Використовуються такі форми як дискусії, диспути, групові заняття тощо. Здобувачі вищої освіти мають можливість будувати власну освітню траєкторію, реалізовувати своє право на академічну мобільність, брати участь в органах студентського самоврядування та

долучатися до мистецьких і культурних заходів.

Також, одним із підтверджень того, що в Університеті створено умови для забезпечення академічних свобод, є практика проведення анкетування «Викладач очима студентів».

В Університеті налагоджена система своєчасного надання інформації учасникам освітнього процесу щодо цілей, змісту та очікуваних результатів навчання, порядку та критеріїв оцінювання тощо. Основна інформація про діяльність університету розміщена на його офіційному веб-сайті. Сайт можна використовувати в україномовному та англомовному режимах.

Інформація щодо організації освітнього процесу за ОПП висвітлюється на сторінці Факультету інформаційних технологій та управління. Там оперативно оновлюється інформація для всіх студентів факультету: графік освітнього процесу, розклади занять, графік консультацій викладачів, програми семестрових іспитів з критеріями оцінювання тощо.

На сторінці випускової кафедри інформаційної та кібернетичної безпеки розміщується інформація щодо ОПП, за якими здійснюється навчання, навчальних планів (НП), РПНД тощо.

Крім інформації, яка розміщена на сайті Університету, загальна інформація про ОПП надається на організаційних зборах перед початком навчання. Також студентів ознайомлюють із особливостями роботи в електронному середовищі університету, факультету та кафедри. Для вільного користування необхідними ресурсами університету кожному студенту на період навчання надається власний логін та пароль. Інформація щодо критеріїв оцінювання у межах окремих освітніх компонентів доводиться до студентів на першому занятті з кожної дисципліни або на настановчій конференції з кожного виду практики.

Поєднання навчання і наукових досліджень під час реалізації ОПП передбачає практикоорієнтовану тактику вивчення НПП та студентами певного завдання/проблеми. Цьому сприяє відкриття в Університеті Центрів компетентностей: «Дослідження технологій функціонування та захисту інформаційно-комунікаційних систем і мереж» та «Дослідження технологій захисту інформаційних активів» У комп’ютерних класах Центрів встановлене програмно-апаратне забезпечення, яке детально описане у Додатку (табл.1 «Інформація про обов'язкові освітні компоненти ОП»). Воно дозволяє:

вивчати мови програмування високого рівня, сучасні математичні пакети та пакети прикладних програм, досліджувати особливості функціонування та захисту сучасних ОС і БД;

організовувати роботу з мережами середніх розмірів, встановлювати та конфігурувати комутатори і маршрутизатори в LAN і WAN мережах, шукати та усувати їх несправності;

будувати віртуальні конфіденційні мережі, захищені IP і TCP мережі та захищені міжмережеві з’єднання, будувати системи захисту IP-трафіка по ідеології IPSec;

обслуговувати сертифікати відкритих ключів, надавати користувачам засоби ЕЦП та шифрування даних, а також засоби генерації та управління ключами тощо;

організовувати пошук і збір інформації та досліджувати моделі її захисту;

моделювати процеси підтримки необхідного рівня захищеності інформаційних активів;

виявляти інциденти підвищеної складності та управляти ними;

виявляти радіозакладні пристрої, забезпечувати захист інформації від витоку технічними каналами, будувати системи управління ІКБ відповідно до вимог стандартів ISO, тощо.

Оволодінню зазначеним матеріалом сприяє використання, при викладанні переважної більшості фахових дисциплін, форм і методів навчання, заснованих на дослідженнях. Практикується участь здобувачів вищої освіти в наукових дослідженнях фахових кафедр та їх презентації у форматі круглих столів, студентських конференцій.

Окрім цього поєднанню навчання і досліджень сприяє створення на кафедрі студентських наукових гуртків: «Сучасні технології та проблеми безпеки ІКС» та «Проблеми інформаційно-аналітичного забезпечення систем ІКБ». Студенти беруть участь: у розробці експериментального обладнання для дослідження навантаження мережі, ідентифікації DoS-атак на мережі, організації RFID-сніффінгу, тощо; в роботі

наукових конференцій, семінарів та круглих столів з питань захисту інформації та забезпечення ІКБ; підготовці публікацій до фахових видань України (зокрема електронного наукового періодичного видання «Кібербезпека: освіта, наука, техніка», яке засновано в Університеті рішенням Вченої ради від 26.04.2018 року) та міжнародних видань, матеріали яких індексуються у наукометричних базах Scopus та WoS.

Порядок внесення змін до освітніх програм в Університеті регламентується «Методичними рекомендаціями з розроблення освітніх програм…», затверджених наказом ректора від 29.03.2018 № 206. Зміст освітніх компонентів оновлюється, за потребою, кожним НПП напередодні навчального року. Це відображається в його РПНД.

РПНД розглядається та затверджується на засіданні випускової кафедри. Її зміст узгоджується з гарантом ОПП та затверджується проректором з науково-методичної та навчальної роботи. Порядок внесення змін та підстави для цього визначені пп.1.11. 1.12, 1.13 «Методичних рекомендацій з розроблення робочих програм навчальних дисциплін».

Низовою ланкою цього процесу, зокрема в сфері захисту інформації, є кафедра інформаційної та кібернетичної безпеки. На засіданнях кафедри обговорюються структурно-логічні схеми проходження навчальних дисциплін, навчальні плани та робочі програми навчальних дисциплін ОПП «Безпека інформаційних і комунікаційних систем».

Аргументовані та науково доведені зміни, запропоновані учасниками освітнього процесу, затверджуються на засіданні кафедри й виносяться на розгляд і затвердження вченої ради Факультету. Викладачі кафедри постійно беруть участь у важливих професійних організаційних і науково-практичних зібраннях (семінарах, конференціях, круглих столах тощо), на яких обговорюються сучасні практики та наукові досягнення у сфері захисту інформації. Це дозволяє вносити корективи до змісту навчальних занять, не відхиляючись від затвердженої робочої програми навчальної дисципліни. Прикладом такому є внесення змін до назви та змісту навчальної дисципліни «Технології безпеки мережевої інфраструктури», назву якої після підписання тристоронньої угоди між Університетом, Департаментом ІКТ КМДА та громадською організацією «СМАРТ СИТИ Хаб» (№ УС-269/19 від 27.08.2019 р.) та обговорення такої можливості на міжкафедральному семінарі (кафедри інформаційної та кібернетичної безпеки та кафедри комп'ютерних наук і математики) Факультету інформаційних технологій та управління було вирішено змінити на «Технології безпеки мережевої та Smart інфраструктури».

В ході міжкафедрального семінару було запропоновано оновити список рекомендованої літератури, а також внести зміни в тематику курсової та магістерської роботи.

Порядок реалізації права на академічну мобільність учасників освітнього процесу в Університеті регламентовано «Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу Київського університету імені Бориса Грінченка». Організаційний супровід цих завдань покладено в Університеті на НДЛ інтернаціоналізації вищої освіти.

За час реалізації ОПП прикладів академічної мобільності ще не було, але кафедра активно працює у цьому напрямку. Так, наприклад, з грудня 2018 року кафедру ІКБ залучено до участі у спільному міжнародному проекті (Україна – КНР) бенефіціарами якого зі сторони КНР є корпорації Beijing Zhongshi Chengda Science & Trade Co., Ltd (Пекін) та Jiangyin Sinorus Technology R & D Center Co., Ltd (Цзян Інь). На стадії узгодження за програмою Еразмус+ знаходяться проекти співробітництва з:

компанією Limerick Institute of Technology (LIT), Ірландія;

університетом Collegium Civitas (Варшава, Польща).

Це сприятиме міжнародному обміну студентами та НПП у поєднанні з освітнім процесом, їх участі у міжнародних конференціях в сфері захисту інформації, проведенню стажування НПП в університетах Європи та Китаю, а також участі НПП у професійних об'єднаннях за спеціальністю (наприклад, «Internet Society»).

5. Контрольні заходи, оцінювання здобувачів вищої освіти та академічна доброчесність

Види контрольних заходів визначені в Положенні про організацію освітнього процесу… у п. 9.3.4. В освітньому процесі використовуються такі види контролю: вхідний, проміжний та підсумковий.

Вхідний контроль проводиться на початку вивчення базової (профільної) навчальної дисципліни з метою визначення готовності студентів до її засвоєння. Проміжний контроль проводиться на всіх видах аудиторних занять протягом семестру по закінченню кожного змістового модуля і має на меті перевірку рівня підготовленості студентів з конкретної теми (набору тем, циклу тощо). Форми проведення проміжного контролю та критерії оцінювання визначаються у робочій програмі. Підсумковий контроль включає семестровий контроль (заліки, іспити, захист курсової роботи) та випускну атестацію студентів. Форма проведення семестрового контролю, зміст і структура екзаменаційних матеріалів та критерії оцінювання визначаються рішенням випускової кафедри та відображаються в робочих програмах навчальних дисциплін.

Нормативні форми атестації визначаються навчальним планом. Екзаменаційні вимоги до змісту дипломних, магістерських робіт / проектів, програми випускних екзаменів розробляє випускова кафедра.

Чіткість та зрозумілість форм контрольних заходів та критеріїв оцінювання навчальних досягнень здобувачів вищої освіти забезпечуються ґрунтовним підходом кафедри до їх планування і формулювання; своєчасним висвітленням на сайті факультету відповідної інформації; проведенням поточних та екзаменаційних консультацій.

Формами контрольних заходів, які обрані в ОПП «БІКС» для оцінювання досягнутих результатів навчання, є:

проміжний контроль (опитування, модульна контрольна робота, тестування),

семестровий контроль, який проводиться у формі заліку або іспиту.

Атестація здобувачів освіти здійснюється у формі захисту кваліфікаційної магістерської роботи. Вибір форми контрольних заходів відбувається на етапі підготовки навчального плану: освітні компоненти, результати яких передбачають більш практичне наповнення, завершуються заліком, освітні компоненти більш теоретичного або теоретико-практичного наповнення – екзаменом.

Форми поточного контролю навчальних досягнень, включених до ОПП, передбачають оцінювання результатів: роботи студента на заняттях (робота на семінарському /практичному занятті оцінюється максимум в 10 балів); самостійної роботи (максимум 5 балів за кожну роботу); виконання модульного контролю (максимум 25 балів за одну роботу); індивідуального навчально-дослідного завдання (максимум в 30 балів).

Підсумковий контроль навчальних досягнень за дисципліною проводиться у формі заліку або іспиту. Всі іспити за ОПП письмові. До складання іспиту допускаються студенти, які виконали всі види робіт, передбачені навчальним планом та РПНД і які за результатами проміжного контролю сумарно набрали не менше 35 балів. Студенти, які набрали менше ніж 35 балів, до складання іспиту не допускаються.

За результатами проміжного контролю під час вивчення навчальної дисципліни студент може набрати до 60 балів включно, а за екзамен – до 40 балів включно. Загальне оцінювання здійснюється на підставі суми результатів проміжного і підсумкового контролю знань (екзамену). З навчальних дисциплін, формою підсумкового контролю яких є залік, підсумкова оцінка виставляється, як правило, за результатами проміжного контролю. Результати заліків оцінюються за стобальною шкалою відповідно до кількості набраних балів, і, як правило, оголошуються на останньому практичному, семінарському чи лабораторному занятті. Оцінка виставляється за умови, коли студент успішно виконав усі види робіт для проміжного контролю, передбачені РПНД.

Оцінювання результатів складання комплексних екзаменів та/або захисту дипломних, магістерських робіт / проектів здійснюється у порядку, визначеному в Положенні Університету про порядок створення та організацію роботи Екзаменаційної комісії.

Зазначені форми контрольних заходів у межах навчальних дисциплін ОПП дозволяють перевірити досягнення програмних результатів навчання завдяки тому, що на етапі укладання РПНД формування змісту контрольних заходів проводиться відповідно до результатів дисципліни, які відповідають програмним результатам ОП.

Механізми проведення контрольних заходів, шляхи оцінювання об'єктивності екзаменаторів, процедури запобігання та врегулювання конфлікту інтересів, а також порядок оскарження результатів контрольних заходів та їх повторного проходження визначені в «Положенні про організацію освітнього процесу у Київському університеті імені Бориса Грінченка».

Вимоги до зазначення видів і форм контрольних заходів, а також критеріїв оцінювання знань студентів визначені в «Методичних рекомендаціях з розроблення робочих програм навчальних дисциплін». РПНД ОПП «Безпека інформаційних і комунікаційних систем» розміщені на сайту Університету на сторінці кафедри ІКБ. Інформація про форми контрольних закладів та критерії оцінювання здобувачам вищої освіти дається і уточнюється кілька разів:

1) на початку вивчення кожної дисципліни (кожним НПП);

2) на сайті структурного підрозділу (оновлюється щосеместрово).

Протягом року серед студентів проводяться усні опитування гарантом програми щодо чіткості та зрозумілості критеріїв оцінювання їх навчальних досягнень, а також вчасності та доступності інформації про форми контрольних заходів.

Стандарт вищої освіти за спеціальністю 125 Кібербезпека галузі знань 12 Інформаційні технології для другого (магістерського) рівня вищої освіти відсутній.

В ОПП «»Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня формою атестації є захист кваліфікаційної магістерської роботи. Це відповідає рекомендаціям міжнародного проекту ENGENSEC «Магістерська програма нового покоління експертів в інформаційній безпеці» (угода №2013-5084/001-001 про співробітництво між Україною та Євросоюзом).

Процедура проведення контрольних заходів, їх види та форми в Університеті регулюються «Положенням про організацію освітнього процесу в Київському університеті імені Бориса Грінченка», яке розміщене на сайті Університету. Форми контрольних заходів та критерії їх оцінювання відображаються в робочих програмах навчальних дисциплін.

Доступність форм контрольних заходів та критерії їх оцінювання для учасників освітнього процесу досягається:

відображенням в РПНД, які розміщені на сторінці кафедри інформаційної та кібернетичної безпеки сайту Університету;

оприлюдненням графіку навчального процесу, розкладів занять, графіків заліково-екзаменаційних сесій, програм іспитів, графіків атестації тощо на сторінці Факультету інформаційних технологій та управління у рубриці «Студентам».

Об'єктивність екзаменаторів при оцінюванні знань студентів в процесі підсумкового семестрового контролю забезпечується передусім впровадженням до переліку форм його проведення письмової екзаменаційної роботи або тестового електронного екзаменаційного завдання. Екзамени в Університеті, зокрема і за ОПП «Безпека інформаційних і комунікаційних систем», проводяться у письмовій формі, або у вигляді комп'ютерного тестування. В обох випадках роботи студентів проходять шифрування. Перевірка письмових робіт здійснюється протягом робочого дня у день написання, перевірка

виконання тестових завдань здійснюється автоматично.

У випадку, коли специфіка навчальної дисципліни унеможливлює письмовий контроль результатів, передбачається усний контроль за умови присутності іншого викладача.

Екзамен в усній формі приймається комісією (2-3 особи), до якої входить щонайменше один фахівець, що не брав участі у викладанні цієї дисципліни студентам, котрі екзаменуються

Студент, який вважає, що на екзамені викладач оцінив відповідь не об'єктивно, у результаті чого відбулося заниження оцінки, то у день оголошення оцінки студент може подати в навчальний відділ апеляцію на ім'я керівника структурного підрозділу.

За період навчання магістрів за програмою, що акредитується, конфлікту інтересів не виникало. Скарг студентів на упередженість та необ'єктивність екзаменаторів не було.

Порядок повторного проходження контрольних заходів урегульовується «Положенням про організацію освітнього процесу в Київському університеті імені Бориса Грінченка» п.9.4.

Академічна заборгованість з певної навчальної дисципліни виникає у разі одержання студентом незадовільного балу за результатами підсумкового контролю. Студенти, які одержали під час заліково-екзаменаційної сесії не більше двох незадовільних оцінок (FX), мають право ліквідувати академічну заборгованість у встановлені строки, як правило, до початку наступного семестру. Студенти, які не ліквідували академічні заборгованості у встановлені строки, відраховуються з Університету.

Перескладання екзамену допускається не більше двох разів з кожної дисципліни: один раз – викладачу, другий – комісії. Якщо студент під час складання екзамену комісії отримав незадовільну оцінку, то він відраховується. Студенти, які одержали під час заліково-екзаменаційної сесії три і більше незадовільних оцінок (FX), відраховується з Університету за невиконання індивідуального навчального плану (за академічну неуспішність).

За період навчання магістрів за програмою, що акредитується, до повторного проходження контрольних заходів було залучено 5 студентів, які не в повному обсязі виконали програму навчання. Конфлікту інтересів не виникало. Скарг студентів на упередженість та необ'єктивність екзаменаторів не було. Під час проходження повторного навчання академічна заборгованість була ліквідована.

Порядок оскарження процедури та результатів проведення контрольних захів регулюється «Положенням про організацію освітнього процесу в Київському університеті імені Бориса Грінченка».

Студент, який вважає, що на екзамені викладач оцінив відповідь не об'єктивно, у результаті чого відбулося заниження оцінки, у день оголошення оцінки може подати до навчального відділу апеляцію на ім'я керівника структурного підрозділу. За розпорядженням керівника структурного підрозділу або особи, що його заміняє, створюється комісія у складі: екзаменатора, який приймав екзамен, іншого викладача відповідного профілю, завідувача кафедри та заступника керівника з науково-методичної та навчальної роботи.

Розгляд апеляції проводиться з метою визначення об'єктивності виставленої оцінки.

Якщо екзамен був письмовий, то розглядається лише письмова робота. Додаткове опитування студента не проводиться. Засідання апеляційної комісії відбувається, як правило, наступного дня після отримання заяви студента. Підсумкова оцінка, виставлена комісією, є остаточною і апеляції та перескладанню не підлягає.

Результати контрольних заходів, проведених з використанням комп'ютерної техніки, доступні для проведення апеляції в установлені строки.

За період навчання магістрів за програмою, що акредитується, оскарження процедури та результатів проведення контрольних заходів не було. Конфлікту інтересів не виникало. Скарг студентів на упередженість та необ'єктивність екзаменаторів не було.

В Університеті політика та процедури дотримання академічної доброчесності більш детально відображені у таких нормативно-правових документах:

Стратегія розвитку Університету, п.4.3 (*http://kubg.edu.ua/resursi/dokumenti.html*);

Кодекс корпоративної культури (*http://kubg.edu.ua/resursi/dokumenti.html*);

Декларація про академічну доброчесність науково-педагогічного, наукового, педагогічного працівника Університету (*http://kubg.edu.ua/images/stories/podii/2016/ declaratsiia _vykladachi.pdf*);

Декларація про академічну доброчесність студента, аспіранта, докторанта Університету (*http://kubg.edu.ua/images/stories/podii/2016/declaratsiia_student.pdf*).

«Положення про організацію освітнього процесу..» (*http://kubg.edu.ua/images/stories/Departaments/vdd/documenty/rozdil_10/nakaz_817_15.12.2017.pdf*)

Відповідно до «Положення про організацію освітнього процесу…» здобувачі вищої освіти у випадку порушення академічної доброчесності можуть бути притягнені до відповідальності шляхом повторного проходження оцінювання (контрольна робота, іспит, залік тощо); повторного проходження відповідного освітнього компонента освітньої програми; відрахування з Університету; позбавлення академічної стипендії; позбавлення наданих пільг з оплати навчання. Як інструменти протидії порушенням академічної доброчесності на ОПП використовуються регулярне

інформування НПП щодо потреби запобігати академічній недоброчесності;

система перевірки курсових і магістерських робіт на антиплагіат, тощо.

Процедура обов'язкової перевірки магістерських робіт на наявність текстових запозичень започаткована в Університеті наказом ректора Університету від 30.05.2014 року. Перевірка здійснюється співробітником бібліотеки університету за допомогою спеціального ПЗ (Unicheck) і є безкоштовною для всіх учасників освітнього процесу.

В університеті наявна електронна база магістерських робіт.

Процедура інформування НПП щодо потреби запобігати академічній недоброчесності при вивченні освітніх компонентів в Університеті закріплена обов’язковим підписанням НПП відповідної декларації.

У 2018 році частина аудиторій навчального корпусу №1, в якому ведеться підготовка здобувачів за ОПП, була обладнана відеокамерами, що унеможливлює списування при проведенні письмових іспитів.

Академічна доброчесність є частиною корпоративної культури Університету.

Окрім того, що в Університеті ведеться постійна роз'яснювальна робота серед викладачів та студентів, всі представники академічної спільноти університету на добровільних засадах ознайомлюються та підписують декларацію про дотримання академічної доброчесності. Шляхом підписання декларації співробітники та студенти університету підтверджують свій намір здійснювати власну освітню, наукову, творчу діяльність, дотримуючись місії, візії, цінностей, корпоративної культури Університету, найвищих моральних і правових норм академічної доброчесної поведінки, керуючись загальнолюдськими нормами людяності й моралі, нормами законодавства України, етичними вимогами до професійної, освітньої та наукової діяльності.

Крім того, підписуючи декларацію, учасники освітнього процесу підтверджують розуміння того, що у разі порушення цієї Декларації нестимуть відповідальність перед академічною спільнотою Університету згідно із загальнолюдськими нормами моралі та законодавства

При написанні власних магістерських робіт та опублікуванні результатів досліджень у фахових виданнях України та збірниках студентських наукових праць здобувачі вищої освіти спеціальності 125 Кібербезпека дотримуються політики, стандартів і процедур академічної доброчесності, що впроваджені в Університеті та які для них є особистісною мотивацією і переконанням.

Відповідно до «Положення про організацію освітнього процесу…» здобувачі вищої освіти можуть бути притягнені до відповідальності шляхом повторного проходження оцінювання (контрольна робота, іспит, залік тощо); повторного проходження відповідного освітнього компонента освітньої програми; відрахування з Університету; позбавлення академічної стипендії; позбавлення наданих пільг з оплати навчання.

У разі виявлення академічного плагіату у змісті кваліфікаційної роботи здобувача освіти, така кваліфікаційна робота не допускається до захисту, а студент вважається таким, що не виконав вимоги до підготовки кваліфікаційної роботи магістра. Відповідне рішення фіксується у протоколі засідання кафедри.

Використання студентом під час екзамену матеріалів, не передбачених програмою екзамену і не дозволених екзаменатором, не допускається. У разі виявлення факту списування під час проведення екзамену, у студента вилучається аркуш письмової відповіді, а студент вважається таким, що отримав незадовільну оцінку.

У випадках, коли під час шифрування письмових екзаменаційних робіт виявлено роботу, на якій є особливі позначки, що можуть розкрити її авторство, робота не шифрується і таку роботу, крім екзаменатора, додатково перевіряє завідувач кафедри.

За час реалізації ОП випадків виявлення порушень академічної доброчесності не було.

6. Людські ресурси

Конкурсний добір викладачів регламентується Положенням про конкурс на заміщення вакантних посад науково-педагогічних, педагогічних і наукових працівників. В Положенні передбачені процедури, направлені на оцінювання рівня професіоналізму претендента на посаду НПП (п.22). Так, для оцінювання рівня професійної кваліфікації претендента на посаду НПП кафедра може запропонувати йому прочитати пробні лекції, провести практичні заняття, за результатами яких складається відгук про відкрите заняття. Кандидатури претендентів попередньо обговорюються на кафедрах. За результатами обговорення складається мотивований висновок про професійні якості кожного з претендентів. Рішення про рекомендацію/не рекомендацію приймається кафедрою шляхом таємного голосування. Під час конкурсного добору беруться до уваги наступні показники: наявність відповідної освіти, наукового ступеня, вченого звання; наукова діяльність претендента, досвід роботи, рейтинг викладача за результатами щорічного конкурсу «Лідер року», оцінка діяльності викладача здобувачами освіти через опитування «Викладач очима студентів», рівень трудової дисципліни.

Науково-педагогічні працівники, які викладають на ОПП, мають відповідну освіту та вагомі здобутки в науковій і професійній сферах. Серед штатних працівників 4 доктори наук та 7 кандидатів наук. Два викладача кафедри 29 жовтня 2019 захистили дисертаційні роботи на здобуття наукових ступенів кандидата технічних наук за спеціальністю 05.13.06 «Інформаційні технології».

До організації та реалізації освітнього процесу Університет активно залучає роботодавців. Прикладами такому є залучення до рецензування ОПП кандидата технічних наук, старшого наукового співробітника Татьяніна В’ячеслав Вікторович, директор ТОВ «АВТОР» (м. Київ), а до роботи Екзаменаційної комісії за ОПП «БІКС» - начальника Департаменту інформаційної безпеки НЕК «УкрЕнерго», кандидата технічних наук Валерія Віталійовича Єрмошина.

Кафедрою ІКБ підписані та реалізуються угоди як з державними, так і з комерційними підприємствами (установами). Серед них: компанії «РІАС» та НДІ «АВТОПРОМ», НВФ «КРИПТОН», ТОВ «АВТОР», ТОВ «Інститут інформаційних технологій», ТОВ «Технічний захист інформації», ТОВ «Сапфоріс» (представництво компанії ESET в Україні) та ТОВ «D-Link» (представництво компанії D-Link в Україні), Державне

підприємство «Українські спеціальні системи», Державне підприємство «Державний центр інформаційних ресурсів» тощо. Предметом Угод є науково-технічне співробітництво у сфері кіберзахисту та захисту інформації в ІТ системах та мережах, спрямоване на забезпечення ІКБ, удосконалення вимог до криптографічного та технічного захисту інформації в умовах посилення кіберзагроз, в межах повноважень і компетенції кожної зі Сторін, проведення підготовки/перепідготовки та підвищення кваліфікації власних кадрів шляхом реалізації спільних семінарів і курсів, проведення всіх видів практик і стажувань студентами Університету.

Кафедра залучає до аудиторних занять на ОПП професіоналів-практиків, представників роботодавців, запрошуючи їх для проведення лекційних і практичних занять та тренінгів. Так, Дмитро Петрущенко, заступник директора спеціалізованого комунального підприємства м.Києва «Київтелесервіс» та Юрій Назаров, директор Департаменту ІКТ виконавчого органу КМДА залучені до керівництва відповідно виробничою та науково-дослідною практиками студентів.

На кафедрі на посаді доцента за зовнішнім сумісництвом працює к.т.н. Рой Яніна Володимирівна, яка є завідуючою відділу технічного захисту інформації Департаменту інформаційної безпеки НЕК «УкрЕнерго» (викладає дисципліни «Прикладні аспекти аналізу та синтезу політик безпеки», «Управління ризиками та інцидентами безпеки» та «Методи та засоби управління інформаційною безпекою» бакалаврського рівня вищої освіти), а на посаді старшого викладача Таджділні Махіяр, який є штатним співробітником ТОВ «SI Center» (викладає дисципліни «Безпека безпроводних, мобільних та хмарних технологій», «Безпека Web ресурсів», «Основи захисту конфіденційних даних» бакалаврського рівня вищої освіти).

Відгуки здобувачів освіти про навчальні заняття, які проводять викладачі-практики, схвальні. Проблем організаційного характеру щодо проведення таких занять не спостерігалось. Результативність процедури залучення до аудиторних занять на ОПП професіоналів-практиків, експертів галузі, представників роботодавців підтверджується результатами анкетування «Викладач очима студентів».

Сприяння професійному розвиткові викладачів ОПП становить цілісну систему. В університеті існує постійно діюча система підвищення кваліфікації, яка складається з наступних модулів: лідерський, науковий, дидактичний, ІКТ модуль. Зміст модулів адаптовано під потреби НПП в залежності від займаної посади. Крім того, НПП проходять фахове стажування в інших ЗВО один раз на 5 років, відповідно до «Положення про підвищення кваліфікації науково-педагогічних працівників Університету». Для НПП, які нещодавно працевлаштувались, проводиться адаптаційний тренінг та за необхідності призначається тьютор в особі досвідченого викладача.

НПП кафедри ІКБ, що забезпечують освітній процес за ОПП «БІКС» вживають також заходи щодо власного професійного розвитку. Головними установами-партнерами кафедри, в цьому процесі є: ПАТ УкрТелеком «Центр післядипломної освіти»; ТОВ «Елан»; ТОВ «РДЛ»; НВФ «Криптон»; НТУУ «КПІ ім.Сікорського», Вінницький НТУ, Blekinge Institute of Technology (Karlscrona, Sweden), тощо.

У зазначених установах свій професійний рівень підвищили практично всі НПП кафедри.

Протягом 2018 – 2019 років НПП кафедри взяли участь у роботі понад 6 НПК:: Всеукраїнській НПК «Безпека соціально-економічних процесів у кіберпросторі» 27.03.2019; НТК «Наукоємні технології в інфокомунікаціях» 23-25.05.2019; VII міжнародній НТК «Захист інформації і безпека інформаційних систем» 30-31.05.2019; НПК ESET Security Days 06.06.2019 ; міжнародній НПК «Інтелектуальні системи та ІТ» 19 – 24.08.2019 .

В університеті створена система заохочення викладачів за досягнення у фаховій сфері. Ці питання відображені в «Стратегії (програмі) розвитку Київського університету імені Бориса Грінченка на 2018-2022 роки» (п.2.2).

Також є «Положення про щорічне рейтингове оцінювання професійної діяльності науково-педагогічних і наукових працівників Київського університету імені Бориса Грінченка «Лідер року»», нова редакція якого затверджене наказом ректора від 24.01.2019 № 34-а За результатами рейтингу визначається рівень професійної діяльності викладача, результати рейтингу враховуються при укладанні контракту та наданні рекомендації щодо покращення професійної діяльності. Відповідно до рейтингу визначаються переможці конкурсу «Лідер року», які отримують диплом та матеріальне заохочення.

Питання морального заохочення регламентуються «Положенням про відзнаки Київського університету імені Бориса Грінченка», затвердженого наказом ректора від 28.12.2018 № 853.

З метою розширення можливостей для професійного розвитку працівників в Університеті згідно «Стратегії (програми) розвитку Київського університету імені Бориса Грінченка на 2018-2022 роки» створено «Школу професійного зростання для науково-педагогічних працівників, які не мають педагогічної освіти».

7. Освітнє середовище та матеріальні ресурси

В університеті проводиться постійна робота над поліпшенням матеріально-технічної бази. Відповідні заходи є складовою як Стратегії (програми) розвитку Київського університету імені Бориса Грінченка на 2018-2022 роки, так і щорічних планів. Планування фінансових потреб та їх забезпечення регулюється планово-економічним відділом бухгалтерії за погодженням із керівником ЗВО, в т.ч. з урахуванням пропозицій від структурних підрозділів.

Матеріально-технічні ресурси забезпечують досягнення визначених ОПП цілей та ПРН. Так, в навчальному приміщенні, де здійснюється освітній процес за ОПП:

є достатня кількість аудиторій та 17 комп'ютерних класів, які мають необхідне програмне забезпечення. Перелік обладнання та ПЗ спеціалізованих комп'ютерних лабораторій, які забезпечують виконання навчального плану за ОПП, подано в таблиці 1.

бібліотечний фонд за спеціальністю відповідає Ліцензійним умовам;

створена необхідна соціальна інфраструктура (в наявності дві актові зали, три спортивні зали, басейн, їдальня та буфет, медичний пункт; обладнані місця для відпочинку та культурного дозвілля студентів).

Навчально-методичне забезпечення ОПП дає можливість досягати визначених програмою цілей та програмних результатів навчання завдяки його максимальній змістовій насиченості та постійному оновленню. Студенти мають доступ до навчально-методичних матеріалів, оскільки ті своєчасно розміщуються на сайті університету.

Освітнє середовище, створене в університеті, дозволяє задовольнити потреби та інтереси здобувачів вищої освіти ОПП завдяки збалансованості матеріальних ресурсів (обладнання аудиторій, лабораторій, комп'ютерних класів, центрів практичної підготовки, тренінгових центрів, виділення та оформлення простору для відпочинку студентів тощо) та сприйняття студентів як рівноправних партнерів у вибудові їх освітньої траєкторії, відповідності критеріям студентоцентрованого навчання.

В університеті задля виявлення і врахування потреб та інтересів студентів проводяться регулярні зустрічі зі студентським самоврядуванням, студентське самоврядування залучене до процедур внутрішнього забезпечення якості освіти. Всі здобувачі вищої освіти мають можливість спілкуватися з ректором університету, проректорами через електронну пошту чи безпосередньо. Регулярно відбуваються зустрічі з гарантом

програми та представниками кафедри.З метою вдосконалення ОП, внесення змін в робочі навчальні програми, організацію освітнього процесу проводиться щорічне опитування «Викладач очима студентів».

Університет забезпечує безпечність освітнього середовища для життя та здоров'я здобувачів вищої освіти суворим дотриманням норм техніки безпеки, постійним інструктуванням НПП та здобувачів вищої освіти, проведенням заходів, які стосуються здорового способу життя тощо. Питання безпеки є складовою Стратегії (програми) розвитку Київського університету імені Бориса Грінченка на 2018-2020 роки (п.10). Єдина система організації роботи з охорони праці та безпеки життєдіяльності визначена у «Положенні про організацію роботи з охорони праці та безпеки життєдіяльності учасників освітнього процесу в Київському університеті імені Бориса Грінченка» та інших документах, які оприлюднені на сайті університету.

Освітнє середовище Університету забезпечує не тільки безпечні умови навчання та праці, а також комфортну міжособистісну взаємодію, дотримання прав і норм фізичної, психологічної, інформаційної та соціальної безпеки кожного учасника освітнього процесу.

Підтримка психічного здоров'я здобувачів освіти забезпечується шляхом створення загальної доброзичливої атмосфери співробітництва та підтримки на кафедрі, факультеті та в університеті. За необхідності, психологічна консультація може бути надана НПП університету, які мають відповідну освіту (в університеті здійснюється підготовка психологів, яку забезпечують дві кафедри Інституту людини).

За час реалізації ОП звернень щодо проблем психічного здоров'я не було.

Комунікація зі студентами ОПП здійснюється шляхом очного спілкування під час освітнього процесу або через електронне середовище Університету. З усіх питань, що стосуються організації освітнього процесу, студенти можуть звертатись як до гаранта ОПП та навчального відділу, так і безпосередньо до керівництва Факультету. Здобувачі освіти можуть контактувати з НПП та іншими співробітниками Університету, включаючи керівництво, через корпоративну електронну пошту. В перший місяць після прийому на навчання помічник декана з ІКТ створює для студентів корпоративні електронні скриньки, які одночасно використовуються для доступу до електронного середовища Університету. Адреси електронної пошти всіх співробітників розміщені на сайті Університету.

Суттєвих недоліків описаної системи комунікації за час реалізації ОП не виявлено.

Механізми освітньої, організаційної, інформаційної, консультативної та соціальної підтримки здобувачів вищої освіти виступають як складові єдиної системи. Інформація щодо змін у розкладі навчальних занять, графіків навчального процесу, заборгованості по оплаті за навчання, замовлення довідок з місця навчання тощо доводиться до здобувачів освіти навчальним відділом Факультету. За консультаціями щодо навігації в системі електронного навчання університету, користування електронними сервісами, відновлення паролів тощо здобувачі освіти звертаються, здебільшого, до помічника декана з ІКТ. Уся необхідна для студентів інформація, включаючи розклад занять, розміщується на сайті Факультета та постійно оновлюється. Консультаційна підтримка студентів здійснюється гарантом ОП та, за необхідності, іншими співробітниками Факультету. Навчальні консультації відбуваються згідно графіка консультацій, розміщеному на веб-сторінці кафедри, або за попередньою домовленістю з викладачем. Організаційна підтримка освітнього процесу здобувачів освіти ОП здійснюється навчальним відділом Факультету. Соціальною підтримкою студентів опікується студентська профспілка Університету таа заступник декана з навчально-методичної та соціально-гуманітарної роботи. За необхідності студентам надається ліжко-місце в гуртожитку Університету. Студенти, що належать до певних соціальних категорій, за погодженням з Департаментом освіти і науки Київської міської державної адміністрації, переводяться на навчання за кошти регіонального бюджету. За умови вступу до

профспілки Університету, студенти, які навчаються за кошти регіонального бюджету, один раз на рік можуть отримати матеріальну допомогу. За час реалізації ОП здобувачі освіти не зверталися за підтримкою щодо вирішення їх соціальних проблем. Наведені факультетські та університетські структури дозволяють надавати в повному обсязі освітню, організаційну, інформаційну, консультативну та соціальну підтримку здобувачам вищої освіти. Опитування щодо рівня задоволеності здобувачів освіти щодо зазначених видів підтримки заплановане на грудень 2019 року.
Університет створює достатні умови для реалізації права на освіту особам з особливими освітніми потребами. Зокрема, у навчальному корпусі за адресою вулиця Маршала Тимошенка, 13-Б, де здійснюється навчання за ОПП, проведені роботи з облаштування безбар'єрного середовища та встановлення горизонтальної платформи з похилим підйомом. Корпус також обладнаний ліфтами. У навчальному корпусі за адресою бульвар Ігоря Шамо, 18/2 встановлені пандуси, введений в експлуатацію пасажирський ліфт, обладнані спеціальні санітарні кімнати для осіб з інвалідністю. Встановлений пандус і при вході в приміщення Університетського коледжу. Для врахування потреб студентів та надання їм додаткової підтримки створено Ресурсний центр підтримки студентів з інвалідністю. Згідно концепції діяльності Центру, підтримка має бути технічною, психологічною, педагогічною та соціально-педагогічною. Супровід розпочинається з моменту звернення людини з інвалідністю до Університету й охоплює процеси підготовки до вступу, навчання та працевлаштування. Фахівцями Ресурсного центру здійснюється спеціальна підготовка викладачів до роботи в інклюзивних групах, проводяться майстер-класи, тренінги з вирішення проблем педагогічної взаємодії зі студентами з інвалідністю. Серед здобувачів вищої освіти на ОПП, що акредитується, особи з особливими потребами відсутні.
Політику та процедури врегулювання конфліктних ситуацій (включаючи пов'язаних із сексуальними домаганнями, дискримінацією) регулюються Положенням про засади запобігання і протидії дискримінації, сексуальним домаганням, булінгу та іншим проявам неетичної поведінки. Положення розроблено з метою забезпечення рівних можливостей щодо реалізації прав і свобод усіх співробітників та здобувачів освіти, підтримання в Університеті середовища, вільного від дискримінації, сексуальних домагань, булінгу, принижень честі та гідності особи. Університет не толерує і не толеруватиме дискримінацію, сексуальні домагання, булінг, приниження честі та гідності людини у будь-якій формі, оскільки така поведінка суперечить законодавству України, Статуту, Кодексу корпоративної культури, не відповідає місії та цінностям Університету. Дія Положення поширюється на всіх співробітників і здобувачів освіти та стосується поведінки під час освітнього процесу та/або виконання посадових обов'язків, а також поведінки, що пов'язана з освітнім процесом або виконанням посадових обов'язків. В зазначеному Положенні описані: обов'язки співробітників і здобувачів освіти; процедура повідомлення про дискримінацію, сексуальні домагання, булінг та інші прояви неетичної поведінки; процедура розгляду скарг. Розгляд відповідних скарг здійснюється Комісією з етики, персональний склад та строк повноважень, якої затверджується згідно з наказом ректора. Скарги, які подані здобувачами освіти та стосовно здобувачів освіти, розглядаються розширеним складом Комісії з етики за участю представників з числа здобувачів освіти. Доступність політик і процедур щодо врегулювання конфліктних ситуацій (включаючи випадки дискримінації, сексуальних домагань або корупції) забезпечується за рахунок розміщення інформації щодо основних заходів запобігання та способів сповіщення про такі ситуації на сайті Університету.

У питаннях протидії корупції Університет керується Законом України «Про запобігання корупції». На офіційній веб-сторінці Університету розміщена інформація щодо основних заходів, спрямованих на запобігання, виявлення та протидії корупції. До відома співробітників та здобувачів освіти доведена інформація щодо способу повідомлення про прояви корупції в Університеті**.** Повноваження щодо питань запобігання та виявлення корупції покладені на радника ректора з правових та кадрових питань.

Під час реалізації ОП випадків скарг, пов'язаних із випадками дискримінації, сексуальних домагань або корупції, не було.

8. Внутрішнє забезпечення якості освітньої програми

Моніторинг освітніх програм є важливою складовою системи внутрішнього забезпечення якості вищої освіти Університету.

Процедури розроблення, затвердження, моніторингу та періодичного перегляду ОП регулюються «Методичними рекомендаціями з розроблення освітніх програм», введеними в дію наказом ректора від 29.03.2018 № 206 .

Розробку, впровадження та реалізацію ОП здійснюють відповідні робочі групи (проєктні групи, групи забезпечення спеціальностей). Їх функції чітко визначені п.2.7. «Методичних рекомендацій…». Перегляд та оновлення ОП відбувається з урахуванням: періоду акредитації ОП; вимог державних стандартів, стандартів вищої освіти, професійних стандартів; висновків та пропозицій роботодавців та здобувачів вищої освіти; стратегії (програми) розвитку університету тощо.

Внесення змін до навчального плану ОП в частині уточнення назв освітніх компонентів, структурно-логічної схеми навчання, форм контролю, відбувається за обґрунтованим поданням проєктної групи, погодженим із НМЦ стандартизації та якості освіти. Рішення про затвердження відповідних змін в описі ОП та навчальному плані приймається вченими радами структурних підрозділів. Внесені зміни оформлюються окремим додатком і є невід'ємною складовою ОП.

Так, наприклад, до ОПП, що акредитується, зміни були внесені у 2019 році за ініціативи Департаменту інформаційно-комунікаційних технологій КМДА, з яким на основі підписаної тристоронньої угоди за № УС-269/19 від 27.08.2019 між ним, Університетом та громадською організацією «СМАРТ СИТИ Хаб» здійснюється тісна співпраця. Зміни до ОПП зумовлені необхідністю розширення компетентностей майбутніх фахівців в контексті сучасних SMART-технологій. Потреба у вказаних вище компетентностях була виявлена при аналізі відповідних публікацій, консультацій з роботодавцями в різних галузях науки і економіки сучасного високотехнологічного інформаційного суспільства (влада, державний і бізнес сектора економіки держави, тощо), а також потреб громади та влади міста Києва у створенні комфортної та ефективної цифрової інфраструктури міста.

Зміни стосуються об'єктів вивчення та діяльності, змісту і назви однієї із фахових дисциплін, а саме дисципліни «Технології безпеки мережевої інфраструктури». Її назву змінено на «Технології безпеки мережевої та SMART- інфраструктури». При цьому було уточнено фахові компетентності та програмні результати навчання.

Внесені зміни затверджені в установленому в Університеті порядку.

Здобувачі вищої освіти вже під час вибору спеціальності мають доступ до перегляду ОПП на сайті Університету. До процесу періодичного перегляду ОП та інших процедур забезпечення її якості їх залучають для проведення:

- опитувань щодо змісту конкретних дисциплін;
- робочих нарад зі студентами різних курсів;
- вибіркового опитування серед учасників щодо певних процесів (вибір дисциплін,

звернення до навчального відділу тощо).

Думка здобувачів щодо якості викладання на ОПП збирається шляхом проведення анонімного електронного анкетування «Викладач очима студентів». Пропозиції студентів щодо удосконалення ОПП збираються також безпосередньо під час освітнього процесу шляхом спілкування з гарантом програми, НПП випускової кафедри та адміністрацією факультету. Окрім цього здобувачі вищої освіти, які входять до складу вченої ради факультету, мають змогу поставити свої питання та надати пропозиції щодо змісту ОПП на відповідних засіданнях вченої ради Факультету, науково-методичних семінарах.

Програма, затверджена у 2018 році, глибокому перегляду ще не підлягала. Планується залучення здобувачів вищої освіти до обговорення та перегляду ОПП по завершені навчання набору 2018 – 2019 навчального року у грудні 2019 року у вигляді: проведення анонімного опитування щодо змісту програми в цілому та конкретних дисциплін; робочої наради для обговорення ОПП в цілому та окремих дисциплін.

До процесу періодичного перегляду ОП та інших процедур внутрішнього забезпечення якості освіти в Університеті активно залучаються органи студентського самоврядування.

Згідно з «Положенням про студентське самоврядування в Київському університеті імені Бориса Грінченка» органи студентського самоврядування беруть участь в обговоренні та вирішенні питань удосконалення освітнього процесу, науково-дослідної роботи, призначення стипендій, організації дозвілля, оздоровлення, побуту та харчування (п.2.2); беруть участь у заходах (процесах) щодо забезпечення якості вищої освіти (п.2.4); делегують своїх представників до робочих, консультативно-дорадчих органів (Конференція трудового колективу Університету, інститутів, коледжу, Вчена рада Університету, Вчені ради інститутів, методична рада коледжу, Стипендіальна комісія Університету ін.) (п.2.6); вносять пропозиції щодо змісту навчальних планів і програм (п.2.10).

На сторінці Факультету інформаційних технологій та управління розміщені документи, які відображають діяльність Студентської ради факультету.

Студенти ОПП «Безпека комунікаційних і інформаційних систем» не балотувались до складу студентської ради Факультету.

Університет до організації та реалізації освітнього процесу активно залучає роботодавців. Одним із прикладів такому є участь роботодавців у роботі Екзаменаційних комісій, що регламентується відповідним положенням.

Випусковою кафедрою підписані угоди з: компанією «РІАС», НДІ «АВТОПРОМ», НВФ «КРИПТОН», ТОВ «АВТОР», ТОВ «Інститут інформаційних технологій», «Технічний захист інформації», ТОВ «Сапфоріс» (представництво компанії ESET в Україні),а «D-Link» (представництво компанії D-Link в Україні), ДП «Українські спеціальні системи», «Державний центр інформаційних ресурсів», ТОВ «Інститут комп'ютерних технологій», Департаментом ІКТ КМДА та громадською організацією «СМАРТ СИТИ Хаб»,тощо. Співпрацю з вищезазначеними організаціями забезпечують випускова кафедра та особисто гарант програми.

Під час проходження студентами практик, проводиться опитування керівників від баз практики щодо змісту ОПП. Обговорення ОПП та змісту її окремих освітніх компонентів відбувається на накових конференціях і семінарах, зокрема в ході Круглого столу «Кібербезпека: освітній аспект» (КУБГ, Київ), Cyber Security & Intelligent Manufacturing Conference (Changsha, China), Конкурсу проектів «Програма розвитку лідерських компетентностей студентів» (Британська Рада, Kiev), міжнародного форуму фахівців із ІКБ «Інформаційна безпека: актуальні тренди — 2018» (КУБГ, Київ) та II International Conference on Computer Science, Engineering and Education Applications (КПІ-2019, Київ).

В Університеті сформовано чітку систему збирання інформації щодо кар'єрного шляху випускників університету. Цим займається відділ практики та працевлаштування НМЦ

стандартизації та якості освіти. Працівник відділу здійснює контроль та підведення підсумків працевлаштування випускників; готує статистичну інформацію, яка аналізується на засіданнях Вченої ради університету та фахівцями Департаменту освіти і науки Київської міської державної адміністрації (з метою корегування регіонального замовлення).

На сайті університету у розділі «Випускникам» (*http://kubg.edu.ua/informatsiya/klub-vipusknikiv/oholoshennia.html*) розміщується оперативна інформація: про діяльність Клубу випускників, про наявні вакансії для працевлаштування тощо. На сайті також розміщено Анкету випускника, яка дозволяє проводити періодичний моніторинг щодо працевлаштування випускників Університету.

Незважаючи на те, що ОПП «Безпека інформаційних і комунікаційних систем» проходить первинну акредитацію й випуску за цією програмою ані на першому (бакалаврському), ані на другому (магістерському) рівнях ще не було, випусковою кафедрою опрацьовано алгоритм збирання інформації щодо кар'єрного шляху та траєкторій працевлаштування випускників.

Згідно «Положення про організацію освітнього процесу в Київському університеті імені Бориса Грінченка» внутрішнє забезпечення якості освіти в Університеті реалізується через такі заходи:

–моніторинг якості освітнього процесу;

–психолого-педагогічний супровід адаптаційних періодів;

–постійне оновлення і удосконалення навчально-методичного забезпечення;

–розроблення та впровадження в практику нових освітніх програм і удосконалення та оновлення навчальних планів;

–внесення необхідних змін до змісту підготовки фахівців;

–упровадження інноваційних технологій і підходів;

–неперервне підвищення кваліфікації науково-педагогічного персоналу;

–забезпечення публічності інформації про ОПП, ступені вищої освіти та кваліфікації;

–забезпечення дотримання академічної доброчесності працівниками Університету та здобувачами вищої освіти, у тому числі створення і забезпечення функціонування ефективної системи запобігання та виявлення академічного плагіату.

З метою реалізації зазначених процедур протягом звітного періоду 2018 - 2020 років за ОПП «Безпека інформаційних і комунікаційних систем» в Університеті було проведено:

– самоаналіз стану підготовки фахівців (формування контингенту студентів, кадрове, матеріально-технічне, організаційне, навчально-методичне та інформаційне забезпечення підготовки фахівців тощо);

– аналіз успішності та якості знань студентів (грудень-січень 2018 року та травень-червень 2019 року);

– анкетування студентів «Викладач очима студентів» (щорічно);

– оновлення робочих програм навчальних дисциплін з обов’язковим їх обговоренням на засіданнях кафедри та зазначенням ресурсів, наявних у фондах бібліотеки (основної літератури, фахових періодичних видань, електронних, мультимедійних ресурсів тощо);

Недоліки ані в ОПП «БІКС», ані в освітній діяльності з реалізації ОПП не виявлені.

Для забезпечення освітнього процесу за ОПП «БІКС» переважна більшість навчальних дисциплін другого (магістерського) рівня вищої освіти була забезпечена електронними навчальними курсами. Наразі процес створення таких курсів триває.

Спеціальність 125 Кібербезпека, в рамках якої відкрита ОПП «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня отримала ліцензію на початку 2018 року (Протокол засідання Ліцензійної комісії МОН України від 18.01.2018 № 81/2; наказ МОН України від 18.01.2018 № 53-л). ОПП проходить первинну акредитацію.

Учасники академічної спільноти Університету (адміністрація, НПП, слухачі підготовчих відділень, студенти, аспіранти, докторанти, тощо) змістовно залучені до процедур внутрішнього забезпечення якості ОПП. Зокрема вони :

обговорюють питання якості освіти і процедури їх забезпечення (на засіданнях кафедр та вчених рад інститутів/факультетів, Вченої ради університету);

забезпечують викладання на високому науково-теоретичному і методичному рівні навчальних дисциплін ОПП;

підвищують власний професійний рівень, педагогічну майстерність та/або наукову кваліфікацію;

дотримуються норм академічної доброчесності, педагогічної етики та моралі;

розвивають в осіб, які навчаються, самостійність, ініціативність, творчі здібності;

формують у здобувачів освіти критичне мислення, креативність, ініціативність і підприємливість, навички самопізнання, самоусвідомлення самоосвіти тощо.

виховують осіб, які навчаються, у дусі українського патріотизму і поваги до Конституції України та державних символів України, тощо.

Одними із важливих чинників змістовності залучення до внутрішньої системи забезпечення якості усіх учасників академічної спільноти є корпоративний стандарт Університету та Кодекс корпоративної культури Університету.

Здійснення процесів і процедур внутрішнього забезпечення якості освіти в університеті відбувається в зоні відповідальності декількох підрозділів Університету.

1. НМЦ стандартизації і якості освіти здійснює комплексний аналіз якості освітнього процесу, вивчає інноваційні ідеї і досвід в галузі освіти, вивчає та узагальнює стан організації навчальної та методичної роботи кафедр, здійснює моніторинг якості освітніх послуг, здійснює контроль та підведення підсумків усіх видів практик студентів та працевлаштування випускників тощо.

2. НМЦ акредиації та ліцензування здійснює періодичний моніторинг відповідності кадрового складу, матеріально-технічної бази, бібліотечних ресурсів тощо Ліцензійним умовам та іншим нормативним документам.

3. НДЛ інтернаціоналізації освіти відповідає за академічну мобільність студентів та НПП.

4. НМЦ досліджень, наукових проектів та програм організує та координує НДДКР.

У свою чергу, в навчальних структурних підрозділах повноваження щодо здійснення процедур внутрішнього забезпечення якості розподілені між кафедрами, навчальною частиною і адміністрацією факультету. Загальне керівництво процесами забезпечення якості освіти в структурних підрозділах здійсню декан/директор.

Розподіл функціональних обов'язків, повноважень та прав цих підрозділів, а також алгоритм їх взаємодії викладений і відповідних Положеннях, які розміщені на сайті Університету.

9. Прозорість і публічність

Права та обов'язки усіх учасників освітнього процесу в Університеті регулюються документами, розробленими з урахуванням вимог чинного законодавства. Це:

Статут Київського університету імені Бориса Грінченка (*http://kubg.edu.ua/resursi/dokumenti.html*);

Правила внутрішнього розпорядку (*http://kubg.edu.ua/resursi/dokumenti.html*);

Кодекс корпоративної культури (*http://kubg.edu.ua/images/stories/regulations/reg_docs/corp_code_new.pdf*);

Корпоративна угода про участь у розбудові Київського університету імені Бориса Грінченка (*http://kubg.edu.ua/images/stories/regulations/reg_docs/ugoda_new.pdf*);

Положення про організацію освітнього процесу» (*http://kubg.edu.ua/images/stories/Departaments/vdd/documenty/rozdil_10/nakaz_817_15.12.2017.pdf*);

Положення про ректорат *(http://kubg.edu.ua/images/stories/Departaments/vdd/documenty/rozdil_1/nakaz_32_30_01_17.pdf);*

Положення про кафедру (*http://kubg.edu.ua/images/stories/Departaments/vdd/polozhennia_kafedra_03_01_17.pdf*). Решта документів, якими регулюється права та обов'язки усіх учасників освітнього процесу, своєчасно оприлюднюються на сайті Університету у розділі «Ресурси – Реєстр нормативної бази». В залежності від мети та змісту документів вони проходять обговорення на Вчених радах інститутів/факультетів та Університету, на загальних зборах трудового колективу тощо.
http://fitu.kubg.edu.ua/pro-fakultet/kafedry/2016-06-16-07-27-25/pro-kafedru.html
Адреса веб-сторінки, на якій розміщена освітня програма http://kubg.edu.ua/informatsiya/vstupnikam/napryami-pidgotovki/magistr.html

11. Перспективи подальшого розвитку ОП

Сильні сторони ОПП «БІКС» 1) ОПП відповідає тенденціям розвитку спеціальності та ринку праці, враховує галузевий і регіональний контекст, досвід аналогічних вітчизняних та іноземних ОПП. ОПП ґрунтується на інноваційних технологіях активного навчання, має чітко сформульовані цілі, які визначені з урахуванням позицій і потреб стейкхолдерів та відповідають місії і стратегії Університету. ОПП передбачає практичну підготовку студентів та набуття ними необхідних hard skills та soft skills навичок. 2) Правила прийому та правила визнання результатів навчання за ОПП є чіткими, прозорими і зрозумілими. Форми навчання і викладання є студентоцентрованими, забезпечують академічні свободи, базуються на основі найновіших досягнень і сучасних практик викладання та проведення досліджень. Форми контрольних заходів та критерії оцінювання знань оприлюднюються заздалегідь й дають можливість об'єктивно встановити рівень досягнення студентами результатів навчання для окремого освітнього компонента та ОПП в цілому. 3) Політики, стандарти і процедури дотримання академічної доброчесності за ОПП є чіткими і зрозумілими. Академічна і професійна кваліфікація НПП, задіяних в реалізації ОПП, забезпечує досягнення визначених програмою цілей та ПРН. Добір НПП здійснюється на конкурсній основі. До освітнього процесу Університет активно залучає роботодавців. 4) Університет має чітку систему розроблення, затвердження, моніторингу та періодичного перегляду ОПП. Це дозволяє залучати всіх стейхолдерів та вчасно реагувати на виявлені недоліки. Постійному розвитку ОПП сприяє сформована в Університеті внутрішня система забезпечення якості освіти. 5) Правила і процедури, що регулюють права та обов'язки всіх учасників освітнього процесу, послідовно дотримуються під час реалізації ОПП. **Слабкі сторони ОПП «БІКС»** 1) Недостатня залученість здобувачів освіти до процесів моніторингу якості ОПП. 2) Обмежена можливість надання студентам відомостей (стандартів, нормативних документів, указів та постанов), що містять інформацію, вимоги щодо захисту якої встановлені законодавчими актами. 3) Недостатній рівень допуску студентів до інформації з обмеженим доступом при проходженні практики на відповідних базах.
Перспективи розвитку ОПП «БІКС» другого (магістерського) рівня вищої освіти упродовж найближчих років пов'язані з затвердженням стандарту за спеціальністю 125

Кібербезпека, що буде вимагати перегляду та приведення ОПП у відповідність до нього.

За умови впровадження професійного стандарту в ОПП мають бути внесені зміни щодо неврахованих вимог стейхолдерів.

При подальшій реалізації ОПП будуть посилені міждисциплінарні зв'язки, проведений моніторинг працевлаштування випускників та їх задоволення здобутою освітою в контексті займаних посад.

Реалізація зазначених перспектив дозволить підвищити якість підготовки студентів за ОПП, розробити та запровадити програми перепідготовки фахівців споріднених галузей та підвищення кваліфікації фахівців за спеціальністю.

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

Назва освітнього компонента	Вид компонента (дисципліна/курсова робота/практика/дипломна робота/інше)	Поле для завантаження силабуса або інших навчально-методичних матеріалів	Якщо викладання навчальної дисципліни потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
Іноземна мова професійного спрямування	Навчальна дисципліна	РНП кіб.pdf	**Лінгафонний комплекс Sanako Lab 90** Інтерактивна дошка SMART Board ПК Intel Core 2 Duo, 512 МБ, 230 Гб ПЕОМ: Intel Celeron CPU 1.80 GHz., навушники Sven GD- 010 MV **Лінгафонний комплекс Sanako Lab 90** Інтерактивна дошка SMART Board ПК Intel Core 2 Duo, 512 МБ, 230 Гб ПЕОМ: Intel Celeron CPU 1.80 GHz., навушники Sven GD- 010 MV
Організація науки і наукових досліджень	Навчальна дисципліна	http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/5к/V_Buriachok_ONND.pdf	**Лабораторія вбудованих систем та 3-D моделювання** Комп'ютер тип#1 Сервер на базі NetNavigatorE, E3-1230V, 16 Гб Комп'ютер тип#2 ПК, Intel Core i3 4160, 4 Гб Комп'ютер тип#3 ПК Intel Core 2 Duo, 512 МБ, 230 Гб Спеціальне обладнання ВС: Навчальна плата Arduino Mega 2560 R3 Плата розширення Danger-Shield Bausant (Spark Fan) Плата розширення mSD-Shield v2 (Datenlogger Shield) Покроковий потенціометр Drehencoder mit Taster PEC12R-4225F-S0024 Плата розширення GLCD-Shield mit Dispay Плата розширення Ethernet-Shield R3 (Arduino) Навчальна плата для програмування Raspberry Pi 2 Modell B ARM Cortex-A7 Quad Core Плата розширення Shield-Bridge (Raspberry Pi Arduino Adapter) Навчальна плата STM32F4-Discovery Плата розширення MI0283AV2 Adapter v2 Плата Intel Galileo Плата Altium NanoBoard 3000 Двоколісна демонстраційна модель Formula Flowcode Buggy Макет лабіринту (Maze walls) **Лабораторія GOLDi із можливістю віддаленої роботи** *електромеханічна система, цифрова плата швидкого прототипування, відеокамера, інтерфей)* 3D-принтер Leapfrog Creatr HS 3D-сканер III-D Scanner Gotcha Інтерактивна дошка SMART Board
Прикладна загальна теорія систем безпеки	Навчальна дисципл	http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/5к/V_Buriachok_PZTSB.pdf	

<table>
<tr><td>Моніторинг, аудит та адміністрування захищених IT систем і мереж</td><td>Навчальна дисципліна</td><td>http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/5к/A_Anosov_MAAZ.pdf</td><td><u>Центр дослідження технологій захисту інформаційних ресурсів</u>
<u>Лабораторія технічного захисту інформації</u>
Детектор (індикатор) поля PROTECT 1210i
Детектор (індикатор) поля PROTECT 1206i
Скануючий приймач IC-R20
Багатофункціональний пошуковий прилад ST-033 «Піранія»
Виявник прихованих відеокамер
Антена рамкова жорстка "PIAC-1АЖ"
Генератор акустичного шуму "PIAC-2ГС"
Вібровипромінювач п'єзоелектричний "PIAC-2ВП"
Випромінювач акустичний "PIAC-2ВА"
Квадрокоптер DJI Mavic PRO
Контроллер Matrix-II Net
Застосування обладнання лабораторії дозволяє студентам Університету отримувати знання щодо виявлення радіозакладних пристроїв, забезпечення захисту об'єктів інформаційної діяльності від витоку конфіденційної інформації акустичними і віброакустичними каналами, а також забезпечення контролю та управління доступом на об'єктах інформаційної діяльності з використанням ПЗ захисту ІзОД від НСД в АС класу “1” (автономна ПЕОМ) та класу “2” (ЛОМ), а саме системи “Лоза”, комплексу засобів захисту (КЗЗ) “Гриф”, комплексу засобів захисту (КЗЗ) “Рубіж”</td></tr>
<tr><td rowspan="2">Технології безпеки мережевої та Smart інфраструктури</td><td>Навчальна дисципліна</td><td rowspan="2">http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/Технології_безпеки_мережевої_та_Smart_інфраструктури_КБ pdf</td><td rowspan="3"><u>Центр дослідження технологій функціонування і захисту ІКС та мереж</u>
<u>Лабораторія комп’ютерних мереж</u>
Комп'ютер тип#1 Intel Core i3 3.0GHz, 4GB RAM, 1000GB HDD, 22” LED. Кількість: 12+1 ПК
Міжмережевий екран ASA5506-K8
Комутатор WS-C2960+24TC-L
Роутер Cisco ISR 4321 Sec bundle w/SEC license
Інтерфейсна карта Cisco HWIC-2T
Комутатори Catalyst 3650 24 Fast 4x1 G
Інтерактивна дошка SMART Board
Інтерактивна дошка SMART Board</td></tr>
<tr><td>Курсова робота</td></tr>
<tr><td>Технології безпеки безпроводових і мобільних мереж</td><td>Навчальна дисципліна</td><td>http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/5к/V_Sokolov_TBBMM.pdf</td></tr>
</table>

<table>
<tr><td>Технології розслідування інцидентів безпеки</td><td>Навчальна дисципліна</td><td>http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/5к/Yu_Borsukovskyi_TRIB.pdf</td><td rowspan="4"><u>Центр дослідження технологій захисту інформаційних ресурсів</u>
<u>Лабораторія безпеки інформаційних активів</u>
Сервер Dell PE R530
Сервер Dell PE R530
Сервер HP ProLiant
KBM-перемикач з підтримкою USB-периферії
Міжмережевий екран FG-100E-BDL-EU – 1 шт.
Комутатор TP-Link T2600G-52TS
Комутатор Mikrotik Cloud Smart Switch CSS326-24G-2S+
Маршрутизатор (router) Cisco
Точка доступу Cisco
Комп'ютер тип#1 Dell OptiPlex 3050 Micro Form Factor – 15 шт.
Комп'ютер тип#2 Dell Precision Tower 3620 XCTO BASE – 1 шт.
Дошка магнітна крейдово-маркерна обертова на колесах
Точка wi-fi доступу Linksys
Cisco SB WAP 121 (WAP 121-E-K9-G5).
Екран для проектора настінний Walfix з механізмом повернення 150" (4:3) 300x225 см
Проектор на стелю мережевий NEC P603X
БФП HP LaserJet Pro M130nw (G3Q58A) + USB cable
Мережева карта Panda Wireless PAU09 N600 Dual
Мережеве сховище Internet Download Manager Synology DS718+
Контур інформаційної безпеки «SearchInform» у складі NetworkSniffer та EndpointSniffer та контур управління інформаційною безпекою «Digital Security» у складі DS Office та DS LifeCycle Management System</td></tr>
<tr><td>Прикладні аспекти тестувань на проникнення та етичного хакінгу</td><td>Навчальна дисципліна</td><td>http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/5к/V_Sokolov_PATPEH.pdf</td></tr>
<tr><td>Технології безпеки Web-ресурсів</td><td>Навчальна дисципліна</td><td>http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/5к/V_Sokolov_TBWR.pdf</td></tr>
<tr><td>Технології протидії злоякісному програмному коду</td><td>Навчальна дисципліна</td><td>http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/Технології_протидії_злоякісному_програмному_коду_КБ_6курс_Семко_1.pdf</td><td rowspan="2"><u>Центр дослідження технологій захисту інформаційних ресурсів</u>
<u>Контур забезпечення всебічного захисту корпоративної мережі</u> ESET Enterprise Inspector
ESET Security Management Center 7;
ESET Remote Administrator;
ESET Enterprise Inspector;
ESET Endpoint Antivirus 7.0.2100.4;
ESET Security Agent;
ESET Targeted Attack Protection;
ESET Mail Security for Microsoft Exchange Server 7.0.10024.0;
ESET File Security for Microsoft Windows Server 7.0.12018.0.
<u>Контур захисту інформації в хмарних сховищах даних</u> від компанії IBM
Security QRadar SIEM;
Security AppScan;
Security Network Intrusion Prevention System</td></tr>
<tr><td>Технології розробки і тестування ПЗ мережевої безпеки</td><td>Навчальна дисципліна</td><td>http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/5к/V_Semko_TRTPZMB.pdf</td></tr>
</table>

Математичні методи криптографії	Навчальна дисципліна	http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/5к/А_Bessalov_ММК.pdf	**<u>Центр дослідження технологій захисту інформаційних ресурсів</u>** **<u>Лабораторія криптографічного захисту інформації</u>** Ноутбук тип#1 Dell Inspiron 15/500 Series IntelCore i5-8250u cpu, 1.8 Ghz, 8 Gb ОЗУ **Програмно-апаратний комплекс "Центр сертифікації ключів"** **(виробництва ТОВ «Інститут інформаційних технологій», м.Харків)** Електронні ключі Кристал-1 – 15 шт. **Програмно-апаратний комплекс криптографічного захисту IP трафіку CryptoIP** **(виробництва ТОВ АВТОР, м.Київ).** Смарт-карта CryptoCard-337 – 6 шт. Електронний USB-ключ SecureToken-337 – 6 шт. Електронний ключ SecureToken-337F – 6 шт.
Методи побудови і аналізу криптосистем	Навчальна дисципліна	http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/Методи_побудови_і_аналізу_криптосистем_КБ_6курс_Бессалов.pdf	
Виробнича (технологічна) практика	практика	http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/11.05/ВИРОБНИЧА_практика_КБ_6_курс.pdf	Виробнича, науково-дослідна та переддипломна практики проводяться згідно укладених угод на підприємствах, в організаціях, науково-дослідницьких та інших установах, що спеціалізуються на наданні послуг в сфері інформаційних технологій та інформаційної безпеки, банках, страхових компаніях, компаніях-операторах зв'язку та інших, що мають у складі своєї структури підрозділ, що відповідає за інформаційну безпеку, або в будь-яких організаціях, де використовуються технічні засоби обробки, зберігання та передачі конфіденційної інформації з використанням наявного спеціального обладнання закладу згідно складених договорів про співпрацю. В ході виробничої практики студенти закріплюють та поглиблюють теоретичні знання у сфері захисту інформації, формують професійні уміння та навички, що сприятимуть прийняттю самостійних рішень у реальних виробничих умовах, шляхом виконання окремих завдань і функцій, властивих майбутній професії. Під час науково-дослідної – студенти набувають досвід самостійної науково-дослідної роботи та опрацьовують методики її проведення, поглиблюють теоретичні знання у сфері захисту інформації, накопичують фактичний матеріал та отримують наукові результати, які будуть використані при написанні магістерської роботи. На переддипломній практиці студенти вдосконалюють набуті ними теоретичні знання, практичні уміння та навички в сфері захисту інформації, здобувають професійний досвід для самостійної трудової діяльності та готують до захисту магістерську роботу.
Науково-дослідна практика	практика	http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/11.05/НАУКОВО-ДОСЛІДНА_практика_КБ_6_курс.pdf	
Переддипломна практика	практика	http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/РНП/11.05/ПЕРЕДДИПЛОМНА_практика_КБ_6_курс.pdf	
Підготовка кваліфікаційної магістерської роботи	Магістерська робота	http://fitu.kubg.edu.ua/images/stories/Departments/kikb/2019/Met_rek.pdf	Виконання кваліфікаційної магістерської роботи здійснюється на базах практик з використанням наявного обладнання закладу згідно складених договорів про співпрацю. Для роботи з науковою літературою надається доступ до наукометричної реферативної міжнародної бази даних Web of Science компанії Clarivate Analytics. Для статистичної обробки результатів наукових дослідження використовується ліцензійні програмні продукти фірми Microsoft (Microsoft Office) і IBM (IBM SPSS Statistics). Захист кваліфікаційних магістерських робіт проводиться в аудиторних кабінетах, які обладнані мультимедійними комплексами (проектор, SMART-дошка, комп'ютер).
Захист кваліфікаційної магістерської роботи	Магістерська робота		

Таблиця 2. Зведена інформація про викладачів

ПІБ викладача	**Посада**	**Чи входить у групу забезпечення відповідної спеціальності?**	**Навчальні дисципліни, що їх викладає викладач на ОПП**	**Обґрунтування**
ФЕДОРЧУК Ірина Володимирівна	Старший викладач кафедри іноземних мов	Ні	Іноземна мова професійного спрямування	**Освіта:** Ніжинський державний університет імені Миколи Гоголя,.2007 р.. Спеціальність: «*Педагогіка та методика середньої освіти. Мова та література (англійська, німецька)*». Кваліфікація: «*Вчитель мови (англійської, німецької) та зарубіжної літератури*». **Науковий ступінь:** немає. **Вчене звання:** немає. **Види і результати професійної діяльності особи за спеціальністю відповідно до п.30 Ліцензійних умов провадження освітньої діяльності:** **п.п. 30.1), 30.2), 30.6), 30.13).** ***30.1) Наявність за останні п'ять років наукових публікацій у періодичних виданнях, які включені до наукометричних баз, рекомендованих МОН, зокрема Scopus або Web of Science Core Collection.*** ***Наукометричні бази Scopus або Web of Science Core Collection або інші науко метричні бази*** 1. Федорчук І. В. Інтернаціоналізація вищої педагогічної освіти: досвід Азербайджану, Вірменії, Грузії / Федорчук І. В. // Science and Education a New Dimension. Pedagogy and Psychology. – Budapest, 2014. – II (12). – Issue 25. – P. 72–75. (журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Index Copernicus, SCRIBD, UlrichsWeb). 2. Doghonadze N. Recent Research in Black Sea Region on Motivation in Education (Review) / Natela Doghonadze, Iryna Fedorchuk // Journal of Education in Black Sea Region. – 2016. – Vol. 1, Issue 2. – P. 2–17. – Режим доступу : https://jebs.ibsu.edu.ge/jms/index.php/jebs/article/view/15/14 (журнал включено до міжнародних каталогів наукових видань і наукометричних баз: ERIC, International Scientific Indexing, ResearchBib, Open Academic Journals Index, JIFACTOR, InfobaseIndex, Global Index Factor). ***30.2) Наявність не менше п'яти наукових публікацій у наукових виданнях, включених до переліку наукових фахових видань України*** 1. Федорчук І. В. Особливості організації вищої педагогічної освіти в умовах інтернаціоналізації освітнього простору в Азербайджані, Вірменії та Грузії / І. В. Федорчук // Вісник Чернігівського національного педагогічного університету імені Т. Г. Шевченка. Серія: Педагогічні науки / голов. ред. М. О. Носко. – Чернігів: ЧНПУ, 2015. – Вип. 131. – С. 158–162. 2. Федорчук І. В. Дослідницька діяльність студентів педагогічних спеціальностей у країнах кавказького регіону (Азербайджан, Вірменія, Грузія) / І. В. Федорчук // Наукові записки Ніжинського державного університету імені Миколи Гоголя. Сер. : Психолого-педагогічні науки. – 2017. – № 2. – С. 178–183. ***30.6) Проведення навчальних занять із спеціальних дисциплін іноземною мовою в обсязі не менше 50 аудиторних годин на навчальний рік.*** 2018-2019 н. р. - дисципліна «Іноземна мова» для студентів спеціальності 125 Кібербезпека першого (бакалаврського) рівня. Мова викладання – англійська. (*166 аудиторних годин на навчальний рік*). 2019-2020 н. р. – дисципліна «Іноземна мова» для студентів спеціальності 125 Кібербезпека першого (бакалаврського) рівня. Мова викладання – англійська. (*166 аудиторних годин на навчальний рік*). 2019-2020 н. р. – дисципліна «Іноземна мова професійного спрямування» для студентів спеціальності 125

				Кібербезпека другого (магістерського) рівня. Мова викладання – англійська. (*102 аудиторних години на навчальний рік*). ***30.13) Наявність виданих навчально-методичних посібників/посібників для самостійної роботи студентів та дистанційного навчання, конспектів лекцій/ практикумів/ методичних вказівок/рекомендацій загальною кількістю три найменування*** 1. Курс у системі електронного навчання Moodle Київського університету імені Бориса Грінченка для студентів спеціальності 125 Кібербезпека першого (бакалаврського) рівня. (розроблено, на стадії сертифікації) 2. Курс у системі електронного навчання Moodle Київського університету імені Бориса Грінченка для студентів спеціальності 125 Кібербезпека другого (магістерського) освітнього рівня. (розроблено, на стадії сертифікації).
БУРЯЧОК Володимир Леонідович	Завідувач кафедри інформаційної та кібернетичної безпеки	Так	Організація науки і наукових досліджень	**Освіта:** Київське вище інженерне радіотехнічне училище ППО ім. О.І.Покришкіна, 1985 р. Спеціальність: «*Математичнее забезпечення автоматизованих систем управління*». Кваліфікація: «*Воєнний інженер-математик*» **Науковий ступінь:** доктор технічних наук, .2013 р., наукова спеціальність 21.05.01 «Інформаційна безпека держави». Тема дисертації: «*Методологія формування державної системи кібернетичної безпеки*» **Вчене звання:** Професор кафедри інформаційної та кібернетичної безпеки, 2016 р. **Види і результати професійної діяльності за спеціальністю відповідно до п.30 Ліцензійних умов провадження освітньої діяльності:** **п.п. 30.1), 30.2), 30.3), 30.4), 30.5), 30.7), 30.8), 30.10), 30.11), 30.13), 30.16), 30.17), 30.18).** ***30.1) Наявність за останні п'ять років наукових публікацій у періодичних виданнях, які включені до наукометричних баз, рекомендованих МОН, зокрема Scopus або Web of Science Core Collection.*** ***Наукометричні бази Scopus або Web of Science Core Collection*** 1. Бурячок В.Л., Слюсар В.І. Model of Signals for Digital Antenna Array with Mutual Coupling on the basis of Face- Splitting Matrixes Product. International Conference on Mathematical Methods in Electromagnetic Theory. Харків.: MMET-98. С. 117-124 (Матеріали конференції включено до міжнародної наукометричної бази **Scopus**) 2. Бурячок В.Л., Богуш В.М, Борсуковський Ю.В., Борсуковська В.Ю., Складанний П.М. Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України. Електронне наукове фахове видання «Інформаційні технології і засоби навчання». Том 67, № 5 (2018). С. 277-291 (Журнал включено до міжнародної наукометричної бази **Web of Science Core Collection**) 3. Lakhno V., Malyukov V. Parkhuts L., Buriachok V.,Satzhanov B., Tabylov A.Funding model for port information system cyber security facilities with incomplete hacker information available. Journal of Theoretical and Applied Information Technology June 2018, Vol.96, No.13. P. 4215-4225 (Журнал включено до до міжнародної наукометричної бази **Scopus**) 4. Lakhno V., Kasatkin D., Buriachok V., Palekha Y., Saiko V. Domrachev V. It support in decision-making with regard to infra-red grain drying management. Journal of Theoretical and Applied Information Technology, November 2018, Vol.96, №22. P 7587-7598 (Журнал включено до міжнародної наукометричної бази **Scopus**) 5. Lakhno V., Buriachok V., Parkhuts L., Tarasova H., Kydyralina L., Skladannyi P., Skrypnyk M., Shostakovska A. Development of a conceptual model of adaptive access rights management with using the apparatus of Petri nets. International Journal of Civil Engineering & Technology (IJCIET), Volume 9, Issue 11, November 2018. P. 95-104 (Журнал включено до міжнародної наукометричної бази **Scopus**) 6. Klimchuk V., Samoylik E., Gnatyuk V., Prysiazhnyy D., Buryachok V.Synthesis of Quite Proof Cryptosystem with Increased Unicity Distance for Cloud Computing. ICT in Education, Research and Industrial Applications. 2018, Kyiv, Ukraine, May 14-17(Part III: 4th International Workshop on Theory of Reliability and Markov Modelling for Information Technologies). P. 596–607 (Матеріали конференції включено до міжнародної наукометричної бази **Scopus**)

				7. Назаркевич М.А., Бурячок В.Л., Лотошинська Н., Дмитрук С.Дослідження фільтру Ateb-Габора у системах біометричного захисту. XIII International Scientific and Technical Conference Computer Science and Information Technologies Lviv, Ukraine, 11-14 September, 2018. P. 310-313 (Матеріали конференції включено до міжнародної наукометричної бази **Scopus** та **Web of Science Core Collection**) 8. Buriachok, V. L., Sokolov V. Yu., Bogachuk I. Monitoring Subsystem for Wireless Systems Based on Miniature Spectrum Analyzers. Proceedings of the V International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T'2018), 9–12 October, 2018: Kharkiv, Ukraine: IEEE. 978-1-5386-6611-1/18/$31.00 ©2018 IEEE (Журнал включено до міжнародних наукометричних баз **Scopus** та **Web of Science Core Collection**) 9. Buriachok, V. L., Sokolov V. Yu. Implementation of Active Learning in the Master's Program on Cybersecurity. The Second International Conference on Computer Science, Engineering and Education Applications (ICCSEEA2019), 26–27 January 2019, Kiev, Ukraine:(Журнал включено до міжнародної наукометричної бази **Scopus**) 10. Mahyar TajDini, Volodymyr Sokolov, Volodymyr Buriachok. Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio. Proceedings of the 8th International Conference on "Mathematics. Information Technologies. Education" (MoMLeT&DS'2019), June 2–4, 2019: abstracts. — Vol. 2386. — Aachen : CEUR, 2019. — P. 287–296 :(Журнал включено до міжнародної наукометричної бази **Scopus**) 11. V.Buriachok, V.Sokolov, P.Skladannyi. Security Rating Metrics for Distributed Wireless Systems. Proceedings of the 8th International Conference on "Mathematics. Information Technologies. Education" (MoMLeT&DS'2019), June 2–4, 2019: abstracts. — Vol. 2386. — Aachen : CEUR, 2019. — P. . 222–233 :(Журнал включено до міжнародної наукометричної бази **Scopus**) 12. Baisarova G., Brzhanov R., Kikvidze O.G., Lakhno V., Buriachok V. Chubaievskyi V. Computer simulation of large displacements of thermoelastic rods. Journal of Theoretical and Applied Information Technology 15th August 2019. Vol.97. No 15. P. 4188 - 4201 (Журнал включено до до міжнародної наукометричної бази **Scopus**) ***Інші наукометричні бази*** 13. Бурячок В.Л., Богуш В.М. Рекомендації щодо побудови та запровадження профілю навчання «кібернетична безпека» в Україні. Безпека інформації. Том 20, 2. 2014. С. 83-87 (Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: eLIBRARY.RU, Ulrichs Web, EBSCO, WorldCat (OAIster), Simple Search Metadata) 14. Семко В.В. Ситуаційне управління доступом в інформаційно-телекомунікаційній системі / В.В. Семко, В.Л. Бурячок, С.В. Толюпа, П.М.Складанний // Проблеми телекомунікацій. № 2 (17), 2015. с. 54-61 (Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Index Copernicus) 15. Бурячок В.Л. Метод побудови класифікатора кібератак на державні інформаційні ресурси / В.Л.Бурячок, Р.В.Грищук, В.М.Мамарев // Технологический аудит и резервы производства, №1/2(21), 2015. С. 38-43 (Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Index Copernicus, РИНЦ, ResearchBib, EBSCO) 16. Семко В.В. Модель управління захистом інформації в інформаційно-телекомунікаційній системі / В.В. Семко, В.Л. Бурячок, С.В. Толюпа, П.М.Складанний // Вісник Національного університету «Львівська політехніка»: Радіоелектроніка та телекомунікації. № 818, 2015. С.151-155 (Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Index Copernicus) 17. Семко В.В. Модель функціонування системи інтелектуального управління об'єктом / В.В. Семко, В.Л. Бурячок // «Наукові записки Українського науково-дослідного інституту зв'язку». №3(43), 2016. С. 21-29 (Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Національна бібліотека імені Вернадського, CrossRef, Google Scholar) 18. Гулак Г.М. Швидкий алгоритм генерації підстановок багатоалфавітної заміни / Г.М. Гулак, В.Л. Бурячок, П.М. Складанний // «Захист інформації» НАУ. Том 19, № 2 (2017). С. 173-177 (Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: WorldCat, Ulrichsweb Global Serials Directory, eLibrary.ru, BASE, Simple Search

				Metadata) 19. Борсуковський Ю.В. Прикладні аспекти розробки політики категорування інформації з обмеженим доступом / Ю.В.Борсуковський, В.Ю.Борсуковська, В.Л. Бурячок, П.М.Складанний // «Системи обробки інформації». № 2(153), 2018. С. 117-126 (Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Ulrich's Periodicals Directory, CrossRef, Index Copernicus, General Impact Factor, Scientific Indexed Service, Citefactor, ResearchBib, Orcid, Academic Resource Index, Google Scholar) 20. Бурячок В.Л. Перспективи розвитку додатків блокчейн в Україні / В.Л.Бурячок, С.О.Спасітєлева // «Кібербезпека: освіта, наука, техніка». № 1(1), 2018. С. 35-48 (Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Index Copernicus, Reasearch Bible, Reasearch Bible, Google Scholar, WorldCat, BASE, Eurasian Scientific Journal Index, Simple Search Metadata, Національна бібліотека імені Вернадського) 21. Бурячок В.Л. Віртуальна лабораторія для моделювання процесів в інформаційній та кібербезпеці як засіб формування практичних навичок студентів / В.Л.Бурячок, С.М.Шевченко, П.М.Складанний // «Кібербезпека: освіта, наука, техніка». № 2(2), 2018. С. 98-104 (Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Index Copernicus, Reasearch Bible, Reasearch Bible, Google Scholar, WorldCat, BASE, Eurasian Scientific Journal Index, Simple Search Metadata, Національна бібліотека імені Вернадського) 22. Бурячок В.Л. Рекомендації щодо розробки та реалізації моделі професійних компетентностей у сфері підготовки фахівців для національної системи кібербезпеки / В.Л.Бурячок, В.М.Богуш // Захист інформації. Том 20, №2. 2018. С. 72-78 (Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: WorldCat, Ulrichsweb Global Serials Directory, eLibrary.ru, BASE, Simple Search Metadata) 20. V.L Buryachok. Low-Cost Spectrum Analyzers for Channel Allocation in Wireless Networks 2.4 GHz Range / Buryachok, V.L. Sokolov V. Yu // World Science. - №3 (31). Vol. 1. Warsaw: RS Global Sp. z O.O., 2018. P. 9-16. (Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Index Copernicus, eLIBRARY.RU) 23. V.L Buryachok.Using 2.4 Ghz wireless botnets to implement denial-of-service attacks / Buryachok, V.L. Sokolov V. Yu // International academy 6(24), Vol.1, June 2018. P. 14-21. Journal web of scholar. (Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Index Copernicus, ResearchBib) 24. Бурячок В.Л. Спосіб генерування паролю для бездротових мереж з використанням змінного правила ускладнення. / В.Л. Бурячок, А.О. Аносов, А.В.Платоненко // «Захист інформації» НАУ. Том 21, № 1, січень – березень 2019. С. 52-59 (Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: eLIBRARY.RU, Ulrichs Web, EBSCO, WorldCat (OAIster), Simple Search Metadata) 25. Бурячок В.Л. Вибір раціонального способу генерування паролів серед множини існуючих / В.Л. Бурячок, А.В. Платоненко, О.В.Семко // «Безпека інформації» НАУ. Том 25, № 1 (2019). С. 59-64 (Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: eLIBRARY.RU, Ulrichs Web, EBSCO, WorldCat (OAIster), Simple Search Metadata) 26. K. Sauanova, S. Sagyndykova, V. Buriachok, N. Mazur, A. Anosov, S. Smirnov. Development of a model of cyber security management for automated systems. International Journal of Civil Engineering and Technology (IJCIET),Volume 10, Issue 03, 2019 Pages: 454-463. (Журнал включено до міжнародної наукометричних баз Google Scolar, PublicationsList.org, Academia.edu, IndexCopernicus, ResearchGate, EBSCO, DOAJ тощо) ***30.2) Наявність не менше п'яти наукових публікацій у наукових виданнях, включених до переліку наукових фахових видань України*** 1. Бурячок В.Л., Невойт Я.В., Хорошко В.О. Процедура визначення моменту часу впливу актуальних загроз на інформаційний ресурс. Сучасний захист інформації. № 1, 2016. С. 74-78 2. Бурячок В.Л., Степанов, І.Р. Пархомей, В.Б. Толубко Проблемні питання та актуальні завдання підготовки фахівців з кібернетичної безпеки галузі знань «інформаційні технології». Сучасний захист інформації. № 2, 2016. С. 4-9 3. Бурячок В.Л., Борсуковський Ю.В., Складанний П.М. Аналіз сучасних вимог до створення парольних політик

				корпоративних користувачів. «Сучасний захист інформації». № 3, 2016. С. 72-76 4. Бурячок В.Л., Семко В.В., Бурячок Л.В. Технологія проведення порівняльного аналізу та оцінювання стану захищеності автоматизованих інформаційних систем. «Сучасний захист інформації». № 4, 2016. С. 16-24 5. Степанов М.М., Вишнівський В.В., Пархомей І.Р., В.Л. Бурячок Криптографічний захист інформації, що циркулює в інформаційних ресурсах ERP-систем. «Зв'язок». № 2, 2016. С.60-63 6. Бурячок В.Л., Борсуковський Ю.В. Роль і місце вищих навчальних закладів в створенні системі інформаційної та кібернетичної безпеки України. «Сучасний захист інформації». № 1, 2017. С. 34-40 7. Бурячок В.Л., Спасітєлєва С.О. Комплексний захист гетерогенних корпо-ративних сховищ даних. «Сучасний захист інформації». № 1, 2017. С. 58-65 8. Борсуковський Ю.В., Бурячок В.Л., Борсуковська В.Ю. Базові напрямки забезпечення кібербезпеки державного та приватного секторів. «Сучасний захист інформації». № 2(30), 2017. С. 85-89 9. Бурячок В.Л., Спасітєлєва С.О., Складанний П.М. Організація розробки безпечних .net прикладних програм у закладах вищої освіти. «Сучасна спеціальна техніка». № 1(52) 2018. С.13-22 10. Семко О.В., Складанний П.М., Семко В.В., Бурячок В.Л. Методологія інтелектуального управління маршрутизацією в конфліктуючих сенсорних мережах варіативної топології. «Сучасна спеціальна техніка». №4(55), 2018, с. 64–76 ***30.3) Наявність виданого підручника чи навчального посібника або монографії*** 1. Бурячок В.Л., Хорошко В.О. Технологія прийняття рішень у складних соціотехнічних системах : Монографія. К. : ДУІКТ, 2012. 344 с. 2. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки : Монографія. К. : НАУ, 2013. 432 с. 3. Бурячок В.Л., Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки: підручник. К. : ПВП «Задруга», 2014. 222 с. 4. Бурячок В.Л., Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки: навчальний посібник. К. : ПВП «Задруга», 2014. 134 с. 5. Бурячок В.Л., Толюпа С.В., Хорошко В.О. Інтелектуальна власність у сфері інформаційної безпеки. К. : ПВП «Задруга», 2014. 196 с. 6. Бурячок В.Л., Толубко В.Б., Толюпа С.В., Хорошко В.О. Інформаційна і кібербезпека: соціотехнічний аспект. [Підручник]. К.: ДУТ, 2015. 288 с. Гриф надано МОН України. Лист № 1/11-7193 від 14.05. 2014 р. 7. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. К.: ДУТ, 2015. 345 с. 8. Бурячок В.Л., Толубко В.Б., Гулак Г.М. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. К.: ДУТ, 2015. 449 с. Гриф надано МОН України. Лист № 1/11-8664 від 22.06. 2015 р. 9. Бурячок В.Л., Семко В.В., Складанний П.М. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. К.: ДУТ, 2016. 132 с. Гриф надано МОН України. Лист № 1/11-8662 від 22.06. 2015 р. 10. Толюпа С.В., Оксіюк О.Г., Бурячок В.Л., Вялкова В.І. Захист об'єктів інформаційної діяльності: навчальний посібник. К.: ККБ та ЗІ ФІТ КНУ імені Тараса Шевченка, 2018. 322 с. 11. Buriachok, V., Sokolov V. Increase the Speed of Spectrum Analyzers based on Atmel Atmega328 and ARM Cortex-M3 RISC Processors; [ed. M. Kozinski]. Bezpieczeństwo w Cyberprzestrzeni Społeczna Przestrzeń Internetu w Kontekście Wartości i Zagrożeń. Kharkiv : NUCPU, 2019. P. 283–297. ISBN: 978-83-63680-28-2. ***Підручники, посібники і монографії, що рекомендовані Вченою радою Київського університету імені Бориса Грінченка як навчальні видання та знаходяться на стадії друку*** 12. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М.. Технології забезпечення безпеки мережевої інфраструктури: підручник. К.: КУБГ, 2019. 225 с.

				13. Бурячок В.Л., Соколов В.Ю., Тадждіні М.М. Безпека безпроводових і мобільних мереж: навчальний посібник. К.: КУБГ, 2019. 132 с. 14. Бурячок В. Л. , Киричок Р. В. , Складанний П. М. Основи інформаційної та кібернетичної безпеки: навчальний посібник. К.: КУБГ, 2019. 213 с. 15. Бурячок В. Л. , Дуравкін Є.В., Лукова-Чуйко Н.В., Складанний П.М. Methods of information protection in telecommunication systems: навчальний посібник. К.: КУБГ, 2019. 74 с. 16. Бурячок В.Л., Соколов В.Ю. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів [Монографія]. К.: КУБГ, 2019. 164 с. ***30.4) Наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня*** *Науковий керівник кандидатських дисертацій:* – МАМАРЄВ Віктор Миколайович, дисертаційна робота на здобуття наукового ступеня кандидата технічних наук на тему "Метод побудови класифікатора кібератак на державні інформаційні ресурси", науковий ступінь присуджено на засіданні СРД 26.861.06 ДУТ за спеціальністю 21.05.01 "Інформаційна безпека держави", наказ МОН України щодо присвоєння вчених звань від 29 вересня 2015 року №988 (Додаток 2 до наказу); – ДОМАРЄВ Дмитро Валерійович, дисертаційна робота на здобуття наукового ступеня кандидата технічних наук на тему "Метод інформаційно-аналітичної підтримки управління інформаційною безпекою на основі структуризації оцінок", науковий ступінь присуджено на засіданні СРД 26.861.06 ДУТ за спеціальністю 21.05.01 "Інформаційна безпека держави", наказ МОН України щодо присвоєння вчених звань від 29 вересня 2015 року №988 (Додаток 2 до наказу); – НЕВОЙТ Яніна Володимирівна, дисертаційна робота на здобуття наукового ступеня кандидата технічних наук на тему "Метод оцінювання стану захищеності інформаційних ресурсів на основі дослідження джерел загроз інформаційній безпеці", науковий ступінь присуджено на засіданні СРД 26.861.06 ДУТ за спеціальністю 21.05.01 "Інформаційна безпека держави", наказ МОН України щодо присвоєння вчених звань від 29 вересня 2016 року №1166 (Додаток 4 до наказу); – СМІРНОВ Сергій Анатолійович, дисертаційна робота на здобуття наукового ступеня кандидата технічних наук на тему "Метод антивірусного захисту даних з використанням хмарних обчислювальних технологій" науковий ступінь присуджено на засіданні СРД 26.861.06 ДУТ за спеціальністю 05.13.21 "Системи захисту інформації", наказ МОН України щодо присвоєння вчених звань від 26 червня 2017 року №936 (Додаток 5 до наказу); – СЕМКО Олексій Вікторович, дисертаційна робота на здобуття наукового ступеня кандидата технічних наук на тему "Інформаційна технологія інтелектуального управління маршрутизацією в сенсорних мережах варіативної топології за умов обмежень і невизначеностей" науковий ступінь присуджено на засіданні СРД 26.255.01 Інституту телекомунікацій і глобального інформаційного простору НАН України за спеціальністю 05.13.06 "Інформаційні технології" 17.09.2019 р., наказ МОН України щодо присвоєння вчених звань від «__» __ 2019 р. №_ (Додаток _ до наказу); – СОКОЛОВ Володимир Юрійович, дисертаційна робота на здобуття наукового ступеня кандидата технічних наук на тему "Методи і засоби підвищення інформаційної та функціональної безпеки безпроводових мереж передавання даних" науковий ступінь присуджено на засіданні СРД 26.255.01 Інституту телекомунікацій і глобального інформаційного простору НАН України за спеціальністю 05.13.06 "Інформаційні технології" 29.10.2019 р., наказ МОН України щодо присвоєння вчених звань від «__» __ 2019 р. №_ (Додаток _ до наказу); – ПЛАТОНЕНКО Артем Вадимович, дисертаційна робота на здобуття наукового ступеня кандидата технічних наук на тему "Технологія забезпечення функціональної безпеки систем бездротового зв'язку на основі вдосконалення парольних політик" науковий ступінь присуджено на засіданні СРД 26.255.01 Інституту телекомунікацій і глобального інформаційного простору НАН України за спеціальністю 05.13.06 "Інформаційні технології" 29.10.2019 р., наказ МОН України щодо присвоєння вчених звань від «__» __ 2019 р. №_ (Додаток _ до наказу). *Науковий консультант докторської дисертації:* – СЕМКО Віктор Володимирович, дисертаційна робота на здобуття наукового ступеня доктора технічних наук на

				тему “Методологія оптимального управління об’єктом в умовах конфлікту, обмежень та невизначеностей”, науковий ступінь присуджено на засіданні СРД 26.255.01 Інституту телекомунікацій і глобального інформаційного простору НАН України за спеціальністю 05.13.06 “Інформаційні технології”, наказ МОН України щодо присвоєння вчених звань від 27.04.2017 № 659 (наказ_доктори_27.04.2017). ***30.5) Участь у міжнародних наукових проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії”*** У 2013 - 2017 був представником Державного університету телекомунікацій в програмі ЄС «ENGENSEC» з підготовки магістрів у сфері інформаційної та кібербезпеки (проект 544 455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR) та впровадженні цієї програми в освітній процес Державного університету телекомунікацій. З 2017 року отриманий досвід застосував при відкритті спеціальності 125 «Кібербезпека» в Київському університеті імені Бориса Грінченка. З 2015 року член, а з 2017 по т.ч. голова секретаріату державного комітету в сфері “Технічного захисту інформації” – ТК-107. Брав участь у формуванні переліку міжнародних стандартів, стандартів ЄС та НАТО в сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки, які потребують перекладу та гармонізації, а також їх імплементації в сферу захисту інформації в Україні ***30.7) Робота у складі експертних рад з питань проведення експертизи дисертацій МОН або галузевих експертних рад Національного агентства із забезпечення якості вищої освіти, або Акредитаційної комісії, або їх експертних рад, або міжгалузевої експертної ради з вищої освіти Акредитаційної комісії, або трьох експертних комісій МОН/зазначеного Агентства, або Науково-методичної ради/науково-методичних комісій (підкомісій) з вищої освіти МОН*** З квітня 2016 по квітень 2019 року секретар підкомісії 125 «Кібербезпека» Науково-методичної комісії з інформаційних технологій, автоматизації та телекомунікацій (НМК № 8) сектору вищої освіти Науково-методичної ради МОН України. (*наказ МОН від 6 квітня 2016 р. № 375, https://zakon.rada.gov.ua/rada/show/v0375729-16*) З 2015 по 2019 рік відповідно до постанови Кабінету Міністрів України від 9 серпня 2001 року № 978 «Про затвердження Положення про акредитацію вищих навчальних закладів і спеціальностей у вищих навчальних закладах та вищих професійних училищах» приймав участь у проведенні 12 акредитаційних експертиз. ***30.8) Виконання функцій наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії наукового видання, включеного до переліку наукових фахових видань України, або іноземного рецензованого наукового видання*** Протягом 1985 - 2013 років брав участь як виконавець, відповідальний виконавець або науковий керівник в 30 науково-дослідних і дослідно-конструкторських роботах на спеціальну тему, що за замовленням Міністерства оборони СРСР і Міністерства оборони України виконувались 10 НДІ ППО СРСР, Центральним науково-досдіним інститутом озброєння і військової техніки МО України та НДІ Головного управління розвідки ЗС України. У 2013 – 2017 роках був науковим керівником НДР «Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем в умовах впливу кібернетичних атак». Метою НДР є підвищення живучості ІКС в умовах впливу кібератак за рахунок протидії спробам порушення захисту таких систем та їх відновлення після злому. Основними завданнями НДР є: 1) аналіз стану живучості типових ІКС та розробка стратегій забезпечення живучості; 2) розробка моделей політики безпеки ІКС, здатних протистояти цілеспрямованим спробам порушення безпеки; 3) визначення типових архітектур та підходів до синтезу ІКС, що відповідають вимогам по забезпеченню живучості. У 2016 – 2017 роках був головним редактором науково-технічного журналу “Сучасний захист інформації” Державного університету телекомунікацій. З 2018 року – головний редактор електронного науково-технічного видання “Кібербезпека: освіта, наука, техніка” Київського університету імені Бориса Грінченка.

				(*http://csecurity.kubg.edu.ua/index.php/journal/about/editorialTeam* *http://jrnl.nau.edu.ua/index.php/ZI/about/editorialPolicies#custom-3*). ***30.10) Організаційна робота у закладах освіти на посадах керівника (заступника керівника) закладу освіти/інституту/ факультету/ відділення (наукової установи)/ філії/кафедри або іншого відповідального за підготовку здобувачів вищої освіти підрозділу/відділу (наукової установи)/навчально-методичного управління (відділу)/лабораторії/іншого навчально-наукового (інноваційного) структурного підрозділу/вченого секретаря закладу освіти (факультету, інституту)/відповідального секретаря приймальної комісії та його заступника*** З 7 жовтня 2013 року по серпень 2017 року – завідувач кафедри інформаційної та кібернетичної безпеки Державного університету телекомунікацій. З 1 березня 2018 року по цей час – завідувач кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка. (*Наказ № 107 від 23.02.2018 р. про створення кафедри ІКБ в КУБГ та № 248-к/тр від 01.03.2018 про призначення завідувачем кафедри ІКБ*) ***30.11) Участь в атестації наукових працівників як офіційного опонента або члена постійної спеціалізованої вченої ради (не менше трьох разових спеціалізованих вчених рад)*** 1. Офіційне опонування дисертації на здобуття наукового ступеня кандидата технічних наук за спеціальністю 20.02.14 – озброєння і військова техніка ПОЗДНЯКОВА Павла Васильовича за темою «Метод комбінованого криптоперетворення та завадостійкого кодування для захисту інформації в радіолініях зв'язку безпілотних розвідувальних систем». Захист на спеціалізованій вченій раді К 14.719.01 Житомирського військового інституту імені С. П. Корольова Національного авіаційного університету, 2013 рік. 2. Офіційне опонування дисертації на здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави РАБЧУНА Андрія Олександровича за темою «методи та моделі Оптимізації показників систем захисту інформації в умовах інформаційного протиборства». Захист на спеціалізованій вченій раді Д 26.062.17 в Національному авіаційному університеті 27.03.2014 року. 3. Офіційне опонування дисертації на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації КАЗАКОВОЇ Надії Феліксівни за темою «Моделі та методи проактивного забезпечення інформаційної безпеки в когнітивних мережах». Захист на спеціалізованій вченій раді Д 35.052.18 в Національному університеті «Львівська політехніка», 2015 рік. 4. Офіційне опонування дисертації на здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави ДОБРОВОЛЬСЬКОГО Євгена Леонідовича за темою «Методи та моделі інформаційно-аналітичної підтримки прийняття рішень в сфері інформаційної безпеки держави». Захист на спеціалізованій вченій раді Д 26.062.17 в Національному авіаційному університеті 07.07.2016 року. 5. Офіційне опонування дисертації на здобуття наукового ступеня доктора технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави РЯБУХИ Юрія Миколайовича за темою «Теоретичні основи і методи підвищення безпеки дистанційних відеоінформаційних ресурсів в системі аеромоніторингу кризових ситуацій». Захист на спеціалізованій вченій раді Д 26.062.17 в Національному авіаційному університеті 27.04.2016 року. 6. Офіційне опонування дисертації на здобуття наукового ступеня доктора технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави БУЧИКА Сергія Степановича за темою «Методологія побудови та захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів». Захист на спеціалізованій вченій раді Д 26.062.17 в Національному авіаційному університеті 13.10.2016 року. 7. Офіційне опонування дисертації на здобуття наукового ступеня доктора технічних наук за спеціальністю 01.05.04 – системний аналіз і теорія оптимальних рішень ПОТЬОМКІНА Михайла Михайловича за темою «Розвиток методології багатокритеріальної оптимізації складних організаційно-технічних систем військового призначення». Захист на спеціалізованій вченій раді Д 26.702.01 Центрального науково-дослідного інституту Збройних Сил України 21.03.2017 року 8. Офіційне опонування дисертації на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи

				захисту інформації КАЗМІРЧУК Світлани Володимирівни за темою «Методологія оцінювання ризиків безпеки ресурсів інформаційних систем». Захист на спеціалізованій вченій раді Д 26.062.17 в Національному авіаційному університеті 25.01.2018 року. https://lib.pedpresa.ua/?s=спецвипуск+освіта+України У 2014 по 2017 роках очолював спеціалізовану вчену раду Д 26.861.06 при Державному університеті телекомунікацій з правом прийняття до розгляду та проведення захисту дисертацій на здобуття наукового ступеня доктора технічних наук за спеціальностями 21.05.01 "Інформаційна безпека держави" та 05.13.21 "Системи захисту інформації" (*http://www.dut.edu.ua/uploads/p_1539_29821168.pdf*). З 2013 року й дотепер – член спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті з правом прийняття до розгляду та проведення захисту дисертацій на здобуття наукового ступеня доктора технічних наук за спеціальностями 21.05.01 "Інформаційна безпека держави" та 05.13.21 "Системи захисту інформації" (*https://nau.edu.ua/ua/menu/universitet/spezializovani-vcheni-radi/spezializovana-vchena-rada-d-26-062-17.html*) ***30.13) Наявність виданих навчально-методичних посібників/посібників для самостійної роботи студентів та дистанційного навчання, конспектів лекцій/ практикумів/ методичних вказівок/рекомендацій загальною кількістю три найменування*** 1. Бурячок В.Л., Соколов В.Ю., Складанний П.М., Корченко А.О., Казмірчук С.В. Методичні рекомендації до виконання дипломних робіт освітнього рівня «Бакалавр» студентів спеціальності 125 «Кібернетична безпека». [Методичні рекомендації]. К.: ДУТ, 2016. 87 с. 2. Taj Dini M., Соколов В.Ю., Бурячок В.Л. Wireless & mobile security [Лабораторний практикум]. К.: ДУТ, 2017. 124 с. 3. Бурячок В.Л., Соколов В.Ю. Ініціатива CDIO. Версія 2.1 [Методичні рекомендації]. К.: КУБГ, 2019. 34 с. ***30.16) Участь у професійних об'єднаннях за спеціальністю*** Член міжнародного товариства «Internet Society». Member ID – 208002 Режим доступу: https://portal.isoc.org/membership/profile. Член Міжнародного союзу електрозв'язку (ITU). Contact ID – 1200190722 Режим доступу: https://www.itu.int/itu_xr_main/main/myAccountHomePage.jsf?pageType= R&selectedMyAccountNodeId=I2&wec-appid=USER_REG&page=6544ACBA39DF44448583E640027C25C4&wec-locale=en_US ***30.17) Досвід практичної роботи за спеціальністю не менше п'яти років*** Досвід практичної діяльності за напрямками створення й впровадження систем технічного і криптографічного захисту інформації на об'єктах інформаційної діяльності та забезпечення безпеки інформаційно-комунікаційних систем в органах виконавчої влади – 20 років. Протягом 1993 - 2013 років відповідні роботи проводились спільно з товариством з обмеженою відповідальністю «Автор» (м.Київ), ТОВ «Криптон» (м.Київ), ТОВ «Елан» (м.Київ), Інститутом програмних систем НАН України (м.Київ), Інститутом проблем математичних машин і систем НАН України (м.Київ), Інститутом інформаційних технологій (м.Харків), тощо у відповідності до ліцензій Служби Безпеки України та Служби спеціального зв'язку і захисту інформації України. У 2007 - 2013 роках в рамках співпраці науково-дослідного інституту Головного управління розвідки МО України із зазначеними вище компаніями та науково-дослідними інститутами України для потреб ЗС нашої держави займався створенням: систем захисту інформації на об'єктах інформаційної діяльності від стороннього кібернетичного впливу та інформації, що циркулює в ІТ системах і мережах; систем пошуку розвідувальної інформації у відкритих і відносно-відкритих електронних джерелах, а також її добування із закритих ІТ і криптосистем; систем первинної обробки, накопичення і передачі інформації між спеціальними кореспондентами та органами управління в тому числі спеціальними засобами. (*Інформація закритого характеру*) ***30.18) Наукове консультування установ, підприємств, організацій протягом не менше двох років.***

				Консультант ТОВ “Elan” (2008 – 2015р.р., м. Київ) з питань захисту інформації. (*Довідка ТОВ «Elan» № 3/2015 від 06.01.2015 року*)
БЕССАЛОВ Анатолій Володимирович	Професор кафедри інформаційної та кібернетичної безпеки	Так	Математичні методи криптографії Методи побудови і аналізу криптосистем	**Освіта:** Київське вище інженерно-авіаційне військове училище ВПС, 1968 р.. Спеціальність: «*Радіотехнічні засоби пілотованих повітряних і космічних літальних апаратів*». Кваліфікація: «*Військовий інженер по радіотехніці*» **Науковий ступінь:** доктор технічних наук, 1993 р. Наукова спеціальність 20.02.14 «Озброєння та військова техніка». Тема дисертації: *спеціальна.* **Вчене звання:** Професор за кафедрою бортових систем. радіозв’язку та радіонавігації, 1994 р. **Види і результати професійної діяльності за спеціальністю відповідно до п.30 Ліцензійних умов провадження освітньої діяльності:** **п.п. 30.1), 30.2), 30.3), 30.4), 30.8), 30.9), 30.11), 30.12), 30.14), 30.17).** ***30.1) Наявність за останні п’ять років (2014 – 2019 р.р.) наукових публікацій у періодичних виданнях, які включені до наукометричних баз, рекомендованих МОН, зокрема Scopus або Web of Science Core Collection.*** ***Наукометричні бази Scopus або Web of Science Core Collection*** 1. Bessalov A.V., Dikhtenko A.A., Tsygankova O.V. An algorithm for selection of a canonic curve isomorphic to the Edwards curve over a prime field. Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika) №175, 2014. PP.193-198 *(Матеріали конференції включено до міжнароднихнаукометричних баз Web of Science та Scopus)* 2. Bessalov, A.V., Tsygankova O.V. New properties of the Edwards form elliptic curve over a prime field. Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika) №186, 2015. PP.137-143 *(Матеріали конференції включено до міжнароднихнаукометричних баз Web of Science та Scopus)* 3. Bessalov, A.V., Kovalchuk L.V. Exact Number of Elliptic Curves in the Canonical Form, Which are Isomorphic to Edwards Curves Over Prime Field. Cybernetics and Systems Analysis: Volume 51, Issue 2 (2015), Page 165-172 *(Матеріали конференції включено до міжнароднихнаукометричних баз Web of Science та Scopus)* 4. Bessalov, A.V., Tsygankova O.V. Interrelation of families of points of high order on the Edwards curve over a prime field. Problems of Information Transmission, Volume 51, Issue 4 (2015), Page 391-397 *(Матеріали конференції включено до міжнароднихнаукометричних баз Web of Science та Scopus)* 5. Kovalchuk, L. V. , Bessalov A. V. & Bespalov O. Y. Algorithms for Base Point Generation on an Edwards Curve with the Use of Point Divisibility Criteria. Cybernetics and Systems Analysis: Volume 52, Issue 5 (2016), PP.14-24 *(Матеріали конференції включено до міжнароднихнаукометричних баз Web of Science та Scopus)* 6. Bessalov A.V., Tsygankova O.V. Number of curves in the generalized Edwards form with minimal even cofactor of the curve order. Problems of Information Transmission, Volume 53, Issue 1 (2017), Page 92-101 *(Матеріали конференції включено до міжнароднихнаукометричних баз Web of Science та Scopus)* ***30.2) Наявність не менше п’яти наукових публікацій у наукових виданнях, включених до переліку наукових фахових видань України*** 1. Бессалов А.В., Дихтенко А.А. Криптостойкие кривые Эдвардса над простыми полями. «Прикладная радиоэлектроника», 2013, Том 12, №2. С. 285-291 2. Бессалов А.В., Третьяков Д.Б. Удвоение точки и обратная задача для кривой Эдвардса над простым полем. «Сучасний захист інформації», №3, 2013. С.56-58 3. Бессалов А.В., Дихтенко А.А. Изоморфные канонической форме эллиптические кривые Эдвардса над расширенными полями характеристики. «Радиотехника», №175, 2014. С.200-205 4. Бессалов А.В., Дихтенко А.А., Цыганкова О.В. Мощность семейства эллиптических кривых, изоморфных

				кривым Эдвардса над простым полем. «Захист інформації». Том 16, №1, січень-березень 2014, с.23-28 5. Бессалов А.В., Дихтенко А.А., Цыганкова О.В. Плотность канонических эллиптических кривых со свойством изоморфизма к форме Эдвардса. «Известия ЮФУ. Технические науки». Вып. №4, 2014. С.146-153 6. Бессалов А.В., Дихтенко А.А. Изоморфизм несуперсингулярных кривых над полями характеристики 2 и кривых Эдвардса с одним параметром. «Радиотехника», №176, 2014. С.88-93 7. Бессалов А.В. Построение кривой Эдвардса на базе изоморфной эллиптической кривой в канонической форме. «Прикладная радиоэлектроника», 2014, Том 13, №3. С. 286-289 8. Бессалов А.В., Третьяков Д.Б., Цыганкова О.В. Новый подход к определению точного числа кривых Эдвардса над простым полем. «Сучасний захист інформації», №3, 2014. С.11-15 9. Бессалов А.В., Цыганкова О.В. Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем. «Захист інформації», Том 17, №1, січень-березень 2015. С.73-80 10. Бессалов А.В., Цыганкова О.В. Изоморфные канонической форме эллиптические кривые Эдвардса над расширенными полями характеристики. «Радиотехника», №181, 2015. С.58-63 11. Бессалов А.В., Цыганкова О.В. Классификация кривых в форме Эдвардса над простым полем. «Прикладная радиоэлектроника», 2015, Том 14, №4. С. 197-203 12. Ковальчук Л.В., Бессалов А.В., Беспалов О.Ю. Алгоритмы генерации базовой точки кривой Эдвардса с использованием критериев делимости точки кривой. «Кибернетика и системный анализ», т.52, №5, 2016. С.14-24 13. Бессалов А.В., Трет'яков Д.Б., Циганкова О.В. Властивості точок малих порядків кривих в узагальненої формі Едвардса. «Сучасний захист інформації», №2, 2016. С.46-54 14. Бессалов А.В. Метод нахождения порядка точки скрученной кривой Эдвардса. «Радиотехника», №186, 2016. С.110-118 15. Бессалов А.В., Олешко К.А., Поречная Д.Н., Цыганкова О.В.,Черный О.Н.Криптостойкие скрученные кривые Эдвардса с минимальной сложностью групповых операцій. «Прикладная радиоэлектроника», 2016, Том 15, №3. С. 141-150 16. Бессалов А.В., Цыганкова О.В. Суперсингулярные полные кривые Эдвардса над простым полем. «Радиотехника», №191, 2017. С.88-98 ***30.3) Наявність виданого підручника чи навчального посібника або монографії*** 1. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография. Монография: Монографія. К.: «Политехника», 2017. 272 с. ***30.4) Наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня*** Загалом (до 1993 року) підготував до захисту 2-х докторів і 8 к.т.н. На даний час керує науковою роботою 2-х аспірантів – Циганкової О.В. (тема: «Методи підвищення ефективності роботи криптосистем на базі кривих у формі Едвардса», спеціальність 05.13.21- системи захисту інформації) і Беспалова О.Ю. («Методи факторизації великих чисел в системах криптографічного захисту інформації», спеціальність 05.13.21- системи захисту інформації). ***30.8) Виконання функцій наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії наукового видання, включеного до переліку наукових фахових видань України, або іноземного рецензованого наукового видання*** *Відповідальний виконавець*: 1. НДР, шифр «Севрюга». Тема «Дослідження алгебраїчно-ймовірнісних методів крипто аналізу симетричних та

				асиметричних криптосистем та їх застосування в системах криптографічного захисту інформації». ФТІ НТУУ «КПІ» (2013 - 2014). 2. НДР, шифр «Мокрель». Тема «Дослідження та застосування сучасних математичних методів аналізу окремих перетворень у системах криптографічного захисту інформації». ФТІ НТУУ «КПІ» (2015-2016 р.р.). 3. НДР, шифр «Кобія». Тема «Дослідження методів крипто аналізу в застосуванні до сучасних систем криптографічного захисту інформації з урахуванням перспектив розвитку квантових обчислень». ФТІ НТУУ «КПІ» (2017 - 2018 р.р.). *Науковий керівник*: НДР на спеціальну тему (замовник – Державна служба спеціального зв'язку і захисту інформації). Мета: розробка 3-х державних стандартів України в галузі безпеки інформації. ***30.9) Керівництво школярем, який зайняв призове місце III-IV етапу Всеукраїнських учнівських олімпіад з базових навчальних предметів, II-III етапу Всеукраїнських конкурсів-захистів науково-дослідницьких робіт учнів - членів Національного центру "Мала академія наук України"; участь у журі олімпіад чи конкурсів "Мала академія наук України"*** Конкурсна робота «Системи цифрового підпису на еліптичних кривих Едвардса» на Всеукраїнському конкурсі НДР учнів – членів Малої академії наук України (5-6.04.2012р). Автор: Гур'янов О.І., учень 11 класу ліцею №38 ім. В.М.Молчанова Керівник: Бессалов А.В., д.т.н., професор. Робота зайняла 1 місце в Україні по відділенню «математика». Диплом 1-го ступеня підписано міністром освіти і науки та Президентом НАН України. Робота отримала спеціальний приз міжнародного конкурсу молодих вчених у Братиславі в липні 2012 р. ***30.11) Участь в атестації наукових працівників як офіційного опонента або члена постійної спеціалізованої вченої ради (не менше трьох разових спеціалізованих вчених рад)*** 1. Офіційне опонування дисертації ПОЛЯКОВА А.А. Методы и средства построения общесистемных параметров в группе точек эллиптической кривой для криптоприложений. - Дисертація канд. техн. наук за спеціальністю 05.13.21- системи захисту інформації. ХНУРЕ, 2004. 2. Офіційне опонування дисертації ЗБИТНЕВА С.І. Оценка стойкости криптопреобразований в группе точек эллиптических кривых. - Дисертація канд. техн. наук за спеціальністю 05.13.21- системи захисту інформації. ХНУРЕ, 2005. 3. Офіційне опонування дисертації ПОГРЕБНЯКА К.М. Методи та аналітичні моделі оцінки стійкості та складності криптоперетворень зі спарюванням точок еліптичних кривих- Дисертація канд. техн. наук за спеціальністю 05.13.21- системи захисту інформації. ХНУРЕ, 2009. 4. Офіційне опонування дисертації НЕЛАСИ Г.В. Удосконалення методів перетворень в якобіанах гиперэллиптических кривых для криптографічних додатків. - Дисертація канд. техн. наук за спеціальністю 05.13.21- системи захисту інформації. ХНУРЕ, 2010 5. Офіційне опонування дисертації ЯКИМЕНКО Ігоря Зіновійовича. Методи та алгоритми опрацювання інформаційних потоків в комп'ютерних мережах за умови застосування еліптичних кривих.- Дисертація канд. техн. наук: 05.13.05, Терноп. нац. екон. ун-т. - Т., 2012. ***30.12) Наявність не менше п'яти авторських свідоцтв та/або патентів загальною кількістю два досягнення*** 1) Бессалов А.В., Пулавский В.А., Пасечников И.И. Генератор случайной цифровой последовательности. Авторское свидетельство № 1107264 от 10.03.1983. Госкомизобретений СССР, 1983. 2) Харисов В.Н., Бессалов А.В., Патрикеев О.В., Гепко И.А. Генератор псевдослучайных чисел. Авторское свидетельство № 311071 от 02.04.1990. Госкомизобретений СССР, 1990. ***30.14) Керівництво студентом, який зайняв призове місце на I етапі Всеукраїнської студентської олімпіади***

				(Всеукраїнського конкурсу студентських наукових робіт), або робота у складі організаційного комітету/журі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або керівництво постійно діючим студентським науковим гуртком/проблемною групою; керівництво студентом, який став призером або лауреатом Міжнародних мистецьких конкурсів, фестивалів та проектів, робота у складі організаційного комітету або у складі журі міжнародних мистецьких конкурсів, інших культурно-мистецьких проектів; керівництво студентом, який брав участь в Олімпійських, Паралімпійських іграх, Всесвітній та Всеукраїнській Універсіаді, чемпіонаті світу, Європи, Європейських іграх, етапах Кубка світу та Європи, чемпіонаті України; виконання обов'язків тренера, помічника тренера національної збірної команди України з видів спорту; виконання обов'язків головного секретаря, головного судді, судді міжнародних та всеукраїнських змагань; керівництво спортивною делегацією; робота у складі організаційного комітету, суддівського корпусу Конкурсна робота «Параметри генераторів криптосистем на кривих Едвардса над простими полями». Автор: Линьов В.К., студент 5-го курсу Інституту суспільства Київського університету імені Бориса Грінченка. Керівник: Бессалов А.В., д.т.н., професор. Робота зайняла 1 місце у ІІ етапі Всеукраїнського конкурсу студентських наукових 2013/2014 н.р. у галузі «інформаційна безпека». ***30.17) Досвід практичної роботи за спеціальністю не менше п'яти років*** Досвід практичної діяльності за напрямками створення й впровадження систем криптографічного захисту інформації – 43 роки. Останнім часом такі роботи виконувались у відповідності до ліцензій Служби Безпеки України та Державної служби спеціального зв'язку і захисту інформації (ДССЗЗІ) України. До головних досягнень у цій сфері в період з 2013 по 2018 роки доцільно віднести рішення щодо впровадження у системи криптографічного захисту інформації на об'єктах інформаційної діяльності: сучасних алгебраїчно-ймовірнісних методів криптоаналізу симетричних і асиметричних криптосистем (2013-2014); сучасних математичних методів аналізу окремих перетворень (2015-2016 р.р.); перспективних технологій квантових обчислень (2017-2018 р.р.); З грудня 2018 року за замовленням ДССЗЗІ на абазі ТОВ «Криптон» спільно зі службою Зовнішньої розвідки України розпочато роботу над розробкою проектів національних стандартів: цифрового підпису, автентифікації та інкапсуляції ключів (2019 – 2020 р.р.).
СЕМКО Віктор Володимирович	Професор кафедри інформаційної та кібернетичної безпеки	Так	Технології безпеки мережевої та смарт інфраструктури Технології розробки і тестування ПЗ мережевої безпеки Технології протидії злоякісному програмному коду	**Освіта:** Київський інститут інженерів цивільної авіації, 1973р. Спеціальність: «*Електронні обчислювальні машини*». Кваліфікація: «*Інженер-електрик*». **Науковий ступінь:** доктор технічних наук, 2017 р. Наукова спеціальність 05.13.06 – «Інформаційні технології». Тема дисертації: *«Методологія оптимального управління об'єктом в умовах конфлікту, обмежень та невизначеності».* **Вчене звання:** доцент за кафедрою інформаційної та кібернетичної безпеки, 2015 р. **Види і результати професійної діяльності за спеціальністю відповідно до п.30 Ліцензійних умов провадження освітньої діяльності:** **п.п. 30.1), 30.2), 30.3), 30.4),), 30.5), 30.8), 30.11), 30.12), 30.16), 30.17), 30.18).** ***30.1) Наявність за останні п'ять років (2014 – 2019 р.р.) наукових публікацій у періодичних виданнях, які включені до наукометричних баз, рекомендованих МОН, зокрема Scopus або Web of Science Core Collection.*** ***Наукометричні бази Scopus або Web of Science Core Collection*** 1. Семко ВВ. Логіко-математична модель опису простору рішень. «Вісник Чернігівського державного технологічного університету» № 2(65), 2013, с. 147–155 *(Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Національна бібліотека імені Вернадського, Google Scholar, eLIBRARY.RU)* 2. Семко ВВ. Моделювання турбулентності приземного шару атмосфери. «Вісник Чернігівського державного технологічного університету» № 2(78), 2015, с. 230–234 *(Журнал включено до міжнародних каталогів наукових видань і*

				наукометричних баз: Національна бібліотека імені Вернадського, Google Scholar, eLIBRARY.RU) 3. Семко В.В., Бурячок В.Л., Толюпа С.В., Складанний П.М. Ситуаційне управління доступом в інформаційно-телекомунікаційній системі. Проблеми телекомунікацій. №2 (17), 2015. с. 54-61 *(Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Національна бібліотека імені Вернадського, Index Copernicus)* 4. Семко В.В., Бурячок В.Л., Толюпа С.В., Складанний П.М Модель управління захистом інформації в інформаційно-телекомунікаційній системі. Вісник Національного університету «Львівська політехніка»: Радіоелектроніка та телекомунікації. № 818, 2015. с.151-155 *(Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: РИНЦ, Index Copernicus)* 5. Семко В.В. Метод побудови областей керованих станів динамічного об'єкту. Математичні машини і системи. 2015. Вип. №3. С.44-52. *(Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Національна бібліотека імені Вернадського, Google Scholar, eLIBRARY.RU)* 6. Семко В.В. Топологічний ситуаційний аналіз та синтез стратегій управління об'єктом в умовах конфлікту, невизначеності поведінки та варіативної множини об'єктів спостереження. «ScienceRise», 2016, №9/2(26), Видавництво "Технологічний Центр". с. 62– 69 *(Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: РИНЦ, Index Copernicus)* 7. Семко В.В., Бурячок В.Л. Модель функціонування системи інтелектуального управління об'єктом. «Наукові записки Українського науково-дослідного інституту зв'язку». №3(43), 2016. с.21–29 *(Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Національна бібліотека імені Вернадського, CrossRef, Google Scholar)* 8. Lakhno V., Kazmirchuk S, Tkach Y., Malyukov V., Kasatkin D., Semko V., Turgynbayeva., Chernysh L. Computer support system for choosing the optimal managing strategy by the mutual investment procedure in smart city. Preprint (Журнал включено до міжнародної наукометричної бази **Scopus**) ***30.2) Наявність не менше п'яти наукових публікацій у наукових виданнях, включених до переліку наукових фахових видань України*** 1. Семко В.В. Формальний опис простору пошуку при синтезі рішень. Проблеми інформатизації та управління. 2013. Вип. 2(42). С.104-111. 2. Семко В.В. Модель взаємодії кібернетичних організмів та синтез стратегій оптимального керування в кібернетичному просторі. Проблеми інформатизації та управління. 2013. Вип.3(43). С.75-82. 3. Семко В.В., Семко О.В. Дослідження властивостей рішення задачі конфлікту за методом інтегрального усікання варіантів. Проблеми інформатизації та управління. 2014. Вип. 2(46). С.60-71. 4. Семко В.В. Використання методу інтегрального усікання варіантів при вирішенні задач конфлікту взаємодії об'єктів в просторі спостереження. Телекомунікаційні та інформаційні технології. 2015. Вип. № 1. С.59-66. 5. Семко В.В. Вирішення задачі конфлікту за методом інтегрального усікання варіантів. Телекомунікаційні та інформаційні технології. 2015. Вип. № 2. С.40-50. 6. Семко В.В., Гулак Г.М., Складанний П.М. Модель системи виявлення вторгнень з використанням двоступеневого критерію виявлення мережних аномалій. Сучасний захист інформації. 2015. Вип. № 4. С.81-85. 7. Семко В.В., Чепіженко В.І. Побудова областей керованих станів динамічного об'єкта Телекомунікаційні та інформаційні технології. 2015. Вип. № 3. С.25-30. 8. Бурячок В.Л., Семко В.В., Бурячок Л.В. Технологія проведення порівняльного аналізу та оцінювання стану захищеності автоматизованих інформаційних систем. «Сучасний захист інформації». № 4, 2016. с. 16–24 9. Семко В.В. Квазілінійна система інтелектуального управління конфліктом. Зв'язок. 2016. № 5. С.68-71. 10. Семко В.В. Алгебраїчний підхід до рішення конфлікту за методом інтегрального усікання варіантів. Сучасний захист інформації. 2016. № 3. С.4-10. 11. Khmelevskoy R., Khmelevskoy Y., Kozachok V., Semko V., Ilin O. Information Security and Development Problems

				eGovernment Systems in Ukraine. «Сучасний захист інформації». № 3, 2018. с. 71–77 12. Семко О.В., П.М.Складанний, В.В.Семко, В.Л.Бурячок Методологія інтелектуального управління маршрутизацією в конфліктуючих сенсорних мережах варіативної топології. «Сучасна спеціальна техніка». №4(55), 2018, с. 64 – 76 ***30.3) Наявність виданого підручника чи навчального посібника або монографії*** 1. Бурячок В.Л., Семко В.В., Складанний П.М. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. К.: ДУТ, 2016. 132 с. Гриф надано МОН України. Лист № 1/11-8662 від 22.06. 2015 р. ***30.4) Наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня*** *Науковий керівник кандидатської дисертації:* Приступа Володимир Віталійович, дисертаційна робота на здобуття наукового ступеня кандидата технічних наук на тему "Інформаційна технологія забезпечення достовірності інформації при обміні даними на основі каскадного кодування", науковий ступінь присуджено на засіданні спецради Д 26.255.01 Інституту телекомунікацій і глобального інформаційного простору НАН України за спеціальністю 05.13.06 "Інформаційні технології", наказ МОН України щодо присвоєння вчених звань від 26.02.2015 № 217. ***30.5) Участь у міжнародних наукових проектах, залучення до міжнародної експертизи, наявність звання "суддя міжнародної категорії".*** Наукове керівництво науковим проектом (2014р.) EUROPEAID/114372/C/S/UA "Enhancing Border Management: Supply of Border Management. Equipment to the Sumy Border Guard ***30.8) Виконання функцій наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії наукового видання, включеного до переліку наукових фахових видань України, або іноземного рецензованого наукового видання*** Наукове керівництво НДР та ДКР: 1. Шифр «Модернізація-С» - тема «Модернізація існуючих засобів функціональних центрів, комплексів та систем подвійного призначення, які знаходяться у сфері управління НКАУ, для виконання завдань спеціального інформаційного призначення» (номер держреєстрації 0103U005355). 2. Шифр «Сейсмологія» - тема «Комплекс робіт з розробки системи технічного захисту інформації для інформаційно-обчислювального центра Головного центру спеціального контролю» (номер держреєстрації 0103U008106). 3. Шифр «Моніторинг-С» (тема «Обстеження інформаційно-аналітичної системи НКАУ та розробка рекомендацій щодо забезпечення вимог технічного захисту інформації в ІАС НКАУ» (номер держреєстрації 01032U008326). 4. Шифр «Мережа» (тема «Створення комп'ютерної мережі на базі технології WI-FI та дослідження питань щодо створення системи захисту інформації» (номер держреєстрації 0104U004812). 5. Шифр «Мережа» - тема «Розроблення технічного завдання на комплексну систему захисту інформації мультисервісної мережі Київської міської державної адміністрації» (номер держреєстрації 0106U005506). 6. Шифр «Сховище» - тема «Розробка системи захисту інформації технології сховища даних» (номер держреєстрації 0106U012519). 7. Шифр «Радіус» - тема «Створення концепції та політик технічного захисту інформації у інформаційно-телекомунікаційних системах, що належать ВАТ "Укртелеком"» (номер держреєстрації 0108U000999). 8. Шифр "ДЦІР5-1" – тема "Послуги з доопрацювання складових компонентів інформаційно-телекомунікаційної системи електронної взаємодії органів виконавчої влади з придбанням примірнику програмної продукції перевірки/накладання електронного цифрового підпису та примірнику програмної продукції платформи віртуалізації серверів VMWare vSphere (ESX/ESXi) з системою vCenter Server" (номер держ. реєстрації 0115U006734). 9. Шифр "НП/2-2015" – тема "Розробка вимог до архітектури Системи електронної взаємодії державних електронних інформаційних ресурсів" (номер держ. реєстрації 0115U007171).

				У 2013 – 2017 роках був виконавцем НДР «Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем в умовах впливу кібернетичних атак» (номер державної реєстрації 0114U000391, шифр «Живучість»). ***30.11) Участь в атестації наукових працівників як офіційного опонента або члена постійної спеціалізованої вченої ради (не менше трьох разових спеціалізованих вчених рад)*** 2017 – 2018р.р. член спеціалізованої вченої ради Д 26.861.06 Державного університету телекомунікацій з правом прийняття до розгляду та проведення захисту дисертацій на здобуття наукового ступеня доктора технічних наук за спеціальностями 21.05.01 "Інформаційна безпека держави" та 05.13.21 "Системи захисту інформації" З 2018 року й дотепер – член спеціалізованої вченої ради Д 26.062.03 при Національному авіаційному університеті з правом прийняття до розгляду та проведення захисту дисертацій на здобуття наукового ступеня доктора технічних наук за спеціальностями 05.13.03 "Системи та процеси керування", 05.22.20 "Експлуатація та ремонт засобів транспорту" та 05.22.13 "Навігація та управління рухом". Офіційне опонування дисертації на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – "Телекомунікаційні системи та мережі" Андерса КАРЛССОНА за темою «Модель та метод виявлення низькоінтенсивних атак на прикладному рівні». Захист на спеціалізованій вченій раді Д 64.052.09 Харківського Національного університету радіоелектроніки, 02.12.2017р. Офіційне опонування дисертації на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – "Інформаційні технології" ВАСИЛЕНКА Владислава Михайловича за темою «Засоби адаптивного управління системою передачі інформації в умовах апріорної невизначеності». Захист на спеціалізованій вченій раді Д 26.255.01 Інституту телекомунікацій і глобального інформаційного простору НАН України, 27.12.2018р. ***30.12) Наявність не менше п'яти авторських свідоцтв та/або патентів загальною кількістю два досягнення*** 1. Свідоцтво про реєстрацію авторського права на твір №25553 від 24.09.2008. Комп'ютерна програма «Програма для ПЕОМ щодо ведення бази даних дозволів на викиди забруднюючих речовин у атмосферне повітря та надання інформації громадськості» («Дозвіл») / В.В.Семко, О.О.Михайловський; заявник та власник авторських прав Товариство з обмеженою відповідальністю «Елан»; заява №26809 від 22.08.2008; видане Державним департаментом інтелектуальної власності Міністерства освіти і науки України; опубл. Кат. №12, Бюл. №17. 2. Свідоцтво про реєстрацію авторського права на твір №26411 від 11.11.2008. Комп'ютерна программа «Психодіагностичні методики» до тематичного блоку «Пізнай себе» Програмно-апаратного комплексу «Профорієнтаційний термінал» / В.В.Семко, О.О.Михайловський; заявник та власник авторських прав Товариство з обмеженою відповідальністю «Елан»; заява №27406 від 27.10.2008; видане Державним департаментом інтелектуальної власності Міністерства освіти і науки України; опубл. Кат. №12, Бюл. №17. 3. Свідоцтво про реєстрацію авторського права на твір №39113 від 11.07.2011. Комп'ютерна программа «Крос-платформена клієнт-серверна технологія захищеного обміну електронними даними з використанням терміналів мобільного телефонного зв'язку» («ТЗОД») / Семко В.В., Михайловський О.О., Гіденко О.В., Зінов'єв О.В., Мельник В.Т., Барткова В.А; заявник та власник авторських прав Товариство з обмеженою відповідальністю «Елан»; заява №39558 від 20.05.2011; видане Державним департаментом інтелектуальної власності Міністерства освіти і науки України; опубл. Кат. №15, Бюл. №25. ***30.16) Участь у професійних об'єднаннях за спеціальністю;*** Аерокосмічна академія України, академік АКАУ. ***30.17) Досвід практичної роботи за спеціальністю не менше п'яти років;*** Досвід практичної діяльності за напрямками створення й впровадження систем технічного і криптографічного захисту інформації та спеціальних системами негласного зняття інформації з каналів зв'язку 21 рік. Роботи проводились в товаристві

				з обмеженою відповідальністю "Елан" (м.Київ) у відповідності до ліцензій Служби Безпеки України та Державної служби СЗЗІ України. З 2014 по 2017 рік приймав участь в створенні і впровадженні систем електронного врядування України в частині концептуальних і технологічних рішень, включаючи напрямок технічного та криптографічного захисту інформації. В 2018 році приймав участь в створенні і впровадженні Єдиної автоматизованої системи управління Збройними Силами України, включаючи напрямок технічного та криптографічного захисту інформації. ***30.18) Наукове консультування установ, підприємств, організацій протягом не менше двох років.*** Державне підприємство «Державний центр інформаційних ресурсів України» (2016 – 2017р.р.)
БОРСУКОВ-СЬКИЙ Юрій Володимирович	Професор кафедри інформаційної та кібернетичної безпеки	Ні	Технології розслідування інцидентів безпеки	**Освіта:** Київський державний університет ім. Т.Г. Шевченка, 1980 р. Спеціальність: «Прикладна математика». Кваліфікація: «Математик». **Науковий ступінь:** кандидат технічних наук, 1986 р. Наукова спеціальність 05.22.14 «*Експлуатація повітряного транспорту*»). Тема дисертації: «*Автоматизація процесу оцінки параметрів моделей ВС і оптимальне планування тестових режимів польоту*». **Вчене звання:** немає. **Види і результати професійної діяльності за спеціальністю відповідно до п.30 Ліцензійних умов провадження освітньої діяльності:** **п.п. 30.1), 30.2), 30.3), 30.15), 30.16), 30.17).** ***30.1) Наявність за останні п'ять років (2014 – 2019 р.р.) наукових публікацій у періодичних виданнях, які включені до наукометричних баз, рекомендованих МОН, зокрема Scopus або Web of Science Core Collection.*** ***Наукометричні бази Scopus або Web of Science Core Collection*** 1. Бурячок В.Л., Богуш В.М., Борсуковський Ю.В., Складанний П.М., Борсуковська В.Ю., Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України. Електронне наукове фахове видання «Інформаційні технології і засоби навчання», 2018, Том 67, №5, с.277-291. ISSN: 2076-8184. ***Інші наукометричні бази*** 2. Борсуковський Ю.В. Прикладні аспекти розробки політики категорування інформації з обмеженим доступом / Ю.В.Борсуковський, В.Ю.Борсуковська, В.Л. Бурячок, П.М.Складанний // «Системи обробки інформації». № 2(153), 2018. С. 117-126 (*Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Ulrich's Periodicals Directory, CrossRef, Index Copernicus, General Impact Factor, Scientific Indexed Service, Citefactor, ResearchBib, Orcid, Academic Resource Index, Google Scholar*) 3. Borsukovskii Y., Borsukovska V., Buriachok V. Strategy of the higher educations of Ukraine in training of experts on informational and cyber security / XIV International Conference "Strategy of Quality in Indastry and Education", June 4-8 2018, Varna Bulgaria, Proceedings Volume 1, p. 226-234. URL: r*epositsc.nuczu.edu.ua/bitstream/123456789/7002/1/Файл1212056703.pdf* 4. Бурячок В.Л., Богуш В.М., Борсуковський Ю.В., Складанний П.М., Борсуковська В.Ю., Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України. ISSN: 2076-8184. Інформаційні технології і засоби навчання, 2018, Том 67, №5, с.277-291. URL: *https://journal.iitta.gov.ua/index.php/itlt/issue/view/96/showToc* ***30.2) Наявність не менше п'яти наукових публікацій у наукових виданнях, включених до переліку наукових фахових видань України:*** 1. Борсуковський Ю.В., Аналіз сучасних вимог до створення парольних політик корпоративних

користувачів. Сучасний захист інформації, - 2016, № 3, с. 72-76

2. Борсуковський Ю.В. Визначення сучасних вимог до створення політики управління доступом корпоративних користувачів. Сучасний захист інформації, - 2016, № 4, с. 5-9

3. Борсуковський Ю.В. Напрямки формування політик кібербезпеки для державного, банківського та приватного секторів. Modern Methodologies, Innovations, and Operational Experience on the Field of Technical Science: Conference proceedings, December 27-28, 2017, Radom, Republic of Poland, с. 8-11

4. Борсуковський Ю.В., Бурячок В.Л. Роль і місце вищих навчальних закладів у створенні системи інформаційної та кібернетичної безпеки України. Сучасний захист інформації, - 2017, № 1(30), с. 34-40

5. Борсуковська В. Ю., Борсуковський Ю. В. Безперервність бізнесу: новий тренд або необхідність. Економіка. Менеджмент. Бізнес. - 2017, № 2(20), с. 48-52

6. Борсуковський Ю.В., Бурячок В.Л., Борсуковська В.Ю. Базові напрямки забезпечення кібербезпеки державного та приватного секторів. Сучасний захист інформації, - 2017, № 2(30), с. 85-89

7. Борсуковська В. Ю., Борсуковський Ю. В. Рекомендації по категоріюванню інформації з обмеженим доступом. Сучасний захист інформації, - 2017, № 4(32), с. 9-17

8. Борсуковський Ю.В., Борсуковська В.Ю., Бурячок В.Л., Складанний П.М. Прикладні аспекти розробки політики категорування інформації з обмеженим доступом/ DOI: 10.30748/soi.2018.153.15 / Системи обробки інформації. — 2018. — № 2(153). – с. 117-126.

9. Борсуковський Ю. В., Борсуковська В. Ю. Визначення сучасних вимог щодо політики використання засобів криптографічного захисту інформації. Сучасний захист інформації, - 2018, № 1(33), с. 74-81

10. Борсуковський Ю. В., Борсуковська В. Ю. Прикладні аспекти захисту інформації в сучасних умовах. Сучасний захист інформації, - 2018, № 2(34), с. 6-11

11. Борсуковський Ю.В., Борсуковська В.Ю. Прикладні аспекти захисту аутентифікаційних даних. DOI: https://doi.org/10.28925/2663-4023.2019.3 . Кібербезпека: освіта, наука, техніка, 2019, Том 3, №3, с.42-51.

12. Борсуковський Ю.В., Борсуковська В.Ю. Прикладні аспекти захисту інформації в умовах обмеженого фінансування. DOI: 10.28925/2663-4023.2018.1.2634X. Кібербезпека: освіта, наука, техніка, 2019, Том 3, №3, с.26-34.

30.3) Наявність виданого підручника чи навчального посібника або монографії

1. Borsukovskyi Y.V., Borsukovska V.Y., Model for cryptography protection of confidential information. Engineering sciences: development prospects in countries of Europa at the beginning of the third millennium. ISBN: 978-9934-571-63-3. Economics College in Stalowa Wola, Poland. Collective monograph. Volume 1, 2018, 460 p. (p.43-63).

30.15) Наявність науково-популярних та/або консультаційних (дорадчих) та/або дискусійних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій:

1	Новий підхід до забезпечення безпеки кінцевих точок	Блог	Інтернет видання «Комп'ютерний огляд» - 2016
2	Чи є життя у антивірусів	Блог	Інтернет видання «Комп'ютерний огляд» - 2016
3	Про ввімкнуте за замовчуванням шифрування	Блог	Інтернет видання «Комп'ютерний огляд» - 2016
4	Про ввімкнуте за замовчуванням шифрування	Блог	Інтернет видання «Комп'ютерний огляд», - 2016
5	Забезпечення безпеки кінцевих точок потребує нових підходів	Блог	Інтернет видання «Комп'ютерний огляд», - 2016
6	Новий підхід до забезпечення безпеки кінцевих точок	Блог	Інтернет видання «Комп'ютерний огляд», - 2016

				7 | Кібербезпека переходить на національний рівень | Блог | Інтернет видання «Комп'ютерний огляд» - 2017 8 | А чи був хлопчик (за результатами атак шифрувальників Wannacry та Petya) … ? | Блог | Інтернет видання «Комп'ютерний огляд» - 2017 9 | Національні особливості інформаційної безпеки 2018 | Блог | Інтернет видання «Комп'ютерний огляд» - 2018 10 | Трохи про практику захисту паролів | Блог | Інтернет видання «Комп'ютерний огляд» - 2018 ***30.16) Участь у професійних об'єднаннях за спеціальністю*** Член міжнародного товариства «Internet Society». Member ID – 2187523 Режим доступу: https://admin.internetsociety.org/. ***30.17) Досвід практичної роботи за спеціальністю не менше п'яти років*** 1. Керівник служби інформаційної безпеки Остхем (міжнародний холдинг, 20 тис. співробітників), заступник директора, Київ, Україна, 2012 – 2015 Розроблено нову технологію зберігання, захисту та моніторингу конфіденційної інформації міжнародного холдингу, розроблені базові принципи розвитку і стандартизації ІТ, проведені роботи з модернізації ІТ та ІБ керуючої компанії, розроблені політики, процедури, інструкції ІТ та ІБ. Впроваджено систему контролю інформаційних потоків (пошта, інтернет), впроваджена корпоративна система шифрування інформації. Розроблено та впроваджено спеціальну автоматизовану система активної протидії несанкціонованому доступу до конфіденційної інформації. Проведено навчання співробітників, впроваджені регламентуючі документи з управління інформаційними технологіями та інформаційною безпекою. Брав безпосередню участь в розробці плану впровадження заходів щодо захисту конфіденційної інформації Груп ДФ і Надра-банк на період 2012-2017. 2. Президент ТОВ «Бартек», Київ, Україна, 1994 – 2012 Розроблено архітектуру та впроваджені: система запобігання вторгнень, система контролю додатків, система контролю інтернет і поштового трафіку, система криптографічного захисту інформації, система контролю зберігання і перенесення інформації на зовнішніх пристроях. Проведено консалтинг систем інформаційної безпеки. Замовники: Альфа-банк, ВТБ банк, ВАБ банк, Банк «Форум», Брокбізнесбанк, Райффайзен банк Аваль, Корпорація Interpipe (EastOne), ДП «Українські спеціальні системи» СБ України, Адміністрація Президента України, Державна податкова адміністрація України, Державна митна служба України, Міністерство внутрішніх справ України, Державний аеропорт «Борисполь», АТ «Укртранснафта», АТ «Укроборонсервіс», Департамент спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України, та інші.
АНОСОВ Андрій Олександрович	Доцент кафедри інформаційної та кібернетичної безпеки	Так	Моніторинг, аудит та адміністрування захищених ІТ систем і мереж	**Освіта:** Воронізьке вище воєнно-інженерне училище радіоелектроніки, 1988 р. Спеціальність: «Радіоелектронні засоби». Кваліфікація: «Радіоінженер». Національний університет оборони України, 1999 р. Спеціальність: «*Організація бойового та оперативного забезпечення військ(сил)*». Кваліфікація: «*Магістр військового управління*». **Науковий ступінь:** кандидат військових наук, 2005 р. Наукова спеціальність 20.01.12 «*Радіоелектронна боротьба, способи та засоби*». Тема дисертації: «*Методика обґрунтування раціональних способів радіоелектронного подавлення супутникових систем зв'язку*». **Вчене звання:** доцент за кафедрою інформаційної та кібернетичної безпеки, 2016 р.. **Види і результати професійної діяльності за спеціальністю відповідно до п.30 Ліцензійних умов провадження освітньої діяльності:** **п.п. 30.1), 30.2), 30.3), 30.5), 30.8), 30.13), 30.17), 30.18).** ***30.1) Наявність за останні п'ять років (2014 – 2019 р.р.) наукових публікацій у періодичних виданнях, які включені до наукометричних баз, рекомендованих МОН, зокрема Scopus або Web of Science Core Collection.***

				<u>Наукометричні бази Scopus або Web of Science Core Collection</u> 1. Аносов А.О., Бржевська З.М., Гайдур Г.І. Вплив на достовірність інформації як загроза для інформаційного простору. Електронне наукове видання «Кібербезпека: освіта, наука, техніка». №2 (2), 2018. С. 105-112 *(Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Національна бібліотека імені Вернадського, Google Академія, Reasearch Bibl, PKP Index)* 2. Бржевська З.М., Довженко Н.М., Киричок Р.В., Гайдур Г.І., Аносов А.О. Інформаційні війни: проблеми, загрози та протидія. Електронне наукове видання «Кібербезпека: освіта, наука, техніка». №3 (3), 2019. С. 105-112 *(Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: Національна бібліотека імені Вернадського, Google Академія, Reasearch Bibl, PKP Index)* 3. Бурячок В.Л., Аносов А.О., Платоненко А.В. Спосіб генерування паролю для бездротових мереж з використанням змінного правила ускладнення. «Захист інформації». Preprint (2019). *(Журнал включено до міжнародних каталогів наукових видань і наукометричних баз: WorldCat, Ulrichsweb Global Serials Directory, eLibrary.ru, BASE, Simple Search Metadata)* 4. K. Sauanova, S. Sagyndykova, V. Buriachok, N. Mazur, A. Anosov, S. Smirnov. Development of a model of cyber security management for automated systems. International Journal of Civil Engineering and Technology (IJCIET),Volume 10, Issue 03, 2019 Pages: 454-463. (Журнал включено до міжнародної наукометричних баз Google Scolar, PublicationsList.org, Academia.edu, IndexCopernicus, ResearchGate, EBSCO, DOAJ тощо) 5. Бурячок В.Л., Богуш В.М, Аносов А.О., Соколов В.Ю., Складанний П.М. Впровадження технологій активного навчання в освітній процес закладів вищої освіти України за спеціальністю «кібербезпека». Електронне наукове фахове видання «Інформаційні технології і засоби навчання». Preprint (2019). (*Журнал включено до міжнародної наукометричної бази* ***Web of Science Core Collection****)* 6. Lakhno V., Anosov A. and etc. Conceptual Model Of The Automated Decision-Making Process In Analysis Of Emergency Situations On Railway Transport. International Conference on Research and Practical Issues of Enterprise Information Systems, 2019. Preprint (Журнал включено до міжнародної наукометричної бази **<u>Scopus</u>**) ***30.2) Наявність не менше п'яти наукових публікацій у наукових виданнях, включених до переліку наукових фахових видань України*** 1. Аносов А.О. Створення на основі шумових процесів стеганоконтейнерів для забезпечення потрібного рівня стійкості до стеганоатак за відсутності шифрування корисного повідомлення. «Системи озброєння і військова техніка». № 4(36), 2013. С. 43–46. 2. Аносов А.О., С.П. Василенко, О.В. Сторожук. Модель комп'ютерної радіомережі військово-морського об'єднання як об'єкта програмно-комп'ютерного подавленняпід час оборони держави з морського напрямку. «Наука і техніка Повітряних Сил Збройних Сил України». № 4(13), 2013. С. 117–122. 3. Аносов А.О. Моделювання DDos атак на комп'ютерні мережі для визначення ознак їх проведення «Сучасний захист інформації». № 3. 2015 С. 13 – 17. 4. Аносов А.О., Платоненко А.В. Генерування унікального паролю зі змінним правилом ускладнення. «Сучасний захист інформації». №3 (31), 2017, С. 81-85. 5. Платоненко А.В., Аносов А.О. Модель перехоплення та захист інформації в бездротових мережах. «Сучасний захист інформації» №2 (30), 2017, С. 90–94. 6. Аносов А.О., Пузняк З.М. Інформаційно-орієнтована модель як реалізація методики виявлення впливу на достовірність інформації в інформаційному просторі. «Сучасний захист інформації». №4(32), 2017, С. 55-59. 7. А.О. Аносов, М.М. Проценко, О.Л. Дубинко, М.Я. Павлунько Застосування вейвлет-перетворення для аналізу цифрових сигналів. «Сучасний захист інформації» №1(33). 2018, С. 38-42. ***30.3) Наявність виданого підручника чи навчального посібника або монографії*** 1. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в

інформаційній безпеці: підручник. К.: ДУТ, 2015. 345 с.

2. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М. Технології забезпечення безпеки мережевої інфраструктури: підручник. К.: КУБГ, 2019. 225 с.

30.5) Участь у міжнародних наукових проектах, залучення до міжнародної експертизи, наявність звання "суддя міжнародної категорії"

З 2013 року по 2017 рік був приймав участь в програмі ЄС "ENGENSEC" з підготовки магістрів у сфері інформаційної та кібербезпеки (проект 544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR), яка впроваджувалась у Державному університеті телекомунікацій.

30.8) Виконання функцій наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії наукового видання, включеного до переліку наукових фахових видань України, або іноземного рецензованого наукового видання

Протягом 2002 - 2013 років брав участь як виконавець, відповідальний виконавець або науковий керівник в 18 науково-дослідних і дослідно-конструкторських роботах на спеціальну тему, що за замовленням Міністерства оборони України виконувались Національною академією оборони України та НДІ Головного управління розвідки ЗС України.

У 2013 – 2017 роках був виконавцем НДР «Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем в умовах впливу кібернетичних атак» (номер державної реєстрації 0114U000391). Метою НДР є підвищення живучості ІКС в умовах впливу кібератак за рахунок протидії спробам порушення захисту таких систем та їх відновлення після злому. Основними завданнями НДР є:

1) аналіз стану живучості типових ІКС та розробка стратегій забезпечення живучості;
2) розробка моделей політики безпеки ІКС, здатних протистояти цілеспрямованим спробам порушення безпеки;
3) визначення типових архітектур та підходів до синтезу ІКС, що відповідають вимогам по забезпеченню живучості.

30.10) Наявність виданих навчально-методичних посібників/посібників для самостійної роботи студентів та дистанційного навчання, конспектів лекцій/ практикумів/ методичних вказівок/рекомендацій загальною кількістю три найменування

№ з/п	Назва	Характер роботи	Вихідні дані	Обсяг, стор.	Співавтори
1.	Безпека мережевої інфраструктури	Посібник з дистанційного навчання	К.: ДУТ, 2016.	87	
2.	Технології адміністрування та експлуатація захищених ІКС	Посібник з дистанційного навчання	К.: ДУТ, 2017.	124	
3.	Комплексні системи інформаційної безпеки	Посібник з дистанційного навчання	К.: ДУТ, 2017.	94	

30.17) Досвід практичної роботи за спеціальністю не менше п'яти років

Досвід практичної діяльності за напрямками створення та впровадження систем технічного захисту інформації – 19 років. Так протягом 1988 – 1997 років створював, супроводжував та проводив технічне обслуговування систем технічного захисту інформації на об'єктах інформаційної діяльності у участинах та підрозділах радіоелектронної боротьби МО СРСР. З 2011 по 2013 р.р. – займався проектуванням, здійснював впровадження та забезпечував функціонування комплексних систем захисту інформації за замовленням Міністерства оборони України. В цей час в рамках співпраці науково-дослідного інституту Головного управління розвідки МО України із вендорами в сфері захисту інформації та забезпечення безпеки інформаційно-комунікаційних систем такими, як ТОВ «Криптон» (м.Київ) та Інститутом інформаційних технологій (м.Харків), тощо займався створенням систем добування інформації із закритих ІТ і криптосистем. У 2013 - 2017 р.р. брав участь у програмі ЄС "ENGENSEC" з підготовки магістрів у сфері інформаційної та кібербезпеки

				(проект 544 455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR) та практично реалізовував її окремі елементи в Державному університеті телекомунікації. ***30.18) Наукове консультування установ, підприємств, організацій протягом не менше двох років.*** ТОВ "Криптон" (2011 – 2013 р.р., м. Київ).
ЖДАНОВА Юлія Дмитрівна	Доцент кафедри інформаційної та кібернетичної безпеки	Так	Прикладна загальна теорія систем безпеки	**Освіта:** Луганський державний педагогічний інститут ім.Т.Г. Шевченка, 1981 р. Спеціальність: «Математика». Кваліфікація: «Викладач математики». Державний університет телекомунікацій, 2017 р. Спеціальність: «Безпека інформаційних і комунікаційних систем». Кваліфікація: «Інженер із захисту інформації в інформаційних і комунікаційних системах». **Науковий ступінь:** кандидат фізико-математичних наук, 1992 р. Наукова спеціальність 01.01.05 «Теорія ймовірностей і математична статистика». Тема дисертації: «Випадкові блукання та випадкові еволюції на скінченних розв'язуваних групах». **Вчене звання:** доцент за кафедрою вищої математики, 2005р.. **Види і результати професійної діяльності за спеціальністю відповідно до п.30 Ліцензійних умов провадження освітньої діяльності:** **п.п. 30.1), 30.2), 30.3), 30.16).** ***30.1) Наявність за останні п'ять років (2014 – 2019 р.р.) наукових публікацій у періодичних виданнях, які включені до наукометричних баз, рекомендованих МОН, зокрема Scopus або Web of Science Core Collection.*** ***Наукометричні бази Scopus або Web of Science Core Collection*** 1. Бурячок В.Л., Жданова Ю.Д., Спасітєлєва С.О., Складанний П.М., Шевченко С.М., Мазур Н.П. Формування та розвиток дослідницьких умінь студентів інформаційної та кібернетичної безпеки засобами освітніх технологій. ISSN: 2076-8184. Електронне наукове фахове видання «Інформаційні технології і засоби навчання». Preprint (2019). (Журнал включено до міжнародної наукометричної бази **Web of Science Core Collection**) ***Інші наукометричні бази*** 2. Жданова Ю.Д. Автоматизація процесу генерування і перевірки індивідуальних навчальних завдань для студентів з теми «Дії в кільці многочленів» / Ю.Д. Жданова, С.О. Спасітєлєва, С.М. Шевченко // Фізико-математична освіта: науковий журнал. – 2017. – Вип. 1 (11). – С. 42 – 47. (*Журнал включено до міжнародних каталогів наукових видань і наукометричних баз:* Index Copernicus) 3. Жданова Ю.Д. Формування у студентів ІТ-спеціальностей компетентностей в області захисту інформації з використанням криптографічних служб .NET FRAMEWORK / Ю.Д. Жданова, С.О. Спасітєлєва, С.М. Шевченко // Фізико-математична освіта: науковий журнал. – 2019. – Вип. 1 (19). – С. 48 – 54. (Index Copernicus) ***30.2) Наявність не менше п'яти наукових публікацій у наукових виданнях, включених до переліку наукових фахових видань України*** 1. Жданова Ю.Д. Вплив інтелектуального рівня фахівців ІТ-галузі на економіку держави / О.В. Барабаш, С.М. Шевченко, Ю.Д. Жданова // Зв'язок. – 2015. – №6 (118) – С. 14-18. 2. Жданова Ю.Д. Математичні компетенції майбутніх фахівців інформаційної безпеки / С.М. Шевченко, Ю.Д. Жданова // Сучасний захист інформації. – К.: ДУТ, 2016. – № 4. – С. 90 – 96. 3. Жданова Ю.Д. Статистична обробка експериментальних даних як одна з форм науково-дослідної роботи студентів напряму «Кібербезпека» / С.М. Шевченко, Ю.Д. Жданова, С.О. Спасітєлєва, О.В. Адамович // Сучасний захист інформації. – К.: ДУТ, 2017. – № 2(30). – С. 95 – 103.

				4. Жданова Ю.Д. Формування практичних навичок студентів спеціальності 125 Кібербезпека за допомогою віртуальних лабораторій / Ю.Д. Жданова, С.О. Спасітєлєва, С.М. Шевченко // Матеріали VII Міжнар. наук.-практ. конф. «Математика в сучасному технічному університеті», Київ, 28—29 грудня 2018 р. — Вінниця: Видавець ФОП Кушнір Ю. В., 2019. — С. 253 – 255. 5. Жданова Ю.Д. Застосування бібліотеки класів SECURITY.CRYPTOGRAPHY для практичної підготовки спеціалістів з кібербезпеки / Ю.Д. Жданова, С.О. Спасітєлєва, С.М. Шевченко // "Кібербезпека: освіта, наука, техніка", № 4, 2019. – С. 44 – 53. 6. Жданова Ю.Д. Математичні методи в кібербезпеці: фрактали та їх застосування в інформаційній та кібернетичній безпеці / Ю.Д. Жданова, С.О. Спасітєлєва, С.М. Шевченко, О.В. Негоденко, К.В. Кравчук // "Кібербезпека: освіта, наука, техніка", Preprint (2019). № 5. ***30.3) Наявність виданого підручника чи навчального посібника або монографії*** 1. Shevchenko S., Zhdanova Yu. Development of analytical thinking of students in the process of applied cryptology / S. Shevchenko, Yu. Zhdanova // Information and technologies in the development of socio-economic systems. Monograph 6. – Katowice: Katowice School of Technology, 2016. – С. 117 – 123. 2. Комп'ютерні дискретні структури: навчальний посібник для студентів галузі знань 12 – Інформаційні технології / Шевченко С.М., Онищенко В.В., Жебка В.В., Жданова Ю.Д. – К.: ДУТ, 2018. – с. 155 3. Теоретико-ймовірнісні та статистичні методи в захисті інформації. Підручник для студентів спеціальності 125 Кібербезпека / В.М. Астапеня, Ю.Д. Жданова, С.М. Шевченко. – К. Київський університет ім. Б.Грінченка. (подано до рецензування) ***30.16) Участь у професійних об'єднаннях за спеціальністю*** Член міжнародного товариства «Internet Society». Member ID – 2187060 Режим доступу https://admin.internetsociety.org/622619/Entity/Details?entityTypeId=d601a3bf-efa2-4bb7-907b-269e91ee1bc5&EntityId=37188942-23bf-4bdd-8943-d649b7009eb1
СОКОЛОВ Володимир Юрійович	Старший викладач кафедри інформаційної та кібернетичної безпеки	Так	Технології безпеки безпроводових і мобільних мереж Технології безпеки Web-ресурсів Прикладні аспекти тестувань на проникнення та етичного хакінгу	**Освіта:** Київський політехнічний інститут, .2005 р. Спеціальність: «Електронні системи». Кваліфікація: «Магістр електроніки». Державний університет інформаційно-комунікаційних технологій 2005–2008 роки: аспірантура за спеціальністю 05.13.21 «Системи захисту інформації». **Науковий ступінь:** Немає. 29 жовтня на засіданні СРД 26.255.01 Інституту телекомунікацій і глобального інформаційного простору НАН України захистив дисертаційну роботу на тему «Методи і засоби підвищення інформаційної та функціональної безпеки безпроводових мереж передавання даних» на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 «Інформаційні технології». **Вчене звання:** немає. **Види і результати професійної діяльності за спеціальністю відповідно до п.30 Ліцензійних умов провадження освітньої діяльності:** **п.п. 30.1), 30.2), 30.3), 30.5), 30.8), 30.10), 30.13), 30.16), 30.17).** ***30.1) Наявність за останні п'ять років (2014 – 2019 р.р.) наукових публікацій у періодичних виданнях, які включені до наукометричних баз, рекомендованих МОН, зокрема Scopus або Web of Science Core Collection.*** ***Наукометричні бази Scopus або Web of Science Core Collection*** 1. Astapenya V. M., Sokolov V. Yu. Research Results of the Impact of Spatial and Polarization Value of the Antennas on Network

				Capacity of Wireless Channels Standard IEEE 802.11. Antenna Theory and Techniques (ICATT) : in IX Int. Conf., 16–20 Sept. 2013. Odessa : IEEE, 2013. P. 172–174. DOI: 10/cvdr. (*Журнал включено до міжнародної наукометричної бази* ***Scopus***). 2. Astapenya V. M., Sokolov V. Yu. Modified Accelerating Lens as a Means of Increasing the Throughput, Range and Noise Immunity of IEEE 802.11 Systems. Antenna Theory and Techniques (ICATT) : in X Anniversary Int. Conf., 21–24 Apr. 2015. Kharkiv : IEEE, 2015. P. 267–269. DOI: 10/cvdq. (*Журнал включено до міжнародних наукометричних баз* ***Scopus*** *та* ***Web of Science Core Collection***). 3. Astapenya V. M., Sokolov V. Yu. Experimental Evaluation of the Shading Effect of Accelerating Lens in Azimuth Plane. Antenna Theory and Techniques : in XI Int. Conf., 24–27 May 2017. Kyiv : IEEE, 2017. P. 389–391. DOI: 10/cvdp. (*Журнал включено до міжнародних наукометричних баз* ***Scopus*** *та* ***Web of Science Core Collection***). 4. Sokolov V. Yu., Carlsson A., Kuzminykh I. Scheme for Dynamic Channel Allocation with Interference Reduction in Wireless Sensor Network. Problems of Infocommunications. Science and Technology (PIC S&T) : in IV Int. Sc. and Pract. Conf., 10–13 Oct. 2017. Kharkiv : IEEE, 2017. P. 564–568. DOI: 10/gc8w52. (*Журнал включено до міжнародних наукометричних баз* ***Scopus*** *та* ***Web of Science Core Collection***). 5. Bogachuk I., Sokolov V. Yu., Buriachok V. Monitoring Subsystem for Wireless Systems based on Miniature Spectrum Analyzers. Problems of Infocommunications. Science and Technology (PIC S&T) : in V Int. Sc. and Pract. Conf., 9–12 Oct. 2018. Kharkiv : IEEE, 2018. P. 581–585. DOI: 10/c4xt. (*Журнал включено до міжнародних наукометричних баз* ***Scopus*** *та* ***Web of Science Core Collection***). 6. Buriachok, V. L., Sokolov V. Yu. Implementation of Active Learning in the Master's Program on Cybersecurity. The Second International Conference on Computer Science, Engineering and Education Applications (ICCSEEA2019), 26–27 January 2019, Kiev, Ukraine:(Журнал включено до міжнародної наукометричної бази **Scopus**) 7. Mahyar TajDini, Volodymyr Sokolov, Volodymyr Buriachok. Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio. Proceedings of the 8th International Conference on "Mathematics. Information Technologies. Education" (MoMLeT&DS'2019), June 2–4, 2019: abstracts. — Vol. 2386. — Aachen : CEUR, 2019. — P. 287–296 :(Журнал включено до міжнародної наукометричної бази **Scopus**) 8. V.Buriachok, V.Sokolov, P.Skladannyi. Security Rating Metrics for Distributed Wireless Systems. Proceedings of the 8th International Conference on "Mathematics. Information Technologies. Education" (MoMLeT&DS'2019), June 2–4, 2019: abstracts. — Vol. 2386. — Aachen : CEUR, 2019. — P. . 222–233 :(Журнал включено до міжнародної наукометричної бази **Scopus**) ***Інші наукометричні бази*** 9. Buryachok V. L., Sokolov V. Yu. Low-Cost Spectrum Analyzers for Channel Allocation in Wireless Networks 2.4 GHz Range. World Science. 2018. No. 3 (31). Vol. 1. P. 9–16. DOI: 10/c4xx (*Журнал включено до міжнародних каталогів наукових видань і наукометричних баз:* Index Copernicus). 10. Buryachok V. L., Sokolov V. Yu. Using 2.4 GHz Wireless Botnets to Implement Denial-of-Service Attacks. Web of Scholar. 2018. No. 6 (24). Vol. 1. P. 14–21. DOI: 10/cvdn (*Журнал включено до міжнародних каталогів наукових видань і наукометричних баз:* Index Copernicus). ***30.2) Наявність не менше п'яти наукових публікацій у наукових виданнях, включених до переліку наукових фахових видань України*** 1. Богуш В. В., Соколов В. Ю. Дослідження захищеності Wi-Fi мереж. Зв'язок. 2009. №4 (88). С. 29–31. 2. Соловьев В. Р., Богуш В. В., Соколов В. Ю., Соловьева М. В. К вопросу о совершенствовании методики защиты информации от помех и вирусных атак в системах подвижной связи. Системный подход. Зв'язок. 2010. №1 (89). С. 54–61. 3. Соколов В. Ю. Кількісні показники оцінювання захищеності і ризиків від порушення безпеки у розподілених системах рухомого зв'язку. Захист інформації. 2010. №3 (48). С. 19–34. DOI: 10/cvds. 4. Соколов В. Ю. Порівняння математичних і функціональних моделей широкосмугових сигналів з ортогональним частотним розділенням. Управління розвитком складних систем. 2010. №4. С. 109–113. 5. Соколов В. Ю. Підвищення захищеності Wi-Fi мереж: пошук триває. Зв'язок. 2011. №1 (93). С. 53–57.

				6. Соколов В. Ю. Електромагнітна сумісність транспортних мереж і мереж доступу технологій IEEE 802.11g і 802.15.1. Зв'язок. 2011. №2 (94). С. 67–70. 7. Соколов В. Ю., Карацюба К. І. Використання дерев атак для аналізу захищеності безпроводових технологій стандарту IEEE 802.11. Вісник ДУІКТ. 2012. Т. 10, №1. С. 42–49. 8. Астапеня В. М., Соколов В. Ю. Використання прискорювальної лінзи для підвищення ефективності та завадозахищеності мереж IEEE 802.11b. Зв'язок. 2012. №2 (98). С. 33–37. 9. Астапеня В. М., Соколов В. Ю. Підвищення пропускної здатності безпроводових каналів зв'язку на основі поляризаційних ефектів у мережах IEEE 802.11. Зв'язок. 2012. №3 (99). С. 36–41. 10. Соколов В. Ю. Модифікація прямокутної квадратурної амплітудної модуляції для зменшення взаємного впливу двох безпроводових систем. Зв'язок. 2012. №4 (100). С. 50–57. 11. Бурячок В. Л., Астапеня В. М., Соколов В. Ю. Способы повышения доступности информации в беспроводных системах стандарта IEEE 802.11 с MIMO. Сучасний захист інформації. 2016. №2. С. 60–68. 12. Taj Dini M., Sokolov V. Yu. Internet of Things Security Problems. Сучасний захист інформації. 2017. №1. С. 120–127. DOI: 10/c56m. 13. Астапеня В. М., Соколов В. Ю. Методы и средства контроля доступности в беспроводных сетях. Сучасний захист інформації. 2017. №3. С. 28–35. 14. Taj Dini M., Sokolov V. Yu. Penetration Tests for Bluetooth Low Energy and ZigBee using the Software-Defined Radio. Сучасний захист інформації. 2018. №1. С. 82–89. DOI: 10/c4xz. 15. Соколов В. Ю., Курбанмурадов Д. М. Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності. Кібербезпека: освіта, наука, техніка. 2018. №1. С. 6–16. DOI: 10/c4xr. 16. Соколов В. Ю. Порівняння можливих підходів щодо розробки низькобюджетних аналізаторів спектру для сенсорних мереж діапазону 2,4–2,5 ГГц. Кібербезпека: освіта, наука, техніка. 2018. №2. С. 31–46. DOI: 10/c4xp. ***30.3) Наявність виданого підручника чи навчального посібника або монографії*** 1. Buriachok, V., Sokolov V. Increase the Speed of Spectrum Analyzers based on Atmel Atmega328 and ARM Cortex-M3 RISC Processors; [ed. M. Kozinski]. Bezpieczeństwo w Cyberprzestrzeni Społeczna Przestrzeń Internetu w Kontekście Wartości i Zagrożeń. Kharkiv : NUCPU, 2019. P. 283–297. ISBN: 978-83-63680-28-2. 2. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М.. Технології забезпечення безпеки мережевої інфраструктури: підручник. К.: КУБГ, 2019. 225 с. 3. Бурячок В.Л., Соколов В.Ю., Тадждіні М.М. Безпека безпроводових і мобільних мереж: навчальний посібник. К.: КУБГ, 2019. 132 с. 4. Бурячок В.Л., Соколов В.Ю. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів [Монографія]. К.: КУБГ, 2019. 164 с ***30.5) Участь у міжнародних наукових проектах, залучення до міжнародної експертизи, наявність звання "суддя міжнародної категорії"*** У 2013-2017 був представником Державного університету телекомунікацій в програмі ЄС «ENGENSEC» з підготовки магістрів у сфері інформаційної та кібербезпеки (проект 544 455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR) та впровадженні цієї програми в освітній процес Державного університету телекомунікацій, Національного університету «Львівська політехніка» і Харківського національного університету радіоелектроніки.У грудні 2017 року в рамках магістерського курсу «Wireless and Mobile Security» отримав диплом впровадження від 12.11.2017. З 2018 року отриманий досвід застосував при відкритті спеціальності 125 «Кібербезпека» в Київському університеті імені Бориса Грінченка року. ***30.8) Виконання функцій наукового керівника або відповідального виконавця наукової теми (проекту), або головного***

				редактора/члена редакційної колегії наукового видання, включеного до переліку наукових фахових видань України, або іноземного рецензованого наукового видання У 2013 – 2017 роках був виконавцем НДР «Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем в умовах впливу кібернетичних атак». Метою НДР є підвищення живучості ІКС в умовах впливу кібератак за рахунок протидії спробам порушення захисту таких систем та їх відновлення після злому. Основними завданнями НДР є: 1) аналіз стану живучості типових ІКС та розробка стратегій забезпечення живучості; 2) розробка моделей політики безпеки ІКС, здатних протистояти цілеспрямованим спробам порушення безпеки; 3) визначення типових архітектур та підходів до синтезу ІКС, що відповідають вимогам по забезпеченню живучості. З 2017 року й по цей час член редакційної колегії наукового видання, включеного до переліку наукових фахових видань України (іноземного рецензованого наукового видання) Problems of Infocommunications. Science and Technology (IEEE PIC S&T, **http://picst.org/).** ***30.10) Організаційна робота у закладах освіти на посадах керівника (заступника керівника) закладу освіти/інституту/ факультету/ відділення (наукової установи)/ філії/кафедри або іншого відповідального за підготовку здобувачів вищої освіти підрозділу/відділу (наукової установи)/навчально-методичного управління (відділу)/лабораторії/іншого навчально-наукового (інноваційного) структурного підрозділу/вченого секретаря закладу освіти (факультету, інституту)/відповідального секретаря приймальної комісії та його заступника*** З 1 вересня 2018 року по цей час – завідувач лабораторії «Безпеки інформаційних активів» кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка за внутрішнім сумісництвом ***30.13) Наявність виданих навчально-методичних посібників/посібників для самостійної роботи студентів та дистанційного навчання, конспектів лекцій/ практикумів/ методичних вказівок/рекомендацій загальною кількістю три найменування*** 1. Бурячок В.Л., Соколов В.Ю., Складанний П.М., Корченко А.О., Казмірчук С.В. Методичні рекомендації до виконання дипломних робіт освітнього рівня «Бакалавр» студентів спеціальності 125 «Кібернетична безпека». [Методичні рекомендації]. К.: ДУТ, 2016. 87 с. 2. Taj Dini M., Соколов В.Ю., Бурячок В.Л. Wireless & mobile security [Лабораторний практикум]. К.: ДУТ, 2017. 124 с. 3. Бурячок В.Л., Соколов В.Ю. Ініціатива CDIO. Версія 2.1 [Методичні рекомендації]. К.: КУБГ, 2019. 34 с. ***30.16) Участь у професійних об'єднаннях за спеціальністю*** Член міжнародного товариства European Microwave Association (EuMA). Member ID – AM3743. Режим доступу: **http://www.eumwa.org/**. Член Міжнародного союзу електрозв'язку (ITU). Member ID – 1200190674. Режим доступу: **https://www.itu.int**. Член міжнародного товариства Center for Internet Security (CIS). Режим доступу: **https://www.cisecurity.org/**. Член міжнародного товариства Internet Society (IS). Member ID – 175645. Режим доступу: **http://www.cybersecuritysig.org**. Член міжнародного товариства Malware Information Sharing Platform (MISP). Member ID – 1607. Режим доступу: **https://www.misp-project.org/**. ***30.17) Досвід практичної роботи за спеціальністю не менше п'яти років*** Досвід практичної діяльності за напрямками створення й впровадження систем технічного захисту інформації на об'єктах інформаційної діяльності та забезпечення безпеки безпроводових інформаційно-комунікаційних систем в органах виконавчої влади – 20 років. Протягом 2004-2019 років відповідні роботи проводились спільно з АТЗТ «Датекс Україна» (м. Київ), ТОВ «Мобільні торгівельні платіжні системи» (м. Київ), ТОВ «Э-Ком» (м. Київ), ДП «Компания «ATLAS» (м. Київ), ТОВ «Торгівельний дім «Система» (м. Київ) і ТОВ «Хелсі» (м. Київ).

Таблиця 3. Матриця відповідності

Організація науки і наукових досліджень

Програмні результати навчання	Методи навчання	Форми оцінювання
Вміти застосовувати знання іноземних мов для забезпечення ефективності професійної комунікації. Вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати теорії, принципи, методи і поняття у навчанні та професійній діяльності. Вміти представляти отримані знання та навички з теорії та практики ІКБ в усній та/або письмових формах перед фаховою і нефаховою аудиторією.	самостійна робота	
Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки. Вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні технології. Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях. Знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж. Вміти проектувати захищені (з урахуванням загроз) проводові телекомунікаційні системи. Знати методи організації захищеної передачі даних у незахищеному середовищі.	наочні (ілюстрація через презентацію), лабораторні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку

Іноземна мова професійного спрямування

Програмні результати навчання	Методи навчання	Форми оцінювання
Вміти застосовувати знання іноземних мов для забезпечення ефективності професійної комунікації. Вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати теорії, принципи, методи і поняття у навчанні та професійній діяльності. Вміти представляти отримані знання та навички з теорії та практики ІКБ в усній та/або письмових формах перед фаховою і нефаховою аудиторією.	наочні (ілюстрація через презентацію), практичні роботи, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді заліку

Прикладна загальна теорія систем безпеки

Програмні результати навчання	Методи навчання	Форми оцінювання
Вміти застосовувати знання іноземних мов для забезпечення ефективності професійної комунікації. Вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати теорії, принципи, методи і поняття у навчанні та професійній діяльності. Вміти представляти отримані знання та навички з теорії та практики ІКБ в усній та/або письмових формах перед фаховою і нефаховою аудиторією.	самостійна робота	
Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки. Вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні технології. Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях. Знати способи боротьби з даними уразливостями, а також спеціалізоване	наочні (ілюстрація через презентацію), лабораторні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку

Програмні результати навчання	Методи навчання	Форми оцінювання
мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж. Вміти проектувати захищені (з урахуванням загроз) проводові телекомунікаційні системи. Знати методи організації захищеної передачі даних у незахищеному середовищі.		

Моніторинг, аудит та адміністрування захищених IT систем і мереж

Програмні результати навчання	Методи навчання	Форми оцінювання
Володіти практичними навичками проведення аудиту безпеки ІКС, адміністрування та експлуатації. Вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, семінарські заняття, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді заліку, підсумковий семестровий контроль у виді іспиту

Технології безпеки мережевої та SMART інфраструктури

Програмні результати навчання	Методи навчання	Форми оцінювання
Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки. Вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні технології. Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях. Знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж. Вміти проектувати захищені (з урахуванням загроз) проводові телекомунікаційні системи. Знати методи організації захищеної передачі даних у незахищеному середовищі.	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, лабораторні роботи, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді курсової роботи, підсумковий семестровий контроль у виді іспиту
Знати уразливості й методи їх застосування в безпроводових і мобільних мережах. Вміти виявляти загрози проникнення або доступу зловмисників до таких мереж. Знати спеціалізоване обладнання для забезпечення безпеки безпроводових і мобільних мереж. Вміти проектувати захищені (з урахуванням загроз) безпроводові мережі;	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, лабораторні роботи, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді курсової роботи, підсумковий семестровий контроль у виді іспиту
Знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки. Вміти знаходити шляхи для їх усунення.	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, лабораторні роботи, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді курсової роботи, підсумковий семестровий контроль у виді іспиту

Технології безпеки мережевої та SMART інфраструктури

Програмні результати навчання	Методи навчання	Форми оцінювання
Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки. Вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні технології. Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях. Знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж. Вміти проектувати захищені (з урахуванням загроз) проводові телекомунікаційні системи. Знати методи організації захищеної передачі даних у незахищеному середовищі.	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, лабораторні роботи, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді курсової роботи, підсумковий семестровий контроль у виді іспиту
Знати уразливості й методи їх застосування в безпроводових і мобільних мережах. Вміти виявляти загрози проникнення або доступу зловмисників до таких мереж. Знати спеціалізоване обладнання для забезпечення безпеки безпроводових і мобільних мереж. Вміти проектувати захищені (з урахуванням загроз) безпроводові мережі;	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, лабораторні роботи, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді курсової роботи, підсумковий семестровий контроль у виді іспиту
Знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки. Вміти знаходити шляхи для їх усунення.	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, лабораторні роботи, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді курсової роботи, підсумковий семестровий контроль у виді іспиту

Технології безпеки безпроводових і мобільних мереж

Програмні результати навчання	Методи навчання	Форми оцінювання
Знати уразливості й методи їх застосування в безпроводових і мобільних мережах. Вміти виявляти загрози проникнення або доступу зловмисників до таких мереж. Знати спеціалізоване обладнання для забезпечення безпеки безпроводових і мобільних мереж. Вміти проектувати захищені (з урахуванням загроз) безпроводові мережі;	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, семінарські заняття, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді заліку

Технології розслідування інцидентів безпеки

Програмні результати навчання	Методи навчання	Форми оцінювання
Вміти організовувати процеси розслідування інцидентів у відповідності зі стандартами ISO 27001, ISO 20000, ISO 27035, ISO	словесні (лекція), наочні (ілюстрація через презентацію),	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті,

Програмні результати навчання	Методи навчання	Форми оцінювання
27037, ISO 27031, ISO/IEC TR 18044, NIST SP 800-61, CMU/SEI-2004-TR-015.	практичні роботи, семінарські заняття, самостійна робота	тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді заліку
Володіти практичними навичками проведення аудиту безпеки ІКС, адміністрування та експлуатації. Вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, семінарські заняття, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді заліку

Прикладні аспекти тестувань на проникнення та етичного хакінгу

Програмні результати навчання	Методи навчання	Форми оцінювання
Знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, брандмауери, сніфери, сканери портів).	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, семінарські заняття, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді заліку, підсумковий семестровий контроль у виді іспиту
Вміти проводити семантичний аналіз файлів. Вміти виявляти злоякісне ПЗ й файли за їх структурою та поведінкою. Вміти відновлювати пошкоджену інформацію. Вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ.	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, семінарські заняття, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді заліку, підсумковий семестровий контроль у виді іспиту
Володіти практичними навичками проведення аудиту безпеки ІКС, адміністрування та експлуатації. Вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, семінарські заняття, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді заліку, підсумковий семестровий контроль у виді іспиту

Технології безпеки Web-ресурсів

Програмні результати навчання	Методи навчання	Форми оцінювання
Знати існуючі уразливості веб-ресурсів (SQL-ін’єкції, брутфорс, XSS і т. ін.) та способи боротьби з ними на етапі розробки та в процесі експлуатації. Знати шаблони проектування безпечних веб-додатків.	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, семінарські заняття, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді заліку

Технології протидії злоякісному програмному коду

Програмні результати навчання	Методи навчання	Форми оцінювання

Програмні результати навчання	Методи навчання	Форми оцінювання
Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки. Вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні технології. Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях. Знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж. Вміти проектувати захищені (з урахуванням загроз) проводові телекомунікаційні системи. Знати методи організації захищеної передачі даних у незахищеному середовищі.	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, семінарські заняття, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо, проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді іспиту
Знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, брандмауери, сніфери, сканери портів).	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, семінарські заняття, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо, проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді іспиту
Вміти проводити семантичний аналіз файлів. Вміти виявляти злоякісне ПЗ й файли за їх структурою та поведінкою. Вміти відновлювати пошкоджену інформацію. Вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ.	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, семінарські заняття, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо, проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді іспиту

Технології розробки і тестування ПЗ мережевої безпеки

Програмні результати навчання	Методи навчання	Форми оцінювання
Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки. Вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні технології. Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях. Знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж. Вміти проектувати захищені (з урахуванням загроз) проводові телекомунікаційні системи. Знати методи організації захищеної передачі даних у незахищеному середовищі.	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, семінарські заняття, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо, проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді іспиту
Знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, брандмауери, сніфери, сканери портів).	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, семінарські заняття,	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо, проміжний контроль у виді модульного колоквіуму, тестування, тощо,

Програмні результати навчання	Методи навчання	Форми оцінювання
	самостійна робота	підсумковий семестровий контроль у виді іспиту

Математичні методи криптографії

Програмні результати навчання	Методи навчання	Форми оцінювання
Володіти практичними навичками проведення аудиту безпеки ІКС, адміністрування та експлуатації. Вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді заліку

Методи побудови і аналізу криптосистем

Програмні результати навчання	Методи навчання	Форми оцінювання
Володіти практичними навичками проведення аудиту безпеки ІКС, адміністрування та експлуатації. Вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.	словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, самостійна робота	вхідний контроль (усне/письмове опитування, індивідуальне опитування, виступ студента на занятті, тощо), проміжний контроль у виді модульного колоквіуму, тестування, тощо, підсумковий семестровий контроль у виді заліку

Виробнича (технологічна) практика

Програмні результати навчання	Методи навчання	Форми оцінювання
Вміти застосовувати знання іноземних мов для забезпечення ефективності професійної комунікації. Вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати теорії, принципи, методи і поняття у навчанні та професійній діяльності. Вміти представляти отримані знання та навички з теорії та практики ІКБ в усній та/або письмових формах перед фаховою і нефаховою аудиторією.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки. Вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні технології. Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях. Знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж. Вміти проектувати захищені (з урахуванням загроз) проводові телекомунікаційні системи. Знати методи організації захищеної передачі даних у незахищеному середовищі.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Знати уразливості й методи їх застосування в безпроводових і мобільних мережах. Вміти виявляти загрози проникнення або доступу зловмисників до таких мереж. Знати спеціалізоване обладнання для забезпечення безпеки безпроводових і мобільних мереж. Вміти проектувати захищені (з урахуванням загроз) безпроводові мережі;	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, брандмауери, сніфери, сканери портів).	практичні роботи, самостійна	підсумковий семестровий контроль

Програмні результати навчання	Методи навчання	Форми оцінювання
	робота	у виді заліку
Вміти проводити семантичний аналіз файлів. Вміти виявляти злоякісне ПЗ й файли за їх структурою та поведінкою. Вміти відновлювати пошкоджену інформацію. Вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Знати існуючі уразливості веб-ресурсів (SQL-ін'єкції, брутфорс, XSS і т. ін.) та способи боротьби з ними на етапі розробки та в процесі експлуатації. Знати шаблони проектування безпечних веб-додатків.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки. Вміти знаходити шляхи для їх усунення.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Вміти організовувати процеси розслідування інцидентів у відповідності зі стандартами ISO 27001, ISO 20000, ISO 27035, ISO 27037, ISO 27031, ISO/IEC TR 18044, NIST SP 800-61, CMU/SEI-2004-TR-015.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Володіти практичними навичками проведення аудиту безпеки ІКС, адміністрування та експлуатації. Вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку

Науково-дослідна практика

Програмні результати навчання	Методи навчання	Форми оцінювання
Вміти застосовувати знання іноземних мов для забезпечення ефективності професійної комунікації. Вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати теорії, принципи, методи і поняття у навчанні та професійній діяльності. Вміти представляти отримані знання та навички з теорії та практики ІКБ в усній та/або письмових формах перед фаховою і нефаховою аудиторією.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки. Вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні технології. Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях. Знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж. Вміти проектувати захищені (з урахуванням загроз) проводові телекомунікаційні системи. Знати методи організації захищеної передачі даних у незахищеному середовищі.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Знати уразливості й методи їх застосування в безпроводових і мобільних мережах. Вміти виявляти загрози проникнення або доступу зловмисників до таких мереж. Знати спеціалізоване обладнання для забезпечення безпеки безпроводових і мобільних мереж. Вміти проектувати захищені (з урахуванням загроз) безпроводові мережі;	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, брандмауери, сніфери, сканери портів).	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Вміти проводити семантичний аналіз файлів. Вміти виявляти злоякісне ПЗ й файли за їх структурою та поведінкою.	практичні роботи,	підсумковий

Програмні результати навчання	Методи навчання	Форми оцінювання
Вміти відновлювати пошкоджену інформацію. Вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ.	самостійна робота	семестровий контроль у виді заліку
Знати існуючі уразливості веб-ресурсів (SQL-ін’єкції, брутфорс, XSS і т. ін.) та способи боротьби з ними на етапі розробки та в процесі експлуатації. Знати шаблони проектування безпечних веб-додатків.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки. Вміти знаходити шляхи для їх усунення.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Вміти організовувати процеси розслідування інцидентів у відповідності зі стандартами ISO 27001, ISO 20000, ISO 27035, ISO 27037, ISO 27031, ISO/IEC TR 18044, NIST SP 800-61, CMU/SEI-2004-TR-015.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Володіти практичними навичками проведення аудиту безпеки ІКС, адміністрування та експлуатації. Вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку

Переддипломна практика

Програмні результати навчання	Методи навчання	Форми оцінювання
Вміти застосовувати знання іноземних мов для забезпечення ефективності професійної комунікації. Вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати теорії, принципи, методи і поняття у навчанні та професійній діяльності. Вміти представляти отримані знання та навички з теорії та практики ІКБ в усній та/або письмових формах перед фаховою і нефаховою аудиторією.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки. Вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні технології. Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях. Знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж. Вміти проектувати захищені (з урахуванням загроз) проводові телекомунікаційні системи. Знати методи організації захищеної передачі даних у незахищеному середовищі.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Знати уразливості й методи їх застосування в безпроводових і мобільних мережах. Вміти виявляти загрози проникнення або доступу зловмисників до таких мереж. Знати спеціалізоване обладнання для забезпечення безпеки безпроводових і мобільних мереж. Вміти проектувати захищені (з урахуванням загроз) безпроводові мережі;	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, брандмауери, сніфери, сканери портів).	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Вміти проводити семантичний аналіз файлів. Вміти виявляти злоякісне ПЗ й файли за їх структурою та поведінкою. Вміти відновлювати пошкоджену інформацію. Вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку

Програмні результати навчання	Методи навчання	Форми оцінювання
Знати існуючі уразливості веб-ресурсів (SQL-ін’єкції, брутфорс, XSS і т. ін.) та способи боротьби з ними на етапі розробки та в процесі експлуатації. Знати шаблони проектування безпечних веб-додатків.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки. Вміти знаходити шляхи для їх усунення.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Вміти організовувати процеси розслідування інцидентів у відповідності зі стандартами ISO 27001, ISO 20000, ISO 27035, ISO 27037, ISO 27031, ISO/IEC TR 18044, NIST SP 800-61, CMU/SEI-2004-TR-015.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку
Володіти практичними навичками проведення аудиту безпеки ІКС, адміністрування та експлуатації. Вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.	практичні роботи, самостійна робота	підсумковий семестровий контроль у виді заліку

Підготовка кваліфікаційної магістерської роботи

Програмні результати навчання	Методи навчання	Форми оцінювання
Вміти застосовувати знання іноземних мов для забезпечення ефективності професійної комунікації. Вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати теорії, принципи, методи і поняття у навчанні та професійній діяльності. Вміти представляти отримані знання та навички з теорії та практики ІКБ в усній та/або письмових формах перед фаховою і нефаховою аудиторією.		підсумкова випускна атестація у виді магістерської роботи
Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки. Вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні технології. Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях. Знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж. Вміти проектувати захищені (з урахуванням загроз) проводові телекомунікаційні системи. Знати методи організації захищеної передачі даних у незахищеному середовищі.		підсумкова випускна атестація у виді магістерської роботи
Знати уразливості й методи їх застосування в безпроводових і мобільних мережах. Вміти виявляти загрози проникнення або доступу зловмисників до таких мереж. Знати спеціалізоване обладнання для забезпечення безпеки безпроводових і мобільних мереж. Вміти проектувати захищені (з урахуванням загроз) безпроводові мережі;		підсумкова випускна атестація у виді магістерської роботи
Знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, брандмауери, сніфери, сканери портів).		підсумкова випускна атестація у виді магістерської роботи
Вміти проводити семантичний аналіз файлів. Вміти виявляти злоякісне ПЗ й файли за їх структурою та поведінкою. Вміти відновлювати пошкоджену інформацію. Вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ.		підсумкова випускна атестація у виді магістерської роботи
Знати існуючі уразливості веб-ресурсів (SQL-ін’єкції, брутфорс, XSS і т. ін.) та способи боротьби з ними на етапі		підсумкова випускна

Програмні результати навчання	Методи навчання	Форми оцінювання
розробки та в процесі експлуатації. Знати шаблони проектування безпечних веб-додатків.		атестація у виді магістерської роботи
Знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки. Вміти знаходити шляхи для їх усунення.		підсумкова випускна атестація у виді магістерської роботи
Вміти організовувати процеси розслідування інцидентів у відповідності зі стандартами ISO 27001, ISO 20000, ISO 27035, ISO 27037, ISO 27031, ISO/IEC TR 18044, NIST SP 800-61, CMU/SEI-2004-TR-015.		підсумкова випускна атестація у виді магістерської роботи
Володіти практичними навичками проведення аудиту безпеки ІКС, адміністрування та експлуатації. Вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.		підсумкова випускна атестація у виді магістерської роботи

Захист кваліфікаційної магістерської роботи

Програмні результати навчання	Методи навчання	Форми оцінювання
Вміти застосовувати знання іноземних мов для забезпечення ефективності професійної комунікації. Вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати теорії, принципи, методи і поняття у навчанні та професійній діяльності. Вміти представляти отримані знання та навички з теорії та практики ІКБ в усній та/або письмових формах перед фаховою і нефаховою аудиторією.		підсумкова випускна атестація у виді магістерської роботи
Вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки. Вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні технології. Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях. Знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж. Вміти проектувати захищені (з урахуванням загроз) проводові телекомунікаційні системи. Знати методи організації захищеної передачі даних у незахищеному середовищі.		підсумкова випускна атестація у виді магістерської роботи
Знати уразливості й методи їх застосування в безпроводових і мобільних мережах. Вміти виявляти загрози проникнення або доступу зловмисників до таких мереж. Знати спеціалізоване обладнання для забезпечення безпеки безпроводових і мобільних мереж. Вміти проектувати захищені (з урахуванням загроз) безпроводові мережі;		підсумкова випускна атестація у виді магістерської роботи
Знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, брандмауери, сніфери, сканери портів).		підсумкова випускна атестація у виді магістерської роботи
Вміти проводити семантичний аналіз файлів. Вміти виявляти злоякісне ПЗ й файли за їх структурою та поведінкою. Вміти відновлювати пошкоджену інформацію. Вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ.		підсумкова випускна атестація у виді магістерської роботи
Знати існуючі уразливості веб-ресурсів (SQL-ін’єкції, брутфорс, XSS і т. ін.) та способи боротьби з ними на етапі		підсумкова випускна

Програмні результати навчання	Методи навчання	Форми оцінювання
розробки та в процесі експлуатації. Знати шаблони проектування безпечних веб-додатків.		атестація у виді магістерської роботи
Знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки. Вміти знаходити шляхи для їх усунення.		підсумкова випускна атестація у виді магістерської роботи
Вміти організовувати процеси розслідування інцидентів у відповідності зі стандартами ISO 27001, ISO 20000, ISO 27035, ISO 27037, ISO 27031, ISO/IEC TR 18044, NIST SP 800-61, CMU/SEI-2004-TR-015.		підсумкова випускна атестація у виді магістерської роботи
Володіти практичними навичками проведення аудиту безпеки ІКС, адміністрування та експлуатації. Вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.		підсумкова випускна атестація у виді магістерської роботи

Таблиця 4. Загальна інформація про Київський університет імені Бориса Грінченка

1.	**Кількість ліцензованих спеціальностей**	
	за 1 (бакалаврським) рівнем	26
	за 2 (магістерським) рівнем	25
	за 3 (освітньо-науковим/освітньо-творчим) рівнем	13
2.	**Кількість акредитованих освітніх програм**	
	за 1 (бакалаврським) рівнем	0
	за 2 (магістерським) рівнем	34
	за 3 (освітньо-науковим/освітньо-творчим) рівнем	0
3.	**Контингент студентів на всіх курсах навчання**	8782
	на денній формі навчання	7022 *(з них 1173 - студенти Університетського коледжу)*
	на інших формах навчання (заочна, дистанційна)	1760 *(заочна форма навчання)*
4.	Кількість факультетів	9
5.	Кількість кафедр	39
6.	**Кількість співробітників (всього)**	1029

	* в т.ч. педагогічних	162
	Серед них: - докторів наук, професорів	108
	- кандидатів наук, доцентів	393
7.	**Загальна/навчальна площа будівель (кв.м)**	42916,6/41323,3 *(без врахування площі гуртожитків)*
	Серед них: - власні приміщення (кв.м)	41745,3/40152
	- орендовані (кв.м)	1171,3 *(навчальні площі)*
	- здані в оренду (кв.м)	114,7
8.	**Наявність бібліотеки (в т.ч. кількість місць у читальному залі)**	Так /(203 місця, з них 47 комп'ютеризованих)
9.	**Кількість гуртожитків**	3 *(загальна площа - 7743,74 кв.м);* *з них 1 орендований (1821,2 кв.м)*
	Кількість місць для проживання студентів	861