



НАЦІОНАЛЬНЕ
АГЕНТСТВО
ІЗ ЗАБЕЗПЕЧЕННЯ
ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

| | |
|---------------------|---|
| Заклад вищої освіти | Київський університет імені Бориса Грінченка |
| Освітня програма | 46235 Інформаційна безпека держави |
| Рівень вищої освіти | Доктор філософії |
| Спеціальність | 125 Кібербезпека |

Відомості про самооцінювання є частиною акредитаційної справи, поданої до Національного агентства із забезпечення якості вищої освіти для акредитації зазначеної вище освітньої програми. Відповідальність за підготовку і зміст відомостей несе заклад вищої освіти, який подає програму на акредитацію.

Детальніше про мету і порядок проведення акредитації можна дізнатися на вебсайті Національного агентства – <https://naqa.gov.ua/>

Використані скорочення:

| | |
|--------------|--|
| ID | ідентифікатор |
| ВСП | відокремлений структурний підрозділ |
| ЄДЕБО | Єдина державна електронна база з питань освіти |
| ЄКТС | Європейська кредитна трансферно-накопичувальна система |
| ЗВО | заклад вищої освіти |
| ОП | освітня програма |

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

| | |
|-------------------------------------|--|
| Реєстраційний номер ЗВО у ЄДЕБО | 56 |
| Повна назва ЗВО | Київський університет імені Бориса Грінченка |
| Ідентифікаційний код ЗВО | 02136554 |
| ПІБ керівника ЗВО | Турунцев Олександр Петрович |
| Посилання на офіційний веб-сайт ЗВО | http://kubg.edu.ua/ |

2. Посилання на інформацію про ЗВО (ВСП ЗВО) у Реєстрі суб'єктів освітньої діяльності ЄДЕБО

<https://registry.edbo.gov.ua/university/56>

3. Загальна інформація про ОП, яка подається на акредитацію

| | |
|---|---|
| ID освітньої програми в ЄДЕБО | 46235 |
| Назва ОП | Інформаційна безпека держави |
| Галузь знань | 12 Інформаційні технології |
| Спеціальність | 125 Кібербезпека |
| Спеціалізація (за наявності) | <i>відсутня</i> |
| Рівень вищої освіти | Доктор філософії |
| Тип освітньої програми | Освітньо-наукова |
| Вступ на освітню програму здійснюється на основі ступеня (рівня) | Магістр (ОКР «спеціаліст») |
| Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП | Кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики |
| Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП | Факультет суспільно-гуманітарних наук: кафедра філософії та релігієзнавства; Факультет романо-германської філології: кафедра лінгвістики та перекладу; Факультет педагогічної освіти: кафедра освітології та психолого-педагогічних наук; Факультет права та міжнародних відносин: кафедра міжнародних відносин, кафедра публічного права; Факультет психології, соціальної роботи та спеціальної освіти: кафедра психології особистості та соціальних практик |
| Місце (адреса) провадження освітньої діяльності за ОП | м. Київ, вул. Левка Лук'яненка, 13б |
| Освітня програма передбачає присвоєння професійної кваліфікації | <i>не передбачає</i> |
| Професійна кваліфікація, яка присвоюється за ОП (за наявності) | <i>відсутня</i> |
| Мова (мови) викладання | Українська |
| ID гаранта ОП у ЄДЕБО | 315458 |
| ПІБ гаранта ОП | Коршун Наталія Володимирівна |
| Посада гаранта ОП | Професор |
| Корпоративна електронна адреса гаранта ОП | n.korshun@kubg.edu.ua |
| Контактний телефон гаранта ОП | +38(093)-603-90-64 |
| Додатковий телефон гаранта ОП | +38(050)-385-25-52 |

| Форми здобуття освіти на ОП | Термін навчання |
|-----------------------------|-----------------|
| заочна | 4 р. 0 міс. |
| очна денна | 4 р. 0 міс. |

4. Загальні відомості про ОП, історію її розроблення та впровадження

ОП «Інформаційна безпека держави» (далі – ОП) підготовки на третьому рівні вищої освіти за спеціальністю 125 Кібербезпека у Київському університеті імені Бориса Грінченка (далі – Університет) розроблена відповідно до Закону України «Про вищу освіту», Порядку підготовки здобувачів вищої ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого Постановою Кабінету Міністрів України від 23.03.2016 року №261.

ОП було розроблено робочою групою у складі провідних вчених Університету: гаранта, д.т.н., проф. Бурячка В.Л., д.т.н., проф. Бессалова А.В., д.т.н., доц. Семка В.В., к.військ.н., доц. Аносова А.О. у 2019 р. Рецензентами виступили Толюпа С.В., д.т.н., проф., проф. кафедри кібербезпеки та захисту інформації Київського національного університету ім. Т.Г. Шевченка та Ермошин В.В., к.т.н., директор Департаменту з інформаційної безпеки ДП «НЕК «Укренерго». ОП затверджена Вченою радою Університету (від 24.01.2019, протокол №1) та введена в дію наказом від 29.01.2019 №37. Зміни до ОП, такі як уточнення рівня відповідності НРК в описі ОП та перерозподіл кредитів між освітніми компонентами для посилення практичної підготовки здобувачів до викладацької діяльності затверджено рішенням вченої ради Факультету інформаційних технологій та управління від 16.09.2020 (протокол №7) та введено в дію наказом від 24.09.2020 №539.

У 2022 р. внаслідок аналізу чинників, виявлених у процесі реалізації ОП, результатів проведених опитувань та відгуків стейкхолдерів робочою групою НПП у складі: гаранта, д.т.н., проф. Коршун Н.В., д.т.н., проф., Бессалова А.В., к.т.н., доц. Козачка В.А., д.ф.-м.н., проф., завідувача відділу інформаційної безпеки Інституту телекомунікацій і глобального інформаційного простору НАН України Устименка В.О., аспіранта ОП «Інформаційна безпека держави» Ворохоба М.В. було розроблено нову редакцію ОП (затверджено Вченою радою Університету від 04.04.2022, протокол №2, введено в дію наказом від 05.04.2022 №146). До процесу було долучено адміністративний склад Університету, академічну спільноту та роботодавців за фахом. В новій редакції уточнено загальну інформацію про ОП та назви окремих ОК, оптимізовано їх структуру відповідно до сучасного стану галузі і спеціальності, перерозподілено кредити між освітніми компонентами для посилення теоретико-методологічної складової викладацької діяльності. Рецензентами ОП виступили провідні фахівці сфери кібербезпеки Лукова-Чуйко Н.В., д.т.н., проф., завідувач кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, Опірський І.Р., д.т.н., проф., професор кафедри захисту інформації Національного університету «Львівська політехніка». ОП отримала схвальні рецензії та відгук від представника роботодавців Бегуна В.В., д.т.н., доц., зав. відділу «Інтегровані автоматизовані системи спеціального призначення» Інституту проблем математичних машин і систем НАН України.

5. Інформація про контингент здобувачів вищої освіти на ОП станом на 1 жовтня поточного навчального року у розрізі форм здобуття освіти та набір на ОП (кількість здобувачів, зарахованих на навчання у відповідному навчальному році сумарно за усіма формами здобуття освіти)

| Рік навчання | Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання | Обсяг набору на ОП у відповідному навчальному році | Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року | | У тому числі іноземців | |
|--------------|--|--|--|---|------------------------|---|
| | | | ОД | З | ОД | З |
| 1 курс | 2022 - 2023 | 5 | 4 | 1 | 0 | 0 |
| 2 курс | 2021 - 2022 | 3 | 2 | 1 | 0 | 0 |
| 3 курс | 2020 - 2021 | 3 | 2 | 1 | 0 | 0 |
| 4 курс | 2019 - 2020 | 3 | 1 | 2 | 0 | 0 |

Умовні позначення: ОД – очна денна; ОВ – очна вечірня; З – заочна; Дс – дистанційна; М – мережева; Дл – дуальна.

6. Інформація про інші ОП ЗВО за відповідною спеціальністю

| Рівень вищої освіти | Інформація про освітні програми |
|--|--|
| початковий рівень (короткий цикл) | програми відсутні |
| перший (бакалаврський) рівень | 26188 Безпека інформаційних і комунікаційних систем |
| другий (магістерський) рівень | 26192 Безпека інформаційних і комунікаційних систем |
| третій (освітньо-науковий/освітньо-творчий) рівень | 36858 Кібербезпека 46235 Інформаційна безпека держави |

7. Інформація про площі приміщень ЗВО станом на момент подання відомостей про самооцінювання, кв. м.

| | Загальна площа | Навчальна площа |
|---|----------------|-----------------|
| Усі приміщення ЗВО | 42917 | 41323 |
| Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління) | 41745 | 40152 |
| Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо) | 1171 | 1171 |
| Приміщення, здані в оренду | 115 | 0 |

Примітка. Для ЗВО із ВСП інформація зазначається:

- щодо ОП, яка реалізується у базовому ЗВО – без урахування приміщень ВСП;
- щодо ОП, яка реалізується у ВСП – лише щодо приміщень даного ВСП.

8. Документи щодо ОП

| Документ | Назва файла | Хеш файла |
|----------------------------------|-------------------------------|--|
| Освітня програма | <i>ONP_125_2019.pdf</i> | rBNNLLoAawiBJnTMu3YVzKS2CSRUiOezVTvm09qBUqY= |
| Освітня програма | <i>ONP_ZMINY_125_2020.pdf</i> | PWhN+7gmv2GvJ878sQH4OushiwIYmXUZ94G4Y/wvn7w= |
| Освітня програма | <i>ONP_125_2022.pdf</i> | iPZcwm1vArSjJp+ltiiDP2KGXfcl2FrHBaFeK72ZDV4= |
| Навчальний план за ОП | <i>NP_125_2019.pdf</i> | o3DJLh/XtSzTVDRoqgN1zHi3ifalCmlSm7JvzBvy9GY= |
| Навчальний план за ОП | <i>125_NP_zminy_2020.pdf</i> | I3vAfVO/gS1qonP9rU5w1/CADRHFIMS/Z2u1wnAeEDM= |
| Навчальний план за ОП | <i>NP_125_2022.pdf</i> | HyENhWrAEGNUOojP9L7NHApzAPTPF9OsAQSGzPREyBs= |
| Рецензії та відгуки роботодавців | <i>125_rec.pdf</i> | KV8I9zmBk3zzeapbfSmODMGvabwWHDbY2X8eDdrUtPE= |
| Рецензії та відгуки роботодавців | <i>125_rec_2022.pdf</i> | GEsO5Dq84dBQJoY5BqUF4/6goxZhtaSUh4EmSVmqReM= |

1. Проектування та цілі освітньої програми

Якими є цілі ОП? У чому полягають особливості (унікальність) цієї програми?

Мета ОНП – забезпечити сучасну освітньо-наукову підготовку дослідників з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека із глибинним науковим, аналітичним, дослідницьким, організаторським потенціалом задля успішної професійної самореалізації та здійснення наукових проєктів відповідно до місії Університету – «Служити людині, громаді, суспільству».

Цілями ОНП є підготовка фахівців з кібербезпеки, здатних продукувати нові ідеї, розв'язувати комплексні проблеми у професійній та дослідницько-інноваційній діяльності, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.

Унікальність цієї програми полягає в тому, що:

при розробці ОНП проєктною групою було враховано стандарти вищої освіти підготовки бакалаврів і магістрів спеціальності 125 Кібербезпека, Стратегію розвитку Університету, результати прогнозу трансформації компетентностей компанії World Economic Forum, міжнародні стандарти NIST, а також рекомендації міжнародної ініціативи CDIO;

реалізується принцип поліаспектної інтеграції змісту освітньої підготовки (інтеграції ОК);

поєднано наукові інтереси здобувача з місією Університету й актуальними запитами суспільства; синергійному розвитку компетентностей здобувача.

Особливість ОНП полягає в її спрямуванні на потреби суспільства та держави, передусім – м. Києва та київського регіону щодо фахівців у сфері кібербезпеки.

Продемонструйте, із посиланням на конкретні документи ЗВО, що цілі ОП відповідають місії та

стратегії ЗВО

Відповідність цілей ОНП місії Університету Грінченка «Служити людині, громаді, суспільству»

(<https://tinyurl.com/kubg-statut>) на пряму відображено у формулюванні мети ОНП.

Створення ОНП «Інформаційна безпека держави» було передбачено п.5.3 Стратегії (Програми) розвитку Університету Грінченка на 2018-2022 рр. (<https://tinyurl.com/kubg-strat>).

Цілі ОНП у повній мірі відповідають Стратегії (Програми) розвитку Університету Грінченка на 2018-2022 рр., зокрема в контексті:

- реалізації покликання Університету Грінченка, яке передбачає сприяння особистісному та професійному розвитку успішної особистості шляхом удосконалення її природних здібностей, розкриття потенціалу та формування життєвих компетентностей;

- реалізації стратегічних цілей розвитку Університету на 2018-2022 рр., а саме забезпечення максимального сприяння розвитку здобувачів вищої освіти як свідомих і відповідальних громадян, цілісних та культурних особистостей, конкурентоспроможних професіоналів та лідерів.

Опишіть, яким чином інтереси та пропозиції таких груп заінтересованих сторін (стейкхолдерів) були враховані під час формулювання цілей та програмних результатів навчання ОП:

- здобувачі вищої освіти та випускники програми

При розробці ОНП 2019 р. ані здобувачів, ані випускників за спеціальністю 125 Кібербезпека в Університеті не було, члени проектної групи при формуванні цілей та РН враховували думку випускників інших ЗВО, а саме: Державного університету телекомунікацій, Нац. ун-ту «Львівська політехніка», Нац. авіаційного ун-ту, де ОНП третього (освітньо-наукового) рівня вищої освіти спеціальності 125 Кібербезпека функціонують протягом тривалого часу. При формулюванні цілей та РН було враховано також досвід реалізації ОНП Університету за іншими спеціальностями. В ході розробки нової редакції ОНП були враховані відгуки здобувачів, отримані при проведенні зустрічей та опитувань. Інтереси аспірантів в ОНП 2022 р. було враховано в меті та результатах навчання (РН 4,5,6,8). До складу робочої групи з розробки нової редакції ОНП увійшов аспірант третього р.н. Ворохоб М.В., який представляв інтереси аспірантів. Окрім того, враховуючи запити здобувачів, в Університеті постійно вдосконалюються умови для продукування аспірантами нових знань, ідей, їх імплементації у ЗВО і професійної самореалізації. Оскільки акредитація первинна, випускників цієї ОНП ще немає. У 2023 р. буде проведено опитування випускників. За результатами отриманих відгуків, кафедральних обговорень планується внесення уточнень до ОНП з урахуванням зворотного зв'язку з випускниками.

- роботодавці

На третьому рівні вищої освіти поняття «роботодавець» і «академічна спільнота» з об'єктивних причин тотожні. Першочерговий інтерес до якісної підготовки випускників ОНП, як потенційний роботодавець, проявляє Університет, саме тому на етапах розроблення та оновлення ОНП враховувалися інтереси та стратегічні цілі ун-ту як потенційного місця роботи випускників ОНП. Інтереси роботодавців враховані у контексті підготовки фахівців з розвинутими проф. компетентностями, які могли б демонструвати свої знання, уміння і навички, необхідні для здійснення фахової діяльності у сфері ІТ та ІКБ. З цією метою до формування ОНП було залучено представників роботодавців від ТОВ «АВТОР», НВК «Криптон», ДП «Укр. спеціальні системи», ДП «Держ. центр інформац. ресурсів», Департаменту Кіберполіції України тощо. В обговоренні нової редакції ОНП на засіданні кафедри взяли участь представники Ради роботодавців <http://surl.li/fxeru>. Зокрема, к.т.н., начальник департаменту інформац. безпеки НЕК «Укренерго» Ермошин В.В. вніс пропозиції до уточнення цілей навчання – розв'язувати комплексні проблеми у професійній та дослідницько-інноваційній діяльності; начальник відділу систем захисту інформації НВФ «КРИПТОН» Угрімов В.М. відзначив відповідність РН актуальним трендам сфери кібербезпеки та влучність фокусування уваги в ОНП на захисті ОІД. Відгук на ОНП надав досвідчений практик, д.т.н., доц., завідувач відділу «Інтегровані автоматизовані системи спец. призначення» ІПММС НАН України Бегун В.В.

- академічна спільнота

При формулюванні цілей, фахових компетентностей та РН були враховані Стратегія розвитку Університету, рекомендації академічної спільноти, насамперед фахівців у сфері захисту інформації, які працюють у провідних наукових установах, зокрема, ІПММС НАНУ, ІПС НАНУ, ІТГП НАНУ, а також Університету, НАУ, ХНУРЕ, ОНАЗ та Державного університету телекомунікацій, крім того, дослідників з наукових установ МО, СБУ, ГУР та ДССЗЗІ. Представником від академічної спільноти у робочій групі виступив Устименко В.О., д.ф.-м.н., проф., завідувач відділу інформаційної безпеки Інституту телекомунікацій і глобального інформаційного простору НАН України. При розробці ОНП враховувалися стратегічні цілі Університету як можливого роботодавця і представника академічної спільноти. Інтереси та пропозиції академічної спільноти були враховані при формулюванні цілей, компетентностей, ПРН ОНП та форм організації наукової роботи аспірантів.

Зокрема, НПП кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка було наголошено на академічній і прикладній важливості подальшого розвитку наукової школи <http://surl.li/fvsfe>, заснованої д.т.н., проф. В.Л. Бурячком, визнано актуальним здійснення спільних науково-практичних проєктів викладачів і аспірантів.

Зміст і формулювання освітніх компонентів ОНП було обговорено на засіданнях Вченої ради Факультету інформаційних технологій та управління та Вченої ради Університету.

- інші стейкхолдери

Іншими стейкхолдерами, з якими Університет Грінченка під час формулювання цілей та програмних результатів навчання ОНП здійснював співпрацю, виступили такі громадські організації, як Міжнародний центр протидії кіберзлочинності (NGO «ІССС»), Громадська рада при МО України та Український системний «ІТ.Integrator». За поданням представників від більшості зазначених вище стейкхолдерів до ОНП було додано вибіркові дисципліни.

Це дозволило конкретизувати результати навчання РН6 та РН7 й додати до них такі пункти: «забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф» та «володіти також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в ІТ системах та мережах» відповідно

Продемонструйте, яким чином цілі та програмні результати навчання ОП відбивають тенденції розвитку спеціальності та ринку праці

За результатами аналізу програмних документів, які було враховано при розробці ОНП, а також за цілями і РН, покладеними в її основу, програма відповідає:

тенденціям зростання наявних та потенційних викликів і загроз у сфері ІКБ в Україні й усьому світі; потребам ринку праці, згідно яких формуються запити щодо підготовки конкурентоспроможних фахівців сфери ІКБ для потреб освітніх, наукових і державних установ, структур спецпризначення, центрів і служб ЗІ підприємств та банківських установ різних форм власності, тощо.

У РН відображено такі тенденції розвитку спеціальності 125 Кібербезпека:

- необхідність забезпечення постійного моніторингу та аудиту ІКС для забезпечення ІКБ організацій шляхом встановлення актуальних програмних та програмно-апаратних засобів захисту (РН 4,5,7);

- готовність забезпечувати функціонування систем управління ІКБ з урахуванням інформаційних ризиків, конфліктів, катастроф (РН 6);

- інтернаціоналізація сфери кібербезпеки відображена у формулюванні РН 1-3, які передбачають володіння іноземною мовою та участі у міжнародних проектах;

- необхідність провадження в організаціях навчання персоналу з питань ІКБ, протидії шкідливому програмному забезпеченню та проявам соціальної інженерії (РН 8).

В результаті оволодіння ОНП фахівці зможуть визначати проблеми замовника, знаходити максимально ефективні варіанти їх рішення. Підтвердженням цьому є структурно-логічна схема навчання ОНП, що реалізується в НП та конкретизується в РПНД.

Продемонструйте, яким чином під час формулювання цілей та програмних результатів навчання ОП було враховано галузевий та регіональний контекст

Під час формулювання цілей та РН програми було враховано галузевий контекст у плані визначення загальних пріоритетів сфери ІКБ та ЗІ, бачення процесу підготовки та подальшої діяльності фахівців із ЗІ в ІТ системах і мережах та власне самих ІТСМ, які знають: методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у галузі інформаційної безпеки та/або кібербезпеки; технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі, а також проведення прикладних наукових досліджень та провадження викладацької діяльності у ЗВО та наукових установах.

Зважаючи на те, що Університет є ЗВО комунальної форми власності, підготовка здобувачів за ОНП дозволить суттєво вплинути на вирішення задач захисту інформації як в м. Києві, так і загалом у Київському регіоні (регіональний контекст). З цією ж метою Ун-ом укладено угоди із КП м. Києва «Київтелесервіс» та Департаментом ІКТ виконавчого органу КМДА.

Це дозволило здобувачам отримувати консультації у фахівців зазначених та ін. профільних підприємств, установ та організацій при вирішенні задач досліджень

Продемонструйте, яким чином під час формулювання цілей та програмних результатів навчання ОП було враховано досвід аналогічних вітчизняних та іноземних програм

Робочою групою ОНП був розглянутий та взятий до уваги досвід з підготовки з аналогічної спеціальності в інших ЗВО України, зокрема: КНУ ім. Тараса Шевченка, ХНУРЕ, НУУ «КПІ» ім. Сікорського, НУ «Львівська політехніка». Крім того, при розробці ОНП було проаналізовано зміст програм підготовки в галузі кібербезпеки таких іноземних програм, як University of Colorado (США), College of Engineering and Computing (США). ОНП є логічним продовженням «Магістерської програми підготовки нових експертів з кібербезпеки» (проект ENGENSEC TEMPUS IV №544455- TEMPUS-1-2013—1 SE-TEMPUS-JPCR <http://erasmusplus.org.ua/en/projects/tempus-iv/1013-educating-the-next-generation-experts-in-cybersecurity-the-new-eu-recognized-master-s-program.html>). Також в ОНП враховані міжнародні стандарти: National Science Education Standards, NRC & NAP та K-4 і 9-12 «Наука і дослідження. Розвиток умінь і знань студентів»; рекомендації міжнародної ініціативи CDIO Standard 2.1. Вивчення змісту та досвіду реалізації зазначених вище програм знайшло відображення у формулюванні мети ОНП та РН, зокрема, конкретизовано РН4 – обґрунтувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; доповнено РН 5 та РН6 – забезпечувати процес захисту ІКС шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; виконувати розробку експлуатаційної документації на КЗЗ відповідно.

Продемонструйте, яким чином ОП дозволяє досягти результатів навчання, визначених стандартом вищої освіти за відповідною спеціальністю та рівнем вищої освіти

Стандарт вищої освіти України за спеціальністю 125 Кібербезпека для третього (освітньо-наукового) рівня вищої освіти відсутній.

Якщо стандарт вищої освіти за відповідною спеціальністю та рівнем вищої освіти відсутній, поясніть, яким чином визначені ОП програмні результати навчання відповідають вимогам Національної рамки кваліфікацій для відповідного кваліфікаційного рівня?

Змістовне наповнення РН ОНП, що акредитується, відповідає вимогам восьмого рівня Національної рамки кваліфікацій <https://tinyurl.com/2jt8uw32> за такими дескрипторами:

– знання (концептуальні та методологічні знання в галузі чи на межі галузей знань або професійної діяльності) – РН 3,4,5,6,7;

– уміння (спеціалізовані уміння/навички і методи, необхідні для розв'язання значущих проблем у сфері професійної діяльності, науки та/або інновацій, розширення та переоцінки вже існуючих знань і професійної практики; започаткування, планування, реалізація та коригування послідовного процесу ґрунтовного наукового дослідження з дотриманням належної академічної доброчесності; критичний аналіз, оцінка і синтез нових та комплексних ідей) – РН 4,5,6,7;

– комунікація (вільне спілкування з питань, що стосуються сфери наукових та експертних знань, з колегами, широкою науковою спільнотою, суспільством в цілому; використання академічної української та іноземної мови у професійній діяльності та дослідженнях) – РН 1,2,3,8;

– відповідальність і автономність (демонстрація значної авторитетності, інноваційності, високий ступінь самостійності, академічна та професійна доброчесність, послідовна відданість розвитку нових ідей або процесів у передових контекстах професійної та наукової діяльності здатність до безперервного саморозвитку та самовдосконалення) – РН 1,2,3,4,6,8.

Таким чином, ОНП Інформаційна безпека держави повністю відповідає основним вимогам, які визначені в Національній рамці кваліфікацій.

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

60

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)?

0

Який обсяг (у кредитах ЄКТС) відводиться на дисципліни за вибором здобувачів вищої освіти?

18

Продемонструйте, що зміст ОП відповідає предметній області заявленої для неї спеціальності (спеціальностям, якщо освітня програма є міждисциплінарною)?

Відповідність ОНП предметній області спеціальності 125 Кібербезпека відображена в:

- об'єктах вивчення: об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту;

- цілях навчання, які полягають у підготовці фахівців з кібербезпеки, здатних продукувати нові ідеї, розв'язувати комплексні проблеми у професійній та дослідницько-інноваційній діяльності, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення;

Теоретичний зміст предметної області складають знання законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; теорії, моделей та принципів управління доступом до IP; теорії систем управління інформаційною та/або кібербезпекою; методів та засобів виявлення, управління та ідентифікації ризиків; методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; методів та засобів технічного та криптографічного захисту інформації; сучасних інформаційно-комунікаційних технологій; сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; автоматизованих систем проектування.

Практичну складову формують методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки; технології, методи та моделі дослідження, аналізу,

управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі.

Зміст ОНП сприяє формуванню значного обсягу загальних та спеціальних (фахових) компетентностей, які необхідні для проведення наукових досліджень, перелік вибіркового дисциплін дозволяє урахування дослідницьких інтересів здобувачів. Зміст ОНП чітко структуровано освітніми компонентами, що становлять взаємопідпорядковану систему, логічно пов'язану можливістю досягнення програмних результатів навчання.

Яким чином здобувачам вищої освіти забезпечена можливість формування індивідуальної освітньої траєкторії?

У Положенні про організацію освітнього процесу (п.7.2) закріплено право здобувачів на участь у формуванні інд. навч. плану, що втілює інд. освітню траєкторію. Це право підтверджено пріоритетами Стратегії розвитку Ун-ту на 2018-2022 рр. (п.3.2) та 2023-2027 рр. (р.6), Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу Ун-ту (Р.IV).

Особливістю ОНП з підготовки доктора філософії є більша вмотивованість здобувачів та індивідуалізація їхніх наукових інтересів, яким багато в чому підпорядковується зміст освіти. Положенням про підготовку здобувачів вищої освіти доктора філософії в Ун-ті (п.4.2) передбачено формування на основі ОНП інд. навч. плану та плану наукової роботи, які погоджуються з науковим керівником і затверджуються вченою радою Факультету. Відповідно до Положення аспіранти можуть формувати інд. освітню траєкторію через: вибір форми навчання; вибір ОК з переліку дисциплін за вибором; вибір ОК з Каталогу курсів на відповідну кількість кредитів, що пропонуються для здобувачів інших ОНП і які пов'язані з тематикою дисертації; можливість вивчення аспірантами ОК у рамках акад. мобільності – на базі інших ЗВО; можливість зарахування кредитів, отриманих у неформальній освіті; право на акад. відпустку або перерву в навчанні, а також на поновлення на навчання; самостійне обрання спеціальності та теми дисертації відповідно до власних наукових інтересів з урахуванням науково-дослідної компетентності та наукового напрямку керівника.

Яким чином здобувачі вищої освіти можуть реалізувати своє право на вибір навчальних дисциплін?

Індивідуальний навчальний план аспірантів ОНП містить перелік дисциплін за вибором аспіранта в обсязі не менш як 25 відсотків загальної кількості кредитів ЄКТС, а саме – 19 кредитів ЄКТС за ОНП 2019 р. та 18 кредитів ЄКТС за ОНП 2022 р., при загальному обсязі 60 кредитів, що відповідає вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук, затвердженого Постановою КМУ від 23.03.2016 №261.

Відповідно до п.4.2 Положення про підготовку здобувачів вищої освіти ступеня доктора філософії та доктора наук в Університеті Грінченка свій вибір аспірант підтверджує заявою. Інформація про вибірково освітні компоненти розміщується на сайті Університету та в Каталозі вибіркового дисциплін. Здійснюючи вибір, аспіранти можуть ознайомитися з нею. Вибір, як правило, здійснюється на початку першого року навчання. Як засвідчує практичний досвід, аспіранти здійснюють вибір освітніх компонентів відповідно до власних наукових інтересів і тематики дисертації. Така мотивація вибору зумовлюється усвідомленням аспірантами обов'язкової вимоги до їхньої атестації, що здійснюватиметься на підставі публічного захисту дисертації. До того ж ще під час вступу до аспірантури, презентуючи власні дослідницькі пропозиції чи досягнення на обов'язковому вступному випробуванні, відповідно до Правил прийому, вступник демонструє коло своїх наукових інтересів, у межах якого планує реалізувати власне дослідження.

Положенням про підготовку здобувачів вищої освіти ступеня доктора філософії та доктора наук в Університеті Грінченка (п.4.2) передбачено право аспірантів вибирати навчальні дисципліни, що пропонуються для інших рівнів вищої освіти і які пов'язані з тематикою дисертації, за погодженням зі своїм науковим керівником та деканом Факультету. Особливою вимогою до цих дисциплін є їх пов'язаність із тематикою дисертації аспіранта, що є цілком об'єктивним та виправданим на третьому рівні вищої освіти. Проте на практиці виявилася недостатня аргументованість пов'язаності тем дисертації аспірантів ОНП з навчальними дисциплінами, що пропонуються на магістерському і, тим паче, на бакалаврському рівнях вищої освіти, що наразі унеможлиблює реалізацію такого вибору. Але постійно ведеться робота, яка спрямована на те, щоб при оновленні чи затвердженні нових магістерських програм особливу увагу звертати на аналіз змісту навчальних дисциплін крізь призму можливості вибору їх аспірантами.

Надання кваліфікованих консультацій щодо формування індивідуальної освітньої траєкторії та її реалізації покладається на завідувача аспірантури, докторантури, гаранта ОНП, завідувачів кафедр, наукових керівників.

Опишіть, яким чином ОП та навчальний план передбачають практичну підготовку здобувачів вищої освіти, яка дозволяє здобути компетентності, необхідні для подальшої професійної діяльності

У навчальному плані ОНП передбачено два види практики – науково-викладацька та дослідницька, обсяг яких складає 8 кредитів ЄКТС (за ОНП 2022р).

Організація практик регулюється Положенням про організацію та проведення практики аспірантів <https://tinyurl.com/kubg-phd-prac>

Практична підготовка формує ряд передбачених ОНП компетентностей: науково-викладацька практика забезпечує формування ЗК1, ЗК3-4, СК3, СК8, а дослідницька практика сприяє виробленню ЗК1-4, СК1-7.

ОНП передбачає наступність видів практичної підготовки здобувачів за такою схемою: опанування та поглиблення дослідницьких і педагогічних компетентностей під час проходження науково-викладацької практики (ОК 9); застосування фахових науково-дослідних компетентностей у межах виконання дисертаційного дослідження під час дослідницької практики (ОК 10).

Рівень задоволеності аспірантів компетентностями, здобутими під час практичної підготовки, з'ясовується шляхом отримання зворотного зв'язку на звітній конференції.

Продемонструйте, що ОП дозволяє забезпечити набуття здобувачами вищої освіти соціальних навичок (soft skills) упродовж періоду навчання, які відповідають цілям та результатам навчання ОП результатам навчання ОП

В ОП такі освітні компоненти сприяють набуттю соціальних навичок: ОК 1 «Філософія і методологія наукової діяльності» через зміст навчального модулю «Наукова етика» – дотриманню правил етики в експериментах та обробці даних, а також взаємодії науковців з громадськістю та іншими зацікавленими сторонами; ОК 2 «Стратегії наукових досліджень» через зміст навчального модулю «Інтернаціоналізація науки» - розвитку інформаційної грамотності завдяки темам з основ роботи з інформаційними ресурсами; ОК3 «Наукова комунікація іноземною мовою» для розвитку мовленнєвих навичок, ОК9 «Науково-викладацька практика» та ОК10 «Дослідницька практика» через розвиток навичок тайм-менеджменту, стресостійкості, комунікативних, мовленнєвих, інформаційно-презентаційних умінь - розвитку спільного проведення досліджень, обміну науковими знаннями та досвідом, співпраці між різними країнами та культурами та підтримці розвитку наукової спільноти у різних частинах світу.

В освітньому процесі використовуються такі форми і методи навчання, як тренінгові практики, науково-дослідні презентації, проектна діяльність.

Освітні компоненти ОП дозволяють здобувачам оволодіти комплексом соціальних навичок (soft skills), притаманних сучасному фахівцю, а саме знання професійної етики, вміння працювати в команді, комунікабельність, вміння презентувати.

Яким чином зміст ОП ураховує вимоги відповідного професійного стандарту?

Професійний стандарт відсутній. Професійна кваліфікація не присвоюється

Який підхід використовує ЗВО для співвіднесення обсягу окремих освітніх компонентів ОП (у кредитах ЄКТС) із фактичним навантаженням здобувачів вищої освіти (включно із самостійною роботою)?

Навчальний план ОП складає 60 кредитів (1800 год.) на весь період навчання, виконання яких аспірантом передбачається протягом перших трьох років навчання. Це зроблено з метою, аби останній рік свого навчання аспіранти присвятили виключно підготовці дисертації до захисту. Співвіднесення обсягу окремих освітніх компонентів ОП (у кредитах ЄКТС) із фактичним навантаженням здобувачів вищої освіти регламентується п.11.4 Положення про організацію освітнього процесу <https://tinyurl.com/kubg-edu-proc>, в якому зазначається, що кількість контактних годин на один кредит для здобувачів третього рівня, як правило, становить 8 год.

Максимальне тижневе аудиторне навантаження для аспірантів не перевищує 18 годин (п.11.2).

Для модульного контролю виділяється 2 год. на 1 кредит. На практико-орієнтовані ОК надається більша кількість практичних занять. Решта часу відводиться для самостійної роботи. Для підготовки до екзамену та його складання виділяється 30 год. із загального обсягу годин самостійної роботи.

Обсяг ОП та окремих її ОК відповідає фактичному навантаженню здобувачів: аудиторне навантаження дисциплін становить 1/3 від загального освітнього навантаження; навчальний час, відведений для самостійної роботи, становить 2/3 загального обсягу навчального часу, відведеного для вивчення конкретної дисципліни. Такий розподіл сприяє виконанню аспірантами завдань для самостійної роботи.

Якщо за ОП здійснюється підготовка здобувачів вищої освіти за дуальною формою освіти, продемонструйте, яким чином структура освітньої програми та навчальний план зумовлюються завданнями та особливостями цієї форми здобуття освіти

За ОП «Інформаційна безпека держави» підготовка здобувачів вищої освіти за дуальною формою освіти не здійснюється.

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

<https://tinyurl.com/kubg-vstup>

Поясніть, як правила прийому на навчання та вимоги до вступників ураховують особливості ОП?

Правила прийому на навчання за ОП враховують її специфіку. Конкурсний відбір проводиться відповідно до Правил прийому на навчання до аспірантури Університету на основі освітнього ступеня магістра (ОКР спеціаліста) за результатами вступних випробувань. Вступні випробування складаються зі: вступного іспиту зі спеціальності (фахового іспиту, який дозволяє встановити глибину необхідних знань претендента зі спеціальності та передбачає перевірку здатності до опанування ОП на основі здобутих раніше компетентностей), вступного іспиту з іноземної мови (англ., німецької, французької, іспанської, італійської) в обсязі, який відповідає рівню B2

Загальноєвропейських рекомендацій з мовної освіти; презентації дослідницьких пропозицій чи досягнень, що дозволяє визначити рівень підготовки до самостійної науково-дослідної роботи.

Ціллю освітньої програми є забезпечення освітньо-наукової підготовки дослідників у сфері кібербезпеки. Успіх цього процесу передбачає наявність у здобувача сформованої системи теоретичних знань та практично

зорієнтованих умінь і навичок з різних складових кібербезпеки, зокрема безпеки інформаційних та комунікаційних систем, технічного захисту інформації, управління інформаційною безпекою (в обсязі навчальної програми для магістра). Програми вступних іспитів оприлюднюються на сайті Університету в розділі «Аспірантам» <https://tinyurl.com/kubg-provst>.

Правилами прийому передбачено нарахування вступникам додаткових балів за наукові здобутки протягом останніх трьох років.

Яким документом ЗВО регулюється питання визнання результатів навчання, отриманих в інших ЗВО? Яким чином забезпечується його доступність для учасників освітнього процесу?

Положенням про підготовку здобувачів вищої освіти ступеня доктора філософії та доктора наук в Університеті (п.4.4) <https://tinyurl.com/kubg-phd-pro> та Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу Університету (п.7.2) <https://tinyurl.com/kubg-mob-rul22> передбачено, що у межах навчального плану ОНП можуть визнаватися отримані аспірантом в інших ЗВО (наукових установах), як українських, так і закордонних (зокрема, навчання за програмами академічної мобільності), результати навчання з однієї чи декількох навчальних дисциплін (зараховуватися кредити ЄКТС), здобуття яких передбачено освітньо-науковою програмою.

Рішення про зарахування кредитів і результатів навчання приймається випусковою кафедрою (у засіданні бере участь науковий керівник аспіранта) та вченою радою відповідного факультету. З цією метою аспірант подає завідувачу аспірантури, докторантури заяву разом із сертифікатом чи іншим документом, що підтверджує факт і результати навчання. Результати навчання зараховуються за умови їх відповідності спеціальності, наявності необхідних обсягів, у порівнянні з обсягами дисциплін/змістових модулів, які аспірант має опанувати під час навчання за ОНП.

Опишіть на конкретних прикладах практику застосування вказаних правил на відповідній ОП (якщо такі були)?

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

Яким документом ЗВО регулюється питання визнання результатів навчання, отриманих у неформальній освіті? Яким чином забезпечується його доступність для учасників освітнього процесу?

Положенням про підготовку здобувачів вищої освіти ступеня доктора філософії та доктора наук в Університеті Грінченка (п.4.3) передбачено, що у межах навчального плану ОНП аспіранту можуть зараховуватися кредити і визнаватися результати навчання, які він отримав у неформальній освіті, на підставі відповідного сертифіката або іншого документа. Рішення про зарахування кредитів і результатів навчання приймається випусковою кафедрою (у засіданні бере участь науковий керівник аспіранта) та вченою радою відповідного Факультету. З цією метою аспірант подає завідувачу аспірантури, докторантури заяву разом із сертифікатом чи іншим документом, що підтверджує факт і результати навчання. Курси зараховуються за умови їх відповідності спеціальності, наявності необхідних обсягів, у порівнянні з обсягами дисциплін/змістових модулів, які аспірант має опанувати під час навчання за ОНП.

Аспірант, який підтвердив рівень свого знання іноземної мови, зокрема англійської, дійсним сертифікатом TOEFL, або International English Language Testing System, або Cambridge English Language Assessment, на рівні C1, має право: на зарахування відповідних кредитів, передбачених ОНП як таких, що виконані у повному обсязі; на використання обсягу навчального навантаження, передбаченого для набуття мовних компетентностей, для здобуття інших компетентностей (за погодженням з науковим керівником).

Опишіть на конкретних прикладах практику застосування вказаних правил на відповідній ОП (якщо такі були)?

За час реалізації ОНП звернень здобувачів щодо визнання результатів навчання, отриманих у неформальній освіті, не було.

4. Навчання і викладання за освітньою програмою

Продемонструйте, яким чином форми та методи навчання і викладання на ОП сприяють досягненню програмних результатів навчання? Наведіть посилання на відповідні документи

Зважаючи на пріоритетне завдання реалізації ОНП – освітній процес орієнтується на розвиток та збагачення особистісно-професійного потенціалу аспірантів, використовуючи компетентнісний, системний та інтегративний підходи, інноваційні та інтерактивні технології, дистанційне навчання, виконання проєктів, науково-викладацьку та дослідницьку практики. Це дозволяє встановити гуманістичний та творчий стиль взаємодії між суб'єктами навчання та сприяє науковому розвитку аспірантів.

Освітній процес реалізовується за допомогою ауд. занять (лек., семінар. і практи.), науково-викладацької і дослідницької практик, контрольних заходів (модульного і семестрового контролів) та сам. роботи здобувача (<https://tinyurl.com/kubg-edu-proc>).

Методи та прийоми навчання добираються викладачем самостійно із міркувань доцільності. Форми і види

навчальних занять, методи навчання та викладання сприяють досягненню РН.

Наприклад, для досягнення РН 1-4 при вивченні дисципліни «Філософія і методологія наукових досліджень» застосовуються словесні, наочні, практичні, проблемно-пошукові методи, самостійна робота, інтерактивні методи, заняття з елементами дистанційного навчання.

Для досягнення РН 4-6 в дисциплінах «Прикладні аспекти створення та застосування систем технічного захисту» та «Прикладні аспекти створення та застосування систем криптографічного захисту» застосовується аналіз, синтез, порівняння, дедукція, лекція, навчальні дискусії, мозковий штурм, моделювання, самоаналіз, взаємоаналіз, термінологічний аналіз, рефлексійний аналіз, мікровикладання.

Продемонструйте, яким чином форми і методи навчання і викладання відповідають вимогам студентоцентрованого підходу? Яким є рівень задоволеності здобувачів вищої освіти методами навчання і викладання відповідно до результатів опитувань?

Пріоритетність студентоцентризму закріплено у Положенні про організацію освітнього процесу (Р.VI) та у Стратегіях розвитку Університету (2018-2022 рр. – п.3, 2023-2027 рр. – р.6).

Навчаючись на ОНП, аспіранти можуть формувати індивідуальну освітню траєкторію через вільний вибір ОК відповідно до власних наукових інтересів; реалізовувати академічну мобільність, здобувати неформальну освіту; поєднувати навчання, дослідження, професійну діяльність; враховуючи власні наукові інтереси, обирати тему, наукового керівника, індивідуальну дослідницьку стратегію; у ході взаємодії з викладачами визначати оптимальні методи і технології навчання.

Застосування інтерактивних методів навчання дозволяє аспірантам висловлювати власні наукові та світоглядні позиції.

Вільний доступ до інформаційних ресурсів диверсифікує джерела навчальної інформації і дає аспірантам можливість самостійно їх обирати.

Під час формалізованих опитувань («Викладач очима студентів», анкета для здобувачів третього (освітньо-наукового) рівня щодо задоволеності змістом та організацією освітньо-наукової підготовки) і неформалізованих опитувань, очних зустрічей аспіранти позитивно оцінюють навчання в аспірантурі.

Продемонструйте, яким чином забезпечується відповідність методів навчання і викладання на ОП принципам академічної свободи

Викладачі мають право самостійно обирати методи навчання і викладання з урахуванням інтересів здобувачів освіти (Положення про організацію освітнього процесу, Р.VIII). Зворотний зв'язок забезпечується опитуванням «Викладач очима студентів».

Методи навчання і викладання на ОНП дозволяють реалізувати принцип академічної свободи, адже передбачено їх варіативність, урахування свободи слова та творчості.

ОНП зорієнтована на забезпечення професійного розвитку аспірантів. Зміст більшості ОК під час вивчення адаптується до наукових потреб здобувачів, які можуть працювати з різним емпіричним матеріалом, запропонованим викладачем або ж тим, що становить безпосередній об'єкт їхнього дослідження. Аспіранти можуть пропонувати власні, пов'язані з напрямками їхніх досліджень, теми для самостійних робіт.

При викладанні окремих освітніх компонентів ОНП здобувачам надається можливість розглянути проблемні питання під різними кутами зору. Використовуються такі методи як дискусія, диспут, групове заняття.

Академічна свобода аспірантів як дослідників і майбутніх викладачів забезпечується можливостями вибору наукового керівника з відповідними науковими інтересами, тематики дослідження, його методології та логістики; формування індивідуальної освітньої траєкторії; вільний вибір ОК; участі у наукових заходах; створення е-портфоліо; можливість брати участь у програмах академічної мобільності; долучення до роботи Наукового товариства студентів, аспірантів, докторантів і молодих вчених.

Опишіть, яким чином і у які строки учасникам освітнього процесу надається інформація щодо цілей, змісту та очікуваних результатів навчання, порядку та критеріїв оцінювання у межах окремих освітніх компонентів *

Загальна інформація про особливості освітньої діяльності за ОНП надається на організаційних зборах на початку навчання. Інформація щодо змісту, структури, мети вивчення ОК, очікуваних результатів навчання, порядку та критеріїв оцінювання у межах окремих ОК надається аспірантам на першому занятті з кожної дисципліни згідно з Положенням про організацію освітнього процесу (п.9.3.1), а також на настановчих зборах з усіх видів практик. Така форма інформування дозволяє аспірантам отримати повне уявлення про ОНП, окремі дисципліни та, за потреби, з'ясувати усі запитання.

Задля швидкого доступу до інформації на будь-якому етапі освітнього процесу на сайті ЗВО в розділі «Аспірантам» розміщено всі ОНП, інформацію про вибіркові ОК, робочі програми навчальних дисциплін, програми практик, навчальні плани. Тут є інформація про організацію освітнього процесу для аспірантів усіх спеціальностей: графік освітнього процесу, розклад занять, програми іспитів тощо. Інформація оперативного оновлюється на сайті задля швидкого повідомлення про будь-які зміни.

Для доступу до ресурсів Університету кожному здобувачеві створюється корпоративна пошта, яка забезпечує ефективну комунікацію з викладачами, науковими керівниками, гарантом ОНП, завідувачем кафедри, викладачами, адміністрацією, завідувачем аспірантури, докторантури.

Поєднання різних форм інформування дозволяє забезпечити комунікаційну підтримку здобувачів освіти на всіх етапах освітнього процесу про всі важливі компоненти та зміни.

Опишіть, яким чином відбувається поєднання навчання і досліджень під час реалізації ОП

Поєднання навчання і наукових досліджень в Університеті під час реалізації ОНП передбачає практико-орієнтоване вивчення певного завдання/проблеми. Цьому сприяє:

- 1) здобувачі освіти залучені до реалізації наукової теми кафедри «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (держ. реєстр. номер: 0122U200483);
- 2) відкриття в Університеті Центрив компетентностей: «Дослідження технологій функціонування та захисту інформаційно-комунікаційних систем і мереж» та «Дослідження технологій захисту інформаційних активів», а також розміщення в лабораторіях Центрив сучасного програмно-апаратного забезпечення, використовуваного в освітньому процесі;
- 3) започаткування випуску з 2018 р. електронного наукового фахового видання Університету (рішення Вченої ради від 26.04.2018) «Кібербезпека: освіта, наука, техніка» <https://tinyurl.com/mwfr35au>;
- 4) проведення Університетом наукових конференцій, семінарів і круглих столів з питань ЗІ та забезпечення безпеки ІКС, участь в них беруть як НПП, так і здобувачі. Зокрема у 2019 р. кафедрою спільно з ін. університетами організовано і проведено міжнародні конференції та воркшопи, зокрема: «Problems of Infocommunications. Science and Technology PICS&T» <http://picst.ieee.org.ua/pic-st2019/>, «Cybersecurity Providing in Information and Telecommunication Systems CPITS 2020»; у січні та жовтні 2021 р. , «Cybersecurity Providing in Information and Telecommunication Systems CPITS 2021»; у жовтні 2022 р. «Cybersecurity Providing in Information and Telecommunication Systems CPITS 2022» <https://cpits.kubg.edu.ua/>. Праці вище зазначених конференцій індексуються у наукометричній базі SCOPUS. Аспіранти ОНП активно беруть участь у зазначених заходах та опублікували близько 20 наукових праць;
- 5) функціонування на Факультеті Наукового товариства студентів, аспірантів, докторантів та молодих вчених, в ході роботи якого здобувачі беруть участь у розробці експериментального обладнання для дослідження навантаження мережі, ідентифікації DoS-атак на мережі, організації RFID-снїффінгу тощо;
- 6) логіка побудови ОНП забезпечує дослідницьку компоненту навчання на змістово-методичному рівні, зокрема, аспірантам викладаються ОК «Філософія і методологія наукової діяльності», «Стратегії наукових досліджень», «Наукова комунікація іноземною мовою», яким притаманне використання методів навчання, заснованих на дослідженнях через розробку наукових завдань, аргументацію і презентацію досліджуваних проблем, підготовку доповідей;
- 7) поєднання навчання і досліджень посилюють науково-викладацька та дослідницька практики, які у повному обсязі сприяють отриманню необхідних компетентностей здобувачами.

Продемонструйте, із посиланням на конкретні приклади, яким чином викладачі оновлюють зміст навчальних дисциплін на основі наукових досягнень і сучасних практик у відповідній галузі

Систематичне оновлення змісту освітніх компонентів передбачено Положенням про організацію освітнього процесу (Р.VI) <https://tinyurl.com/kubg-edu-proc> та відбувається відповідно до Методичних рекомендацій з розроблення робочих програм навчальних дисциплін <https://tinyurl.com/kubg-rpn-rul>. Щорічно перед початком навчального року викладачі переглядають робочі програми та, за потреби, оновлюють їх зміст, перелік рекомендованої літератури, завдання для самостійної роботи відповідно до наукових досягнень і практичних запитів галузі кібербезпеки.

Оновленню ОК сприяє активна залученість викладачів кафедри до міжнародних проєктів, наукових конференцій, семінарів, тренінгів, зокрема, участь В. Соколова, П. Складанного, Г. Гулака, Н. Коршун в проєкті «Research of Natural Language Processing» сприяла вдосконаленню змісту дисципліни «Організація захисту розподілених інформаційних ресурсів».

Зміни, уточнення до РПНД затверджуються на засіданнях кафедр. Зміст навчальних дисциплін перевіряється на предмет уникнення повторень і застарілої інформації, беруться до уваги міжгалузеві та міжпредметні зв'язки. У 2022 р. оновлено ОК8 «Прикладні аспекти теорій ризиків, конфліктів і катастроф в системах безпеки» щодо актуальних підходів, методів, методологій та алгоритмів виявлення та протидії ризикам в системах безпеки, ВК 5 «Технології безпеки складних соціотехнічних систем» щодо протидії актуальним загрозам з використанням методів соціальної інженерії.

Опишіть, яким чином навчання, викладання та наукові дослідження у межах ОП пов'язані із інтернаціоналізацією діяльності ЗВО

Провідним вектором інтернаціоналізації діяльності Університету є реалізація права НПП і аспірантів на академічну мобільність, закріпленого у Положенні про порядок реалізації права на академічну мобільність учасників освітнього процесу Університету <https://tinyurl.com/kubg-mob-rul22>

Інформація про проєкти та можливості поширюється через веб-сторінку НДЛ інтернаціоналізації вищої освіти <http://ivo.kubg.edu.ua/>

Здійснюється забезпечення умов для реалізації аспірантами міжнародної академічної мобільності відповідно до договорів про міжнародну співпрацю, у т.ч. у рамках програми Еразмус+, залучення аспірантів до реалізації спільних міжнародних освітніх та дослідницьких проєктів. У рамках модуля «Інтернаціоналізація науки» аспіранти знайомляться з перспективами міжнародної наукової взаємодії, дізнаються про можливості отримання грантів, закордонні видання тощо.

Для здобувачів освіти та НПП забезпечено доступ до міжнародних наукометричних баз Scopus та Web of Science та інших <https://tinyurl.com/kubg-sci-base>

Здобувачі Іосіфов Є., Сукайло І., Цирканюк Д., а також викладачі Коршун Н., Гулак Г., Соколов В., Складаний П. беруть участь у міжнародному проєкті Research of Natural Language Processing за грантом №43-070121 від Ender Turing OÜ (Таллін, Естонія) <https://tinyurl.com/5h6npjbr>

Здобувачі ОНП мають можливість долучатись у якості слухачів до європейських модулів Жана Моне <https://cutt.ly/34jwAYt>, які викладаються в Університеті

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

Опишіть, яким чином форми контрольних заходів у межах навчальних дисциплін ОП дозволяють перевірити досягнення програмних результатів навчання?

З метою всебічного оцінювання досягнення аспірантами результатів навчання (РН) застосовуються такі форми і методи контролю: усний контроль, що використовується з метою перевірки сформованості загальних і фахових компетентностей (індивідуальне, фронтальне опитування, співбесіда, презентація, виступ ін.); письмовий та комбінований (письмовий і усний) контроль: письмові роботи різних типів (тестування; виконання індивідуальних завдань, творчої роботи, аналітичного дослідження для перевірки сформованості інтегральної компетентності); комп'ютерний контроль, у т.ч. тестове опитування, що використовується для об'єктивізації оцінювання; самоконтроль – для розвитку у здобувачів уміння оцінювати свої досягнення. Якісне оцінювання можливе лише при оптимальному поєднанні різних видів, форм, методів контролю, що передбачено ОНП.

Основними видами контролю є проміжний і підсумковий. Проміжний проводиться на всіх видах аудиторних занять та під час виконання самостійної роботи. У дисциплінах методологічного та фахового характеру переважають усні й письмові форми з розгорнутими відповідями, що відповідає специфіці загальнонаукового і фахового матеріалу. Ці форми контролю дозволяють оцінити досягнення аспірантів у межах теми, тематичних блоків, змістового модулю, виявити проміжний стан досягнення РН (засвоєння знань, опанування умінь, вироблення навичок). Важливим є виконання аспірантами завдань для самостійної роботи, що дозволяє викладачу перевірити заплановані параметри, зокрема повноту, структурність, інтегрованість, рівень засвоєння знань ін. Обов'язковим контрольним заходом є проміжне (семестрове) звітування аспірантів про виконання індивідуального плану.

Підсумковий контроль з дисципліни передбачає іспит чи залік; з практики – звітування. Зміст екзаменаційних завдань базується на компетентнісному підході й поєднує теоретичну і практичну складові, що забезпечує поліфункціональну перевірку й оцінку якості засвоєння аспірантом програмних компетентностей. При оцінюванні результатів проходження практики враховується виконання вимог, передбачених програмами практик.

Підсумковий контроль у формі заліку передбачає встановлення підсумкової оцінки за результатами поточної успішності, що мотивує здобувачів демонструвати використання отриманих знань протягом всього періоду опанування освітнього компонента та спрямовано на забезпечення сталості формування програмних компетентностей і результатів навчання аспірантів. Обов'язковим заходом є річне звітування про виконання індивідуального плану.

ОНП передбачено атестацію, що здійснюється разовою спецрадою на підставі публічного захисту наукових досягнень у формі дисертації, що відповідає п.4 ст.6 ЗУ «Про вищу освіту».

Яким чином забезпечуються чіткість та зрозумілість форм контрольних заходів та критеріїв оцінювання навчальних досягнень здобувачів вищої освіти?

Для перевірки досягнутих результатів навчання на ОНП застосовуються різні форми поточного, проміжного (опитування, перевірка письмових, самостійних робіт тощо) та підсумкового (екзамени, заліки, звіти з практики) контролю. Форми проведення проміжного контролю та критерії оцінювання визначаються у робочих програмах навчальних дисциплін.

Обов'язковою формою проміжного та підсумкового контролю при підготовці аспірантів є проміжне (семестрове) та підсумкове (річне) звітування про виконання індивідуального плану роботи.

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 Університету необхідної інформації; розміщенням робочих програм навчальних дисциплін на сайті Університету; установчими зборами перед практиками; проведенням поточних консультацій.

Яким чином і у які строки інформація про форми контрольних заходів та критеріїв оцінювання доводяться до здобувачів вищої освіти?

Механізми проведення контрольних заходів, шляхи оцінювання об'єктивності екзаменаторів, процедури запобігання та врегулювання конфлікту інтересів, порядок оскарження результатів контрольних заходів та їх повторного проходження визначені у Положенні про організацію освітнього процесу.

Інформування аспірантів про форми контрольних заходів та критеріїв оцінювання реалізується кількома способами. До початку навчального року на сайті в розділі «Аспірантам» розміщується графік освітнього процесу із зазначенням атестаційних тижнів; на початку н.р. розміщуються робочі програми дисциплін з переліком форм проміжного та підсумкового контролів і критеріїв оцінювання. На початку першого року навчання аспіранти отримують інд. плани.

Під час перших занять з кожної дисципліни аспіранти отримують вичерпну інформацію щодо форм контролю та критеріїв оцінювання. Програма екзамену з критеріями розміщується на сайті.

Протягом року під час супервізійних зустрічей аспірантів з НПП з'ясується ступінь чіткості і зрозумілості здобувачами критеріїв оцінювання їх навчальних досягнень. За потреби вносяться відповідні правки у структуру та зміст завдань.

Вимоги до оцінювання результатів практики, викладені у програмі практики, доводяться до відома аспірантів на установчих зборах перед початком практики, також розміщуються на сайті.

Зрозумілість форм контролю та критеріїв оцінювання досягнень здобувачів забезпечується також через уніфіковану Систему оцінювання навчальних досягнень студентів Університету.

Яким чином форми атестації здобувачів вищої освіти відповідають вимогам стандарту вищої освіти (за наявності)?

Стандарт вищої освіти за спеціальністю 125 Кібербезпека за третім рівнем вищої освіти відсутній, однак ОНП передбачає, що «Атестація здобувачів вищої освіти ступеня доктора філософії здійснюється постійно діючою або разовою спеціалізованою вченою радою на підставі публічного захисту наукових досягнень у формі дисертації», що відповідає п.3 ст.6 Закону України «Про вищу освіту» та п.30 Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук, затвердженого Постановою Кабінету міністрів України від 26.03.2016 р. №261 (зі змінами).

Яким документом ЗВО регулюється процедура проведення контрольних заходів? Яким чином забезпечується його доступність для учасників освітнього процесу?

Процедура проведення контрольних заходів регулюється документами, розміщеними на сайті Університету у вільному доступі:

Положенням про організацію освітнього процесу <https://tinyurl.com/kubg-edu-proc>

Методичними рекомендаціями з розроблення робочих програм навчальних дисциплін <https://tinyurl.com/kubg-rpn-rul>

Положенням про організацію та проведення практики аспірантів <https://tinyurl.com/kubg-phd-prac>

(Вище перераховані документи, як і більшість інших, що стосуються роботи ЗВО, доступні в Реєстрі нормативної бази <https://tinyurl.com/kubg-norm>)

ОНП, розміщеною на сайті Університету в рубриках «Аспірантам» та «Вступникам».

Форми контрольних заходів та критерії їх оцінювання відображено у робочих програмах навчальних дисциплін, які розміщені на сайті Університету в рубриці «Аспірантам».

Робочі програми кожної навчальної дисципліни передбачають проведення поточного та підсумкового контролю, а також критерії їх оцінювання і шкалу відповідності балів, розподіл балів, які отримують аспіранти.

Строки проведення контрольних заходів зазначено у графіку освітнього процесу, розміщеному на сайті Університету в розділі «Аспірантам».

Яким чином ці процедури забезпечують об'єктивність екзаменаторів? Якими є процедури запобігання та врегулювання конфлікту інтересів? Наведіть приклади застосування відповідних процедур на ОП

Об'єктивність екзаменаторів при оцінюванні знань аспірантів у процесі підсумкового контролю забезпечується передусім впровадженням до переліку форм його проведення письмової екзаменаційної роботи та тестового електронного екзаменаційного завдання. Екзамени, як правило, проводяться у письмовій формі, що забезпечує об'єктивність оцінювання робіт, проте в окремих випадках можлива усна чи комбінована форма. Перевірка виконання тестових завдань здійснюється автоматично.

За період навчання аспірантів за ОНП при проведенні контрольних заходів конфлікту інтересів не виникало. Скарг аспірантів на упередженість та необ'єктивність викладачів не було.

За результатами щорічного анкетування аспірантів щодо задоволеності змістом та організацією освітньо-наукової підготовки, найвищий рівень задоволеності форм проведення поточного та підсумкового контролів знань і критеріями оцінювання продемонструвало 76% здобувачів у 2021 р. і 82% у 2022 р.

Яким чином процедури ЗВО урегулюють порядок повторного проходження контрольних заходів? Наведіть приклади застосування відповідних правил на ОП

Порядок повторного проходження контрольних заходів (ліквідації академічної заборгованості) аспірантами регулюється п.9.4 Положення про організацію освітнього процесу в Університеті <https://tinyurl.com/kubg-edu-proc>.

Академічна заборгованість з певної навчальної дисципліни виникає у разі одержання здобувачем вищої освіти незадовільного балу за результатами підсумкового контролю. Аспіранти, які не виконали індивідуальний навчальний план за підсумками навчального року, вважаються такими, що мають академічну заборгованість.

Аспірантам, яким не зараховано кредитів на дату проходження звітування, рішенням кафедри та вченої ради Факультету призначається дата повторного звітування з урахуванням ліквідації академічної заборгованості. Термін перенесення звіту, а, отже, строки ліквідації академічної заборгованості, як правило, не більше трьох місяців.

Перескладання екзамену допускається не більше двох разів з кожної дисципліни: один раз – викладачу, другий – комісії. За час реалізації ОНП випадків повторного проходження контрольних заходів не було.

Яким чином процедури ЗВО урегулюють порядок оскарження процедури та результатів проведення контрольних заходів? Наведіть приклади застосування відповідних правил на ОП

Порядок оскарження процедури та результатів проведення контрольних заходів регулюється п.9.3.4.3 Положення про організацію освітнього процесу в Університеті <https://tinyurl.com/kubg-edu-proc>.

Здобувач вищої освіти, 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 (студентський офіс) 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 здобувача вищої освіти не проводиться.

Якщо екзамен був усний або комбінований, то проводиться додаткове опитування аспіранта.

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

Засідання апеляційної комісії відбувається, як правило, наступного дня після отримання заяви здобувача вищої освіти. Підсумкова оцінка, виставлена комісією, є остаточною і апеляції та перескладання не підлягає.

На ОНП випадків оскарження здобувачами процедури та результатів проведення контрольних заходів не було.

Які документи ЗВО містять політику, стандарти і процедури дотримання академічної доброчесності?

В Університеті розроблена і дотримується нормативна база щодо політики, стандартів і процедур забезпечення академічної доброчесності. Їх відображено у таких документах:

Кодекс корпоративної культури Університету Грінченка (п.3.5): <https://tinyurl.com/kodeks-korp>

Декларація про академічну доброчесність науково-педагогічних, наукових, педагогічних працівників та студентів, аспірантів, докторантів Університету. Декларації було обговорено та схвалено в Університеті на різних рівнях і затверджено Конференцією трудового колективу у вересні 2016 р. <https://tinyurl.com/deklaratsii>

Положення про академічну доброчесність науково-педагогічних, наукових, педагогічних працівників та здобувачів освіти Університету: <https://tinyurl.com/kubg-integrity>

Положення про підготовку здобувачів вищої освіти ступеня доктора філософії та доктора наук в Університеті Грінченка (п.8.2, п.8.3): <https://tinyurl.com/kubg-phd-pro>

Наказ «Про затвердження складу комісії з академічної доброчесності Університету» від 10.03.2023 №104: <https://tinyurl.com/dobr2023>

Стратегія (Програма) розвитку Університету Грінченка на 2018-2022 рр. (п.1.2, 4.3): <https://tinyurl.com/kubg-strat> та Стратегія розвитку Університету Грінченка на 2023-2027 рр. (п.1,4) <https://tinyurl.com/kubg-stratN>

План роботи Університету на 2023 рік (розділ II «Освітня стратегія» п. 22, 30, розділ III «Наукова стратегія» п. 4, 9-14, 73): <https://tinyurl.com/ybpdm46>

Які технологічні рішення використовуються на ОП як інструменти протидії порушенням академічної доброчесності?

З метою запобігання порушень академічної доброчесності у публікаціях, текстах дисертацій та ін. здійснюється технічна перевірка наукових публікацій за допомогою спеціалізованих програмних засобів, зокрема через сервіс Unicheck, що використовуються в Університеті на умовах договорів з ТОВ «Антиплагіат», та експертної оцінки щодо відсутності/наявності академічного плагіату.

Як інструменти протидії порушенням академічної доброчесності використовуються технологічні рішення: розроблення та запровадження комп'ютерного тестування аспірантів з автоматичним оцінюванням роботи; попереднє експертне оцінювання, зокрема й самооцінювання, та/або технічна перевірка щодо ознак академічного плагіату у текстах, підготовлених до друку;

використання спеціалізованого програмного забезпечення для виявлення плагіату на основі чітких правил і політики щодо його використання;

використання для проведення контрольних заходів аудиторій, обладнаних відеокамерами, розташування яких дозволяє отримати зображення з усіх кутів огляду, що унеможливорює списування.

Навчальний план ОНП містить модуль «Наукова етика», також заняття щодо академічної доброчесності проводяться в межах модуля «Інтернаціоналізація науки». Аспіранти та НПП підписують декларацію про академічну доброчесність, беручи на себе зобов'язання дотримуватись її принципів та підтверджуючи ознайомлення з текстом Положення про академічну доброчесність Університету.

Яким чином ЗВО популяризує академічну доброчесність серед здобувачів вищої освіти ОП?

Дотримання принципів академічної доброчесності є невід'ємною частиною корпоративної культури Університету.

Всі учасники освітнього процесу Університету ознайомлюються з Положенням про академічну доброчесність Університету та на добровільних засадах підписують декларацію про дотримання академічної доброчесності.

У Науковому товаристві студентів, аспірантів, докторантів і молодих вчених Університету діє Школа академічної доброчесності, діяльність якої передбачає підготовку «агентів змін», котрі через різні заходи будуть популяризувати та утверджувати принципи академічної доброчесності серед академічної спільноти Університету. Метою заходів є ознайомлення та інформування учасників освітнього процесу щодо дотримання норм законодавства України про авторське право і суміжні права, правил цитування, об'єктивного оцінювання результатів навчання тощо.

Наукове товариство щорічно проводить Всеукраїнську науково-практичну конференцію «Дослідження молодих вчених: від ідеї до реалізації», один із напрямів роботи якої – «Наука та освіта: утвердження академічної доброчесності та наукової етики», у рамках якого відбувається конкурс проектів, майстер-класи, тренінги відповідної тематики <https://tinyurl.com/kubg-konf22>; <https://tinyurl.com/kubg-konf21>; <https://tinyurl.com/kubg-konf20>; <https://tinyurl.com/konf-2019>

У рамках Програми підвищення кваліфікації НПП Університету за дослідницьким модулем проводиться тренінг для викладачів на тему «Перевірка наукових текстів на плагіат».

Яким чином ЗВО реагує на порушення академічної доброчесності? Наведіть приклади відповідних ситуацій щодо здобувачів вищої освіти відповідної ОП

Положенням про академічну доброчесність передбачено такі види відповідальності за її порушення:

НПП: попередження; відмова у присудженні наукового ступеня чи присвоєнні вченого звання; позбавлення присудженого наукового ступеня чи присвоєного вченого звання; відмова у присвоєнні або позбавлення присвоєного педагогічного звання, кваліфікаційної категорії; позбавлення права брати участь у роботі визначених

законом органів (зокрема вчених рад, спецрад) чи займати визначені законом посади; позбавлення можливості здійснювати наукове керівництво аспірантами/ наукове консультування докторантів; позбавлення можливості викладати дисципліни навчального плану підготовки докторів філософії.

Здобувачі: попередження; повторне проходження оцінювання (проміжного та підсумкового контролю); повторне проходження відповідного освітнього компонента ОП; відрахування; відмова у призначенні академічної стипендії; відмова у наданні позитивного висновку про наукову новизну, теоретичне та практичне значення результатів дисертації; відмова у присудженні ступеня доктора філософії без права повторного захисту дисертації; позбавлення ступеня доктора філософії у порядку, передбаченому законодавством.

Створено постійно діючі комісії з питань академічної доброчесності Університету (наказ ректора) та факультетів (розпорядження деканів).

Завдяки політиці дотримання академічної доброчесності в Університеті на сьогодні не виявлено порушень академічної доброчесності здобувачами ОНП.

6. Людські ресурси

Яким чином під час конкурсного добору викладачів ОП забезпечується необхідний рівень їх професіоналізму?

Професіоналізм викладачів визнається Університетом як провідний чинник якості надання освітніх послуг здобувачам вищої освіти. Відповідно, рівень професіоналізму викладачів є головним критерієм проходження ними конкурсного добору, який регламентується Положенням про конкурс на заміщення вакантних посад НПП <https://tinyurl.com/4j897ynx>.

Кандидатури претендентів на посади НПП попередньо обговорюються на відповідних кафедрах. Для оцінювання рівня професійної кваліфікації претендента на посаду НПП кафедра може запропонувати йому прочитати лекції, провести практичні заняття, за результатами яких складається відгук про відкрите заняття. За результатами обговорення складається мотивований висновок про професійні якості кожного з претендентів.

Рішення про 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, що забезпечують освітній процес на ОНП – це висококваліфіковані викладачі, що мають відповідну освіту, науковий ступінь доктора чи кандидата наук, є кваліфікованими дослідниками відповідно до змісту ОНП.

Опишіть, із посиланням на конкретні приклади, яким чином ЗВО залучає роботодавців до організації та реалізації освітнього процесу

Кафедрою ІКБ підписані та реалізуються угоди як з державними, так і з комерційними установами. Серед них: НДІ «АВТОПРОМ», НВФ «КРИПТОН», ТОВ «АВТОР», ТОВ «Інститут ІТ», ТОВ «ТЗІ», Державне підприємство «Українські спеціальні системи», Державне підприємство «Державний центр ІР», Інститут телекомунікацій та глобального інформаційного простору НАН України, Інститут проблем математичних машин та систем НАН України тощо. Предметом Угод є НТС у сфері кіберзахисту та ЗІ в ІТ СМ, спрямоване на забезпечення ІКБ, удосконалення технологій КТЗІ в умовах посилення кіберзагроз та в межах повноважень і компетенції кожної зі сторін, проведення підготовки/перепідготовки та підвищення кваліфікації власних кадрів.

На засадах науково-освітнього партнерства доктори технічних наук інших ЗВО та НДІ були залучені до рецензування освітньої програми, надають здобувачам консультації з питань міжгалузевих аспектів реалізації дисертаційного дослідження та ін. (за запитом), здійснюють експертизу науково-методичних видань, запрошуються до участі у наукових конференціях та семінарах, до реалізації дослідницьких проектів. Також представники роботодавців залучаються до проведення в Університеті гостьових лекцій, науково-практичних семінарів, круглих столів, панельних дискусій тощо («Імітаційне моделювання. Математичне моделювання процесів» заступника директора з наукової роботи Інституту програмних систем НАН України д.т.н., проф. В.Л. Шевченка <https://tinyurl.com/bdh69jaz>).

Опишіть, із посиланням на конкретні приклади, яким чином ЗВО залучає до аудиторних занять на ОП професіоналів-практиків, експертів галузі, представників роботодавців

Залучення професіоналів-практиків, експертів і представників роботодавців до викладання та організації освітнього процесу відбувається при проведенні гостьових лекцій відомими роботодавцями та авторитетними представниками професійної спільноти, зокрема, Інституту телекомунікацій і глобального інформаційного простору НАН України, Інституту проблем математичних машин і систем НАН України тощо («Сучасні теоретичні та практичні науково-дослідні роботи Інституту кібернетики ім. В.М. Глушкова НАН України» старшого наукового співробітника відділу відеосистем реального часу Інституту кібернетики ім. В.М. Глушкова НАН України, к.т.н. О.В. Багацького <http://surl.li/xfch>, «Аудит інформаційної безпеки – основа ефективного захисту підприємства» начальника відділу інформаційної безпеки Національної енергетичної компанії «Укренерго», к.т.н. Я.В. Рой <https://tinyurl.com/hjje235x>, «Криптовірологія: загрози безпеки гарантоздатним інформаційним системам і заходи протидії шифрувальним вірусам» завідувача лабораторії з питань кібербезпеки Інституту проблем математичних машин та систем НАНУ д.т.н., доц. Г.М. Гулака <https://tinyurl.com/y7b9vzv5>).

До викладання на ОНП залучені професіоналі-практики: д.т.н., доц. Г.М. Гулак, к.в.н., доц. А.О.Аносов, к.т.н., доц.

Опишіть, яким чином ЗВО сприяє професійному розвитку викладачів ОП? Наведіть конкретні приклади такого сприяння

В Університеті згідно з Положенням про підвищення кваліфікації НПП <https://tinyurl.com/4m56463r> створено цілісну систему підвищення кваліфікації, метою якої є забезпечення потреб освітньої галузі у кваліфікованих високопрофесійних кадрах, здатних виконувати фахові завдання і посадові функції, сприяти інноваційним процесам в освіті, упроваджувати новітні технології. Підвищення кваліфікації має пролонгований характер і відбувається в процесі опанування НПП модулів, які забезпечать розвиток: фахової, дидактичної, дослідницької, ІКТ, лідерської компетентностей. Крім того, науково-педагогічні працівники проходять фахове стажування в інших ЗВО. Для нових НПП проводяться адаптаційні тренінги та, за необхідності, призначається тьютор в особі досвідченого НПП Університету відповідно до Положення про адаптацію новопризначених НПП <https://tinyurl.com/kubg-adapt>
Важливу роль у системі професійного розвитку відіграє ННЦ розвитку персоналу та лідерства <https://tinyurl.com/kubg-esc-lead>
Сприяє професійному розвитку викладачів ОНП відкритий в Університеті доступ до міжнародних наукометричних баз даних Scopus і Web of Science та можливість публікації статей у фахових виданнях Університету. Моніторинг професійного рівня відбувається за допомогою щорічного рейтингового оцінювання «Лідер року», яке містить перелік всіх професійних здобутків НПП за рік, та знаходиться у відкритому доступі.

Продемонструйте, що ЗВО стимулює розвиток викладацької майстерності

Підвищення мотивації працівників як одне із завдань передбачено Стратегіями розвитку Університету на 2017-2022 рр. (п.2.2.) <https://tinyurl.com/kubg-strat> та на 2023-2027 рр. (п.2) <https://tinyurl.com/kubg-stratN>. Система заохочення викладачів за досягнення у фаховій сфері регламентується Правилами внутрішнього розпорядку <https://tinyurl.com/kubg-rules>, Положенням про щорічне рейтингове оцінювання професійної діяльності НПП, НП «Лідер року» <https://tinyurl.com/kubg-leader>. Основним агрегатором інформації про діяльність викладача є електронна система «Е-портфоліо» <http://eportfolio.kubg.edu.ua>, завдяки чому забезпечується прозорість та об'єктивність оцінки. Рейтингові показники щороку переглядаються. Результати рейтингу використовуються для матеріального та морального заохочення працівників. Для працівників Університету передбачені види заохочень: оголошення подяки, нагородження грамотою, медаллю Бориса Грінченка, нагрудним знаком «За служіння Університету» відповідно до Положення про відзнаки <https://tinyurl.com/kubg-vidznaku>. У випадках та в порядку, передбаченому законодавством України, працівники можуть представлятися до відзначення державними і відомчими нагородами.
В Університеті діє Положення про преміювання працівників <https://tinyurl.com/kubg-prem>, а також Порядок преміювання працівників за публікації у Scopus та WoS <https://tinyurl.com/kubg-pr-swos>, <https://tinyurl.com/kubg-pr-swos-p>

7. Освітнє середовище та матеріальні ресурси

Продемонструйте, яким чином фінансові та матеріально-технічні ресурси (бібліотека, інша інфраструктура, обладнання тощо), а також навчально-методичне забезпечення ОП забезпечують досягнення визначених ОП цілей та програмних результатів навчання?

В Університеті проводиться постійна робота над поліпшенням матеріально-технічної бази. Планування фінансових потреб та їх забезпечення регулюється планово-економічним відділом бухгалтерії за погодженням із керівником ЗВО, у т.ч. з урахуванням пропозицій від структурних підрозділів. Матеріально-технічні ресурси забезпечують досягнення визначених програмою цілей та програмних результатів навчання. Так, у навчальних приміщеннях, де здійснюється освітній процес за ОНП, є достатня кількість аудиторій та комп'ютерних класів, які мають необхідне програмне забезпечення. Створена необхідна соціальна інфраструктура (в наявності актові зала, їдальня, медичний пункт; обладнані місця для відпочинку та культурного дозвілля здобувачів). Навчально-методичне забезпечення ОНП дає можливість досягати визначених ОНП цілей і РН завдяки його максимальній змістовій насиченості та постійному оновленню. Здобувачі мають доступ до навчально-методичних матеріалів, оскільки вони своєчасно розміщуються на сайті Університету. Для здобувачів вищої освіти і НПП забезпечено доступ до наукометричних баз Scopus та Web of Science, ресурсів SpringerRink, Libraria та ін. (<https://tinyurl.com/kubg-sci-base>).

Продемонструйте, яким чином освітнє середовище, створене у ЗВО, дозволяє задовольнити потреби та інтереси здобувачів вищої освіти ОП? Які заходи вживаються ЗВО задля виявлення і врахування цих потреб та інтересів?

Освітнє середовище, створене в Університеті, дозволяє задовольнити потреби та інтереси здобувачів вищої освіти ОНП завдяки збалансованості матеріальних умов і сприйняття здобувачів як рівноправних партнерів. ЗВО задля виявлення і врахування цих потреб та інтересів проводить зустрічі та обговорення з аспірантами, консультації з представниками Наукового товариства студентів, аспірантів, докторантів і молодих вчених Університету, у т.ч. з виборним представником від аспірантів та докторантів ЗВО до Вченої ради Університету. Викладання дисциплін забезпечене матеріально-технічними засобами, достатніми для досягнення заявлених результатів навчання ОНП. Аудиторії навчального корпусу, в якому проходить навчання за ОНП, обладнано

сучасними мультимедійними комплексами (проектор, комп'ютер, смарт-дошка), доступом до мережі Інтернет, фліпчартами, модульними меблями тощо.

Створено ІТ-інфраструктуру – Цифровий кампус, який розподілено за розділами «Цифрова освіта», «Цифрова наука», «Цифрове управління», «Імідж та лідерство», «Цифровий простір», «Інфраструктура» та категоріями – «Студентам», «Викладачам», «Вчителям». Ключовими складниками є система електронного навчання (Moodle), Wiki-портал, інституційний репозиторій, система Е-портфоліо та ін.

Відбуваються зустрічі аспірантів з гарантом ОНП та викладачами кафедри, завідувачем аспірантури, докторантури, адміністрацією задля виявлення їхніх потреб та інтересів. Результати зустрічей враховуються під час планування роботи Університету.

Опишіть, яким чином ЗВО забезпечує безпечність освітнього середовища для життя та здоров'я здобувачів вищої освіти (включаючи психічне здоров'я)?

ЗВО суворо дотримується норм техніки безпеки, постійно інструктує НПП та здобувачів вищої освіти, проводить заходи, які стосуються здорового способу життя тощо. Питання безпечності здоров'я та життя здобувачів вищої освіти відображено у Стратегіях розвитку Університету на 2018-2022 рр. та на 2023-2027 рр. (р.10)

<https://kubg.edu.ua/resursi/dokumenty.html>

Єдина система організації роботи з охорони праці та безпеки життєдіяльності учасників осв. процесу визначена у відповідному Положенні <https://tinyurl.com/bezp-osvita>, діє наказ «Про систему оповіщення, зміст дій щодо загрози вчинення терористичного акту, виявлення підозрілих предметів або виникнення надзвичайних ситуацій в приміщеннях університету та його територіях» <https://tinyurl.com/syst-opov>, створено умови запобігання поширенню коронавірусу <https://tinyurl.com/kubg-Cov>, розроблено алгоритм дій під час повітряної тривоги <https://tinyurl.com/kubg-sign> та ін. документи, які оприлюднені на сайті ЗВО.

Навчальні корпуси, в яких проходить навчання здобувачів, обладнано контрольно-пропускною системою, відеокameraми безпеки, системою протипожежної безпеки, системою зовн. блискавковідводу та заземлення.

Особливу увагу приділено забезпеченню інформац. та кібербезпеки Ун-ту: створено комплексну систему захисту інформації, проводиться постійне вдосконалення мережі.

Задля збереження психічного здоров'я співробітників Університету та здобувачів діє соц.-психологічна служба, у т.ч. «Допомога психолога онлайн» <https://tinyurl.com/dop-online>

Опишіть механізми освітньої, організаційної, інформаційної, консультативної та соціальної підтримки здобувачів вищої освіти? Яким є рівень задоволеності здобувачів вищої освіти цією підтримкою відповідно до результатів опитувань?

В Університеті діє ряд документів, які унормовують механізми освітньої, організаційної, інформаційної, консультативної та соціальної підтримки здобувачів вищої освіти. Зокрема, це Положення про: підготовку здобувачів вищої освіти ступеня доктора філософії та доктора наук <https://tinyurl.com/kubg-phd-pro>; правила призначення і виплати стипендій в Університеті <https://tinyurl.com/styp-phd>; стипендіальну комісію Університету <https://tinyurl.com/styp-kom>; порядок використання коштів, передбачених для надання матеріальної допомоги та преміювання студентів <https://tinyurl.com/prem-asp>

З усіх питань, що стосуються організації освітнього процесу, здобувачі можуть звертатись до наукового керівника, гаранта ОНП, завідувача кафедри, завідувача аспірантури, докторантури, адміністрації Факультету, Університету. Здобувачі освіти можуть контактувати зі НПП та іншими співробітниками Університету через корпоративну електронну пошту. В перший місяць після прийому на навчання для здобувачів створюються корпоративні електронні скриньки, які одночасно використовуються для доступу до електронного середовища Університету. На сайті Університету є розділ «Аспірантам», що сприяє інформуванню здобувачів.

Інформаційна підтримка аспірантів забезпечується своєчасним і системним наданням необхідної інформації про конференції, проекти, стажування, у т.ч. закордонні, конкурси, різні соціальні заходи та можливість участі в них. Ряд сервісних послуг надає бібліотека Університету, з-поміж яких – тематичний підбір літератури, редагування списків літератури, підбір журналу для публікації, пошук літератури з теми у Scopus та Web of Science, електронна доставка документів, індексування за УДК, МБА (міжбібліотечний абонемент), перевірка на плагіат та ін. Соціальна підтримка здобувачів здійснюється через своєчасну виплату стипендій, можливість отримання матеріальної допомоги (за потреби), безкоштовне користування басейном і тренажерною залом. Діє Положення про соціально-психологічну службу <https://tinyurl.com/kubbg-help> та є можливість звернутися за допомогою до психолога у режимі онлайн.

За результатами анкетування аспіранти високо оцінили рівень задоволеності систематичним і змістовним консультуванням наукових керівників, співпрацею з науковцями Університету, інформаційною підтримкою освітнього процесу, інформуванням щодо можливостей участі у наукових заходах, проектах тощо, ресурсами бібліотеки Університету, доступом до матеріально-технічних та інформаційних ресурсів, необхідних для освітньо-наукової діяльності.

Для з'ясування потреб здобувачів здійснюються опитування, очні чи дистанційні зустрічі, засідання фокус-груп тощо. За час реалізації ОНП здобувачі освіти за підтримкою щодо вирішення їх соціальних проблем не зверталися. Структури факультетів, Університету дозволяють надавати в повному обсязі освітню, організаційну, інформаційну, консультативну та соціальну підтримку здобувачам вищої освіти.

Яким чином ЗВО створює достатні умови для реалізації права на освіту особами з особливими освітніми потребами? Наведіть посилання на конкретні приклади створення таких умов на ОП (якщо такі були)

Збільшення можливостей доступу до здобуття вищої освіти осіб з особливими потребами підтверджено у Стратегіях

розвитку Університету на 2018-2022 рр. (п. 3.2, 6.3, 9.1) та на 2023-2027 рр. (р.5,10). Особливості зарахування на навчання осіб з інвалідністю передбачені у Правилах прийому.

Для потреб здобувачів з інвалідністю пристосована інфраструктура навчальних корпусів, де відбувається освітній процес за ОНП – там облаштовано безбар'єрне освітнє середовище. Навчальний корпус №1 обладнаний ліфтами, пандусами, а у корпусі №2 на кожному поверсі обладнано санітарні кімнати для осіб з інвалідністю, встановлено пандуси та введено в експлуатацію пасажирський ліфт.

На Факультеті психології, соціальної роботи та спеціальної освіти створено Інклюзивний ресурсний центр підтримки студентів з інвалідністю <https://tinyurl.com/kubg-sen-res>, діяльність якого регулюється відповідним Положенням <https://tinyurl.com/kubg-centr> Передбачено надання Центром технічної, психологічної, педагогічної та соціально-педагогічної підтримки. Супровід розпочинається з моменту звернення особи з інвалідністю до Ун-ту та охоплює процеси підготовки до вступу, навчання, працевлаштування.

Веб-сайт Ун-ту адаптовано для людей з особливими освітніми потребами (є можливість збільшити/зменшити шрифт, контрастність). Для незрячих (слабозорих) здобувачів застосовуються усні форми проведення поточних і підсумкових форм контрольних заходів.

Серед аспірантів ОНП, що акредитується, особи з особливими освітніми потребами відсутні.

Яким чином у ЗВО визначено політику та процедури врегулювання конфліктних ситуацій (включаючи пов'язаних із сексуальними домаганнями, дискримінацією та корупцією)? Яким чином забезпечується їх доступність політики та процедур врегулювання для учасників освітнього процесу? Якою є практика їх застосування під час реалізації ОП?

Політику та процедури врегулювання конфліктних ситуацій (у т.ч. пов'язаних із сексуальними домаганнями, дискримінацією) регулюються Положенням про засади запобігання і протидії дискримінації, сексуальним домаганням, булінгу та іншим проявам неетичної поведінки <https://tinyurl.com/kubg-antidis> Положення розроблено задля забезпечення рівних можливостей щодо реалізації прав і свобод усіх співробітників та здобувачів, підтримання в Університеті середовища, вільного від дискримінації, сексуальних домагань, булінгу, приниження честі та гідності особи. Університет не толерує дискримінацію, сексуальні домагання, булінг, приниження честі та гідності людини у будь-якій формі, оскільки це суперечить законодавству України, Статуту, Кодексу корпоративної культури, не відповідає місії, цінностям Університету.

У Положенні описано: обов'язки співробітників і здобувачів освіти; процедуру повідомлення про дискримінацію, сексуальні домагання, булінг та інші прояви неетичної поведінки; процедуру розгляду скарг.

Розгляд відповідних скарг здійснюється Комісією з етики, персональний склад якої затверджується наказом ректора <https://tinyurl.com/kubg-ethcom> Скарги, подані здобувачами та стосовно здобувачів, розглядаються розширеним складом Комісії з етики за участю представників з числа здобувачів освіти.

Доступність політик і процедур щодо врегулювання конфліктних ситуацій (у т.ч. випадки дискримінації, сексуальних домагань або корупції) забезпечується за рахунок розміщення інформації щодо основних заходів запобігання та способів сповіщення про такі ситуації на сайті ЗВО.

У питаннях протидії корупції Університет керується Законом України «Про запобігання корупції». На офіційному веб-сайті Університету розміщена інформація щодо основних заходів, спрямованих на запобігання, виявлення та протидії корупції <https://tinyurl.com/kubg-diskr> До відома співробітників та здобувачів освіти доведено інформацію щодо способу повідомлення про прояви корупції в Університеті.

Університет є учасником проекту «Антикорупційний комплаєнс у вищій освіті: закордонний досвід і національна практика», в рамках якого робоча група Університету, за підтримки експертів, проведе оцінювання корупційних ризиків та розробить антикорупційну програму Університету (березень-грудень 2023 р.).

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

Положенням про підготовку здобувачів вищої освіти ступеня доктора філософії та доктора наук в Університеті (п.2.10) передбачено шляхи вирішення потенційних конфліктів між аспірантом і науковим керівником. У разі виникнення такої конфліктної ситуації письмову заяву аспіранта або наукового керівника, з огляду на характер конфлікту, розглядає Комісія з етики Університету або Комісія з питань академічної доброчесності Факультету/ Університету, чи комісія, до складу якої можуть входити гарант ОНП, завідувач кафедри, декан Факультету, завідувач аспірантури, докторантури, проректор з наукової роботи.

8. Внутрішнє забезпечення якості освітньої програми

Яким документом ЗВО регулюються процедури розроблення, затвердження, моніторингу та періодичного перегляду ОП? Наведіть посилання на цей документ, оприлюднений у відкритому доступі в мережі Інтернет

Процедури розроблення, затвердження, моніторингу та періодичного перегляду ОП регулюються Методичними рекомендаціями з розроблення та оновлення освітніх програм (нова редакція), затвердженими рішенням Вченої ради Університету від 09.06.2021 (протокол №5) та введеними в дію наказом від 09.06.2021 №406 <https://tinyurl.com/kubg-rozrobka-op>

Опишіть, яким чином та з якою періодичністю відбувається перегляд ОП? Які зміни були внесені до ОП за результатами останнього перегляду, чим вони були обґрунтовані?

Моніторинг освітніх програм є важливою складовою системи внутрішнього забезпечення якості вищої освіти Університету. Розробку, впровадження та реалізацію ОНП здійснюють відповідні робочі групи. Їхні функції

визначено у п. 2.7 Методичних рекомендацій з розроблення освітніх програм <https://tinyurl.com/kubg-rozrobka-op>. Перегляд та оновлення ОНП відбувається з урахуванням: моніторингу якості надання освітніх послуг; опитувань здобувачів та випускників, НПП, роботодавців та інших стейкхолдерів щодо актуальності, якості освітньої програми, її реалізації, змістового наповнення тощо; вимог стандартів вищої освіти; результатів акредитації та відповідно до наданих експертами рекомендацій; Стратегії (Програми) розвитку Університету тощо. Внесення змін до навчального плану ОНП в частині уточнення назв освітніх компонентів, структурно-логічної схеми навчання, форм контролю відбувається за обґрунтованим поданням робочої групи, погодженим із завідувачем аспірантури, докторантури. Рішення про затвердження відповідних змін в описі ОНП та навчальному плані приймається вченими радами факультетів. Внесені зміни оформлюються окремим додатком і є невід'ємною складовою ОНП. ОНП започатковано у 2019 р. Перший перегляд ОНП відбувся у 2020 р. Під час перегляду уточнено загальну інформацію про ОНП, зокрема рівень відповідності Національній рамці кваліфікацій в описі ОНП з 9 на 8 рівень згідно постанови Кабінету Міністрів України від 23.11.2011 №1341 (зі змінами); перерозподілено кредити між ОК для посилення практичної складової ОНП (збільшення обсягу кредитів на науково-викладацьку практику з метою підготовки здобувачів до викладацької діяльності).

При оновленні ОНП у 2022 р. враховано лист Національного агентства від 03.09.2021 №672 «Про забезпечення володіння випускниками освітньо-наукових програм доктора філософії методологією педагогічної діяльності», п. 25 Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у ЗВО (наукових установах), затвердженого Постановою Кабінету Міністрів від 23.03.2016 №261 (зі змінами)) та Методичні рекомендації з розроблення та оновлення ОП (нова редакція) Київського університету імені Бориса Грінченка від 09.06.2021 № 406.

Провівши консультації, робочі наради, засідання, врахувавши відгуки стейкхолдерів, внесено зміни, уточнення та доповнення до ОНП, які стосуються: уточнення загальної інформації про ОНП; уточнення назв окремих ОК та оптимізації їх структури відповідно до сучасного стану галузі і спеціальності (у блок обов'язкових компонентів ОНП введено навчальну дисципліну «Педагогіка і психологія вищої школи»); перерозподілу кредитів між освітніми компонентами для посилення теоретико-методологічної складової викладацької діяльності.

Наприкінці 2022–2023 н.р. з'явиться можливість отримати думку випускників цієї ОНП, які завершать повний цикл навчання в аспірантурі.

Продемонструйте, із посиланням на конкретні приклади, як здобувачі вищої освіти залучені до процесу періодичного перегляду ОП та інших процедур забезпечення її якості, а їх позиція береться до уваги під час перегляду ОП

З ОНП та РПНД можуть вільно ознайомитись усі бажаючі на сайті Університету в розділі «Аспірантам». Вступники – під час вибору ОНП, здобувачі – у ході навчання.

Пропозиції здобувачів щодо ОНП збираються в ході освітнього процесу через спілкування з гарантом програми, НПП, адміністрацією, під час семінарів, круглих столів, конференцій, опитувань, які проводять Факультет та Докторська школа Університету.

Позиція аспірантів враховується під час проведення звітів, опитувань тощо. Зокрема, аналіз думок здобувачів щодо якості викладання здійснюється шляхом проведення опитування «Викладач очима студентів», щорічного анкетування для здобувачів ступеня доктора філософії щодо задоволеності змістом та організацією освітньо-наукової підготовки; на веб-сторінці «Обговорення ОНП, змін до ОНП» <https://tinyurl.com/obgovor> здобувачам надано можливість надсилати свої зауваження та пропозиції.

Результати проведених обговорень ОНП зі здобувачами представлено на веб-сторінці кафедри <https://tinyurl.com/5cszthzh>, <https://tinyurl.com/2xvx8rh2>.

До робочої групи з розробки нової редакції ОНП у 2022 р. увійшов здобувач Ворохоб М.В.

З метою вдосконалення змісту ОК щороку переглядаються РПНД і, за потреби, до них вносяться зміни або уточнення з урахуванням пропозицій здобувачів озвучених на звітах, при опитуваннях тощо, які попередньо обговорюються та затверджуються на засіданнях кафедр.

Членами Вчених рад Університету та Факультету є аспіранти, які беруть участь у затвердженні ОНП.

Яким чином студентське самоврядування бере участь у процедурах внутрішнього забезпечення якості ОП

Відповідно до Закону України «Про вищу освіту» здобувачі вищої освіти ступеня доктора філософії входять до складу Наукового товариства студентів, аспірантів, докторантів і молодих учених (НТ), яке діє на різних рівнях – факультету та Університету – відповідно до Положення <https://tinyurl.com/kubg-NTSADMV>. Мета діяльності НТ – створення сприятливих умов для науково-дослідної роботи та інноваційної діяльності студентів, аспірантів, докторантів і молодих вчених Університету, об'єднання їхніх зусиль для вирішення актуальних проблем сучасної науки. НТ сприяє підвищенню якості наукових досліджень та проектної діяльності студентів, аспірантів, докторантів і молодих вчених Університету; розвитку співпраці з вітчизняними та зарубіжними ЗВО, науковими установами, державними й недержавними організаціями; діяльності наукових гуртків, лабораторій, центрів. НТ проводить заходи різних рівнів. За погодженням з НТ приймається рішення про відрахування чи поновлення на навчання осіб, які здобувають ступінь доктора філософії.

До вчених рад усіх факультетів входять голови НТ відповідних підрозділів. До ВР Університету – голова НТ ЗВО та виборний представник з числа аспірантів та докторантів Університету, який таємно обирається Конференцією членів (делегатів) НТ Університету. Це представництво дає змогу репрезентувати інтереси аспірантів ЗВО та брати участь у процесі затвердження нових чи перегляду існуючих ОНП.

Продемонструйте, із посиланням на конкретні приклади, як роботодавці безпосередньо або через свої об'єднання залучені до процесу періодичного перегляду ОП та інших процедур забезпечення її

якості

Представники роботодавців були залучені до процесу розробки ОНП шляхом рецензування опису освітньої програми та навчального плану. Рецензентами постали компетентні вчені: 2019 р. – доктор технічних наук, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка Толюпа С.В., кандидат технічних наук, директор Департаменту з інформаційної безпеки ДП «НЕК «Укренерго» Ермошин В.В.; 2022р. – доктор технічних наук, професор, завідувач кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій Київського національного університету імені Тараса Шевченка Лукова-Чуйко Н.В., доктор технічних наук, професор, професор кафедри захисту інформації Національного університету «Львівська політехніка Опірський І.Р., доктор технічних наук, доцент, завідувач відділу «Інтегровані автоматизовані системи спеціального призначення» Інституту проблем математичних машин і систем Національної академії наук України Бегун В.В.

Роботодавці зазначили, що програма підготовки здобувачів є цілісною, науково-практичною, компетентнісно орієнтованою, відображає сучасні тенденції розвитку галузі, сприятиме науковому зростанню здобувачів.

Опишіть практику збирання та врахування інформації щодо кар'єрного шляху та траєкторій працевлаштування випускників ОП

В Університеті діє система моніторингу розвитку кар'єри, покликана стати дієвим елементом моделі оцінки ефективної підготовки майбутніх фахівців. Координацію збирання інформації щодо кар'єрного шляху випускників здійснює відділ практики та працевлаштування НМЦ стандартизації та якості освіти. Сторінка «Випускникам» <https://tinyurl.com/4eunbx9j> на сайті Факультету містить інформацію про діяльність Ради випускників. Здобувачі ОНП мають вищу освіту та, здебільшого, місце роботи. До прикладу, аспірантка Цирканюк Д.А. займає посаду адміністратора відділу адміністрування систем інформаційної безпеки департаменту безпеки ІТ дирекції інформаційних технологій Акціонерного товариства «Укртелеком», аспірантка Дмитрієнко К.А. займає посаду провідного інженера відділу технічного захисту інформації центру інформаційних систем та захисту інформації Національного центру управління та випробувань космічних засобів. Ця інформація фіксується при вступі до аспірантури. Кар'єрний шлях здобувачів впродовж навчання відстежують гарант програми та наукові керівники. Після першого випуску планується створення інформаційної бази випускників за ОНП, відслідковування працевлаштування, підтримання контактів з метою залучення випускників до процедур оновлення ОНП.

Які недоліки в ОП та/або освітній діяльності з реалізації ОП були виявлені у ході здійснення процедур внутрішнього забезпечення якості за час її реалізації? Яким чином система забезпечення якості ЗВО відреагувала на ці недоліки?

У ході здійснення процедур внутрішнього забезпечення якості освіти за час реалізації ОНП суттєвих недоліків не виявлено. Моніторинг задоволеності здобувачами вищої освіти ОНП виявив достатній рівень їхньої задоволеності ОНП у контексті як освітньої, так і наукової складових.

У ході здійснення процедур внутрішнього забезпечення якості за час реалізації ОНП було виявлено необґрунтований розподіл аудиторних годин за видами в ОК. Також окремі недоліки було виявлено та усунуто в робочих програмах навчальних дисциплін: нечіткість критеріїв оцінювання завдань для проміжного контролю, неоновлені переліки джерел для опрацювання. Загалом ОНП орієнтована на навчання, побудоване на дослідженнях, із реалізацією наукових знань про сучасні теорії та методи дослідження у власній професійній діяльності. Планове проведення моніторингів задоволеності здобувачами всіма компонентами ОНП забезпечує можливість адекватного реагування на недоліки.

Враховуючи зміни, що відбулися в системі підготовки здобувачів наукового ступеня (нововведення у підготовці в аспірантурі, зміна процедури захисту дисертації у разових спецрадах та вимог до опублікування результатів дисертацій, підвищення вимог до якості наукових досліджень, у т.ч. через дотримання принципів академічної доброчесності), кафедрою та науковими керівниками ведеться постійна робота з підготовки здобувачів до виконання ними цих нововведень.

Актуальним питанням реалізації ОНП залишається необхідність поглиблення у програмі аспекту інтернаціоналізації, а саме: академічна мобільність та участь у міжнародних науково-дослідних проектах. Укладено угоди, які передбачають академічну мобільність із зарубіжними університетами, зокрема, Університетом Тойо <http://surl.li/fzpzp>, Вроцлавським університетом, Сілезьким університетом <http://surl.li/fzqae>, у т.ч. в межах програми Еразмус+КА1.

Підсумки реалізації ОНП «Інформаційна безпека держави» будуть здійснені після першого випуску здобувачів. Виявлені моменти, які потребуватимуть усунення, будуть розглянуті на засіданнях кафедри, вчених радах Факультету інформаційних технологій та математики із залученням усіх зацікавлених сторін і враховані у подальшій роботі зі здобувачами.

Продемонструйте, що результати зовнішнього забезпечення якості вищої освіти беруться до уваги під час удосконалення ОП. Яким чином зауваження та пропозиції з останньої акредитації та акредитацій інших ОП були враховані під час удосконалення цієї ОП?

Акредитація цієї ОНП є первинною, проте у 2019-2022 рр. в Університеті було акредитовано 36 ОП різних рівнів вищої освіти, з яких 10 ОНП третього (освітньо-наукового) рівня у 2020-2021 н.р. Звіти експертних груп та висновки галузевих експертних рад Національного агентства із забезпечення якості вищої освіти аналізувались та обговорювались на кафедрах та вчених радах Інститутів/Факультетів, відповідальних за реалізацію програм, що акредитувались, та на рівні ректорату. 21.10.2021 було проведено координаційну нараду гарантів ОП всіх рівнів вищої освіти, присвячену результатам акредитацій ОП та ОНП, обговоренню зауважень та рекомендацій експертів, їх врахуванню в освітньому процесі та наступних акредитаціях <https://cutt.ly/qUxGRLp>. 16.02.2023 відбувся онлайн вебінар для гарантів ОП «Забезпечення якості вищої освіти: погляд експертів Національного агентства із

забезпечення якості вищої освіти», на якому були розглянуті особливості роботи ЕГ під час акредитаційної експертизи у ЗВО, порядок розгляду та особливості аналізу акредитаційної справи ГЕР, важливість процедур внутрішнього і зовнішнього забезпечення якості вищої освіти, формування культури якості в ЗВО, порядок прийняття остаточного рішення про акредитацію Національним агентством <https://cutt.ly/d4tS9ky>. Щодо врахованих рекомендацій: на інституційному рівні до уваги були взяті рекомендації експертів щодо уточнення процедур моніторингу, перегляду та оновлення ОП в Університеті. Рішенням ВРУ: від 29.04.2021 (протокол №4) затверджено «Положення про опитування в Університеті» <https://cutt.ly/9UvQjXOBPU>; від 09.06.2021 (протокол №5) затверджено нову редакцію Методичних рекомендацій з розроблення та оновлення ОП, в якій вдосконалено процедуру перегляду та оновлення ОП <https://cutt.ly/RUvQsNN>. Провівши консультації, робочі наради, засідання, врахувавши лист Національного агентства від 03.09.2021 №672 «Про забезпечення володіння випускниками ОНП доктора філософії методологією педагогічної діяльності», відгуки стейкхолдерів, результати проведених опитувань, а також чинники, які виявилися у процесі реалізації ОНП, у нову редакцію ОНП 2022 р. було внесено зміни, уточнення та доповнення до ОНП, які стосуються:

- включення (за згодою) здобувача ОНП та представника роботодавців до складу робочої групи;
- уточнення назв окремих ОК та оптимізації їх структури відповідно до сучасного стану галузі і спеціальності й перерозподілу кредитів між ОК (зокрема, у блок обов'язкових компонентів ОНП введено навчальну дисципліну «Педагогіка і психологія вищої школи»).

Окрім того, систематичним стало проведення щорічного опитування для здобувачів третього (освітньо-наукового) рівня з метою дослідження рівня задоволеності аспірантами змістом та організацією освітньо-наукової підготовки; на вебсторінці Факультету створено рубрику «Підготовка докторів філософії» задля вдосконалення інформування здобувачів про нормативно-правову базу, ОНП, РПНД тощо.

Опишіть, яким чином учасники академічної спільноти змістовно залучені до процедур внутрішнього забезпечення якості ОП?

Ун-ет активно запроваджує культуру якості освіти в акад. середовищі через роз'яснювальну роботу, просвітницькі заходи, систему морального та матеріал. заохочення тощо. Учасники акад. спільноти залучені до процедур внутр. забезпечення якості вищої освіти у різний спосіб, зокрема вони:

- беруть участь в обговоренні питань ЗЯО і процедури їх реалізації;
- підвищують власний професійний рівень, пед. майстерність та наукову кваліфікацію;
- дотримуються норм акад. доброчесності, пед. етики і моралі;
- розвивають у здобувачів вищої освіти самостійність, ініціативність, творчі здібності;
- формують в аспірантів критичне мислення, креативність, ініціативність і підприємливість, навички самопізнання, самоусвідомлення самоосвіти тощо.

Представники акад. спільноти системно долучені до розробки, перегляду та рецензування ОНП. Проводиться робота щодо ознайомлення учасників акад. спільноти з новими тенденціями через різноманітні заходи. Аспірантам викладалися модулі «Якість вищої освіти та експертний супровід її забезпечення: рух України до ЄС», «Університетська автономія у розвитку демократичних цінностей у вищій освіті: досвід країн ЄС для України» у рамках Програми ЄС Еразмус+: Жан Моне. Студентським Парламентом розроблено анонімну гугл-форму для зв'язку зі здобувачами Ун-ту з можливістю описати наявні проблеми пов'язані з освітнім процесом в Ун-ті. Форму було розміщено в соціальних мережах органів студ. самоврядування <https://tinyurl.com/kubg-st-parl>, а також на сайті Факультету <http://surl.li/fzpyk>.

Опишіть розподіл відповідальності між різними структурними підрозділами ЗВО у контексті здійснення процесів і процедур внутрішнього забезпечення якості освіти

Здійснення процесів і процедур внутрішнього забезпечення якості освіти (ЗЯО) в Університеті складає цілісну багатокомпонентну систему і провадиться на двох рівнях.

На первинному рівні внутрішнє ЗЯО здійснюють члени робочої групи, які відповідають за розроблення, перегляд та оновлення змісту ОНП, та група її забезпечення, члени якої особисто беруть участь в освітньому процесі і відповідають за виконання ОНП. Цей рівень координує та контролює гарант ОНП, який безпосередньо відповідає за здійснення процесів і процедур внутрішнього забезпечення якості освіти. До цього рівня долучаються завідувач кафедри, декан факультету та його заступники.

На вторинному рівні моніторинг якості освіти здійснюють проректор з наукової роботи, проректор з науково-методичної та навчальної роботи, проректор з міжнародної діяльності (у їх підпорядкуванні свою діяльність здійснюють Докторська школа; НМЦ досліджень, наукових проектів та програм; НМЦ стандартизації та якості освіти; НМЦ акредитації та ліцензування; НДЛ інтернаціоналізації вищої освіти).

Так, на первинному рівні на чолі з гарантом забезпечуються організація та реалізація процесів і процедур внутрішнього забезпечення якості освіти, а на вторинному здійснюється координація, загальне керівництво, контроль внутрішнього ЗЯО, що забезпечує продуктивність реалізації ОНП.

9. Прозорість і публічність

Якими документами ЗВО регулюється права та обов'язки усіх учасників освітнього процесу? Яким чином забезпечується їх доступність для учасників освітнього процесу?

Права та обов'язки учасників освітнього процесу в Університеті регулюються документами, розробленими з урахуванням вимог чинного законодавства, які розміщені на сайті ЗВО:

Статут Університету <https://tinyurl.com/kubg-statut>

Правила внутрішнього розпорядку <https://tinyurl.com/kubg-rules>

Кодекс корпоративної культури <https://tinyurl.com/kodeks-korp>

Корпоративна угода про участь у розбудові Університету <https://tinyurl.com/KUBG-korp-agree>

Положення про організацію освітнього процесу <https://tinyurl.com/kubg-edu-proc>

Положення про підготовку здобувачів вищої освіти ступеня доктора філософії та доктора наук <https://tinyurl.com/kubg-phd-pro>

Положення про ректорат <https://tinyurl.com/kubg-rector>

Положення про кафедру <https://tinyurl.com/kubg-depar>

Положення про порядок реалізації права на академічну мобільність учасників освітнього процесу <https://tinyurl.com/kubg-mob-rul22>

Положення про академічну доброчесність НПП, НП, ПП та здобувачів освіти Університету <https://tinyurl.com/kubg-integrity>

Договори про підготовку здобувачів вищої освіти ступенів доктора філософії та докторів наук <https://tinyurl.com/agre2022>

Решта документів, якими регулюється права та обов'язки усіх учасників освітнього процесу, своєчасно оприлюднюються на сайті Університету в Реєстрі нормативної бази <https://tinyurl.com/kubg-norm> Залежно від мети та змісту документів вони проходять обговорення та затвердження на вчених радах факультетів, Університету, на Конференції трудового колективу тощо.

Наведіть посилання на веб-сторінку, яка містить інформацію про оприлюднення на офіційному веб-сайті ЗВО відповідного проекту з метою отримання зауважень та пропозиції заінтересованих сторін (стейкхолдерів). Адреса веб-сторінки

На етапі розробки проект ОНП не оприлюднювався на офіційному веб-сайті ЗВО, оскільки не було такої вимоги. Вже при перегляді ОНП у 2019/2020 н.р. та затвердженні нової редакції ОНП у 2021/2022 н.р. було оприлюднено зміни до ОНП на офіційному веб-сайті Університету та надано можливість усім заінтересованим сторонам (стейкхолдерам) надсилати зауваження та пропозиції щодо змін до ОНП/проекту опису ОНП на електронну пошту гаранта програми <https://tinyurl.com/kubg-obgov>

Наведіть посилання на оприлюднену у відкритому доступі в мережі Інтернет інформацію про освітню програму (включаючи її цілі, очікувані результати навчання та компоненти)

<https://tinyurl.com/5ce4ej68>

10. Навчання через дослідження

Продемонструйте, що зміст освітньо-наукової програми відповідає науковим інтересам аспірантів (ад'юнктів)

Наукові інтереси аспірантів пов'язані з можливістю реалізовувати дослідження з обраної теми, вивчати дисципліни, що дають змогу вирішувати науково-дослідницькі завдання в галузі, сприяють розвитку наукового світогляду та забезпечують можливість представляти наукові результати в Україні і за кордоном.

Обов'язкові освітні компоненти ОНП, спрямовані на здобуття фахових компетентностей (ред. 2019):

«Інформаційно-аналітичні процеси в системах безпеки державних інформаційних ресурсів», «Прикладні аспекти створення та застосування систем технічного захисту», «Прикладні аспекти створення та застосування систем криптографічного захисту», «Прикладні аспекти теорій ризиків, конфліктів і катастроф в системах безпеки»

відповідають науковим інтересам і тематиці досліджень аспірантів.

Вибіркові ОК зорієнтовані на якісне вирішення аспірантом науково-дослідницьких завдань у галузі кібербезпеки,

відповідають науковим інтересам і тематиці досліджень аспірантів.

Розвитку системного наукового світогляду сприяють обов'язкові дисципліни: «Філософія і методологія наукової діяльності» та «Стратегії наукових досліджень».

ОНП передбачає проходження аспірантами науково-викладацької та дослідницької практик, що є складовою фахової підготовки.

Відповідний рівень комунікації в міжнародному науковому просторі забезпечується дисципліною «Наукова комунікація іноземною мовою» (8 кредитів).

Теми дисертацій затверджуються Вченою радою ЗВО і розміщуються на сайті у розділі «Аспірантам»

<http://surl.li/fxffi>

Опишіть, яким чином зміст освітньо-наукової програми забезпечує повноцінну підготовку здобувачів вищої освіти до дослідницької діяльності за спеціальністю та/або галуззю

Належна підготовка аспірантів до дослідницької діяльності у галузі передбачає обізнаність із широким колом питань і дисциплін, які вибудовують теоретичне підґрунтя для їхньої аналітичної роботи та навчають правильно моделювати процес дослідження з теми дисертації. Відповідні компетентності формуються у процесі вивчення обов'язкових дисциплін «Філософія і методологія наукової діяльності» та «Стратегії наукових досліджень» – 10 кредитів ECTS.

Для того, щоб методично грамотно будувати дослідницьку роботу, аспірант не може оминати питання розвитку

наукової галузі, до якої дотична його дисертація, та науково-дослідницької інфраструктури (модуль ОК2 «Сучасні технології інформаційної і кібербезпеки та захисту інформації»).

Обов'язкове проходження аспірантами науково-викладацької та дослідницької практик також спрямовано на підготовку здобувачів до дослідницької діяльності в галузі за спеціальністю, що в сукупності становить 6 кредитів за ОНП 2019 р. та 8 кредитів за ОНП 2022 р.

Окрім цього, аспірант, відповідно до своїх наукових інтересів, обирає освітні компоненти (19 кредитів за ОНП 2019 р. та 18 кредитів за ОНП 2022 р.), які готують до дослідницької діяльності зі спеціальності.

Отже, переважна частина обсягу ОНП спрямована на підготовку аспірантів до дослідницької діяльності у галузі.

Опишіть, яким чином зміст освітньо-наукової програми забезпечує повноцінну підготовку здобувачів вищої освіти до викладацької діяльності у закладах вищої освіти за спеціальністю та/або галузю

Для підготовки аспірантів до викладацької діяльності ОНП містить ряд освітніх компонентів. Зокрема, змістовий модуль «Нормативно-правова база наукових досліджень та наукової діяльності» дисципліни «Стратегії наукових досліджень» забезпечує формування нормативно-правової компетентності у сфері освітньої взаємодії; «Наукова комунікація іноземною мовою» уможливує доступ аспірантів до закордонних науково-методичних напрацювань; змістові модулі «Загальнонаукова методологія» та «Наукова етика» спрямовані на вироблення науково-фахового світогляду і підвищення науково-педагогічної культури відповідно; «Педагогіка і психологія вищої школи» спрямована на посилення теоретико-методологічної складової викладацької діяльності.

Поглиблення фахових, методичних компетентностей, сформованих під час вивчення зазначених освітніх компонентів, з акцентом на прикладному застосуванні забезпечує «Науково-викладацька практика». Критеріями якості підготовки здобувачів вищої освіти до викладацької діяльності за спеціальністю є сформовані результати навчання.

Зазначені освітні компоненти та кількість кредитів, передбачені на них, засвідчує забезпечення змістом ОНП належної підготовки аспірантів до викладацької діяльності.

Продемонструйте дотичність тем наукових досліджень аспірантів (ад'юнктів) напрямом досліджень наукових керівників

Вступник на обов'язковому вступному випробуванні презентує власні дослідницькі пропозиції чи досягнення. Здійснюється аналіз дотичності його наукових інтересів та потенційного керівника. Тема здобувача затверджується згідно з Положенням про підготовку докторів філософії. Про напрями досліджень керівника можна дізнатися у його е-портфоліо, з інформації на сайті ЗВО, переглянувши публікації у відкритому доступі. Частина аспірантів почали співпрацю з потенційними керівниками ще навчаючись на попередніх рівнях вищої освіти в Університеті Грінченка. Теми наукових досліджень аспірантів <http://surl.li/xfffi> дотичні до напрямів досліджень наукових керівників. Так, тема дисертації Абрамова С.В. «Моделі та методи підвищення швидкодії алгоритму CSIDH на основі суперсингулярних скручених кривих Едвардса» відповідає дослідженням наукового керівника Бессалова А.В. («Calculation of Isogenies of Odd Degrees of Supersingular Twisted Edwards Curves»). Тема дисертації Іосіфова Є.А. «Методи і засоби забезпечення безпечного розпізнавання та параметризації результатів обробки голосової інформації» відповідає дослідженням наукового керівника Соколова В.Ю. («Prototyping Methodology of End-to-End Speech Analytics Software»). Участь керівників у реалізації теми кафедри «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» забезпечує дотичність до неї і тем аспірантів.

Опишіть з посиланням на конкретні приклади, як ЗВО організаційно та матеріально забезпечує в межах освітньо-наукової програми можливості для проведення і апробації результатів наукових досліджень аспірантів (ад'юнктів)

У межах ОНП для реалізації досліджень та апробації їх результатів Університет надає аспірантам можливості: брати участь у наукових заходах («Cybersecurity Providing in Information and Telecommunication Systems», «International Conference on Computer Science, Engineering and Education», «Modern Machine Learning Technologies Workshop», «IEEE International Conference on Problems of Infocommunications. Science and Technology»), у яких здобувачі можуть апробувати результати досліджень;

публікувати результати досліджень у науковому виданні Університету «Кібербезпека: освіта, наука, техніка»

<https://csecurity.kubg.edu.ua/index.php/journal> □ науковому фаховому виданні МОН України категорії «Б»;

оперативно ознайомлюватись на веб-сайті ЗВО із новими надходженнями до бібліотеки, доробками викладачів, анонсами семінарів, тренінгів ін.;

двічі на рік звітувати про свою роботу на засіданнях кафедри, що дозволяє ширше досягнути перспективи дослідження;

безкоштовно користуватися міжнародними базами Scopus і Web of Science, журналами вид-ва Wiley, ресурсами Springer Link, бібліотечним фондом Університету, Інституційним репозиторієм; науково-дослідними надбаннями кафедри; хмарними сервісами Microsoft; доступом до інтернет-мережі в Університеті.

Проаналізуйте, як ЗВО забезпечує можливості для долучення аспірантів (ад'юнктів) до міжнародної академічної спільноти за спеціальністю, наведіть конкретні проекти та заходи

В Університеті створено умови для долучення аспірантів до міжнародної академічної спільноти, зокрема через реалізацію права на академічну мобільність, що регламентується Положенням про порядок реалізації права на академічну мобільність <https://tinyurl.com/kubg-mob-rul22>

Аспіранти ОНП були учасниками програми ЄС Еразмус+, напрям Жан Моне – слухачами модулів «Якість вищої

освіти та експертний супровід її забезпечення: рух України до ЄС» <https://tinyurl.com/tgecgad>, «Державне – міжнародне – суспільне: європейські цінності» <http://stipendium.kubg.edu.ua/>, є учасниками модуля «Університетська автономія у розвитку демократичних цінностей у вищій освіті: досвід країн ЄС для України» <https://uaddvhe.kubg.edu.ua/>.

Інформація про проекти та можливості поширюється через веб-сторінку НДЛ ІВО <http://ivo.kubg.edu.ua/>. У рамках модуля «Інтернаціоналізація науки» здобувачі дізнаються про можливості отримання грантів тощо.

Інструментами долучення здобувачів до міжнародної академічної спільноти є публікації у закордонних наукових виданнях, участь у заходах за кордоном.

Здобувачі Іосіфов Є. А., Сукайло І.О., Цирканюк Д.А. беруть участь у міжнародному проекті «Research of Natural Language Processing» за грантом №43-070121 від Ender Turing OÜ (Таллін, Естонія).

Опишіть участь наукових керівників аспірантів у дослідницьких проектах, результати яких регулярно публікуються та/або практично впроваджуються

Наукові керівники аспірантів є керівниками та/або виконавцями дослідницьких проектів, науково-дослідних тем. На кафедрі реалізується тема «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури». На підставі договору про співробітництво між Університетом та Інститутом програмних систем НАН України, наукові керівники здобувачів беруть участь у виконанні теми прикладних досліджень «Розроблення та впровадження програмних технологій підтримки прийняття рішень щодо захисту інформаційних систем Національної академії наук України від атак та інцидентів «нульового дня»». За результатами виконання науково-дослідної теми публікуються тези, матеріали доповідей, статті тощо.

Наукові керівники аспірантів беруть участь у таких міжнародних дослідницьких проектах: Складаний П.М., Гулак Г.М., Соколов В.Ю., Коршун Н.В. «Research of Natural Language Processing» (Таллін, Естонія); Складаний П.М., Соколов В.Ю., Коршун Н.В. «Methods for determining the investment attractiveness of Decentralized Autonomous Organisations» (Сінгапур).

Інформація про наукові публікації керівників та участь у проектах розміщена в Інституційному репозиторії <http://elibrary.kubg.edu.ua/> та в е-портфоліо <http://eportfolio.kubg.edu.ua/login/>

Опишіть чинні практики дотримання академічної доброчесності у науковій діяльності наукових керівників та аспірантів (ад'юнктів)

Дотримання АД передбачено Кодексом корпоративної культури Університету. Діє Положення про академічну доброчесність <https://tinyurl.com/kubg-integrity>

Створення постійно діючих комісій з академічної доброчесності передбачено на рівні факультету та Університету <https://tinyurl.com/dobr2023>.

ОНП містить модуль «Наукова етика», заняття щодо АД проводяться під час модулю «Інтернаціоналізація науки». Всі НПП і аспіранти підписують декларацію про академічну доброчесність.

Публікації у періодичних виданнях Університету перевіряються через Unicheck. Дисертації та наукові публікації перевіряються на наявність текстових збігів.

Наукові керівники проводять заходи із попередження порушень АД у науково-дослідній роботі аспірантів, зокрема через інформаційну допомогу для усунення у науковій роботі фрагментарного, споглядального матеріалу, зворотній зв'язок з базами дослідження. Обов'язковою є процедура надання аспірантами достовірної інформації про результати досліджень на всіх етапах його проведення. Важливим є підтвердження достовірності виконання аспірантами завдань у межах ОНП, що реалізується через комунікацію наукового керівника зі здобувачем.

Контроль за дотриманням АД при попередній експертизі дисертації здійснюють завідувач кафедр та рецензенти. При виявленні порушення АД вони зобов'язані повідомити про цей факт наук. керівника і проректора з наук. роботи. Така дисертація не рекомендується до захисту, надається негативний висновок.

Продемонструйте, що ЗВО вживає заходів для виключення можливості здійснення наукового керівництва особами, які вчинили порушення академічної доброчесності

У Університеті контроль за дотриманням НПП норм академічної доброчесності здійснюють завідувачі кафедр, рецензенти різних рівнів, головні редактори наукових видань та їх заступники, голови і вчені секретарі вчених рад підрозділів. У разі виявлення факту порушення АД НПП при рекомендації рукопису до друку на етапі кафедри, рецензенти зобов'язані повідомити про зазначений факт завідувача кафедри; на етапі факультету – голову та вченого секретаря вченої ради факультету; на університетському етапі – голову та вченого секретаря ВР Університету.

НПП підписують декларацію про дотримання академічної доброчесності.

Положенням про академічну доброчесність в Університеті (п.5.2) <https://tinyurl.com/kubg-integrity> передбачено, що за порушення АД НПП, окрім іншого, можуть бути притягнені до позбавлення можливості здійснювати наукове керівництво аспірантами та викладати дисципліни навчального плану підготовки докторів філософії.

Розгляд порушень академічної доброчесності здійснюють постійно діючими комісіями з питань академічної доброчесності факультету, Університету.

Завдяки політиці дотримання академічної доброчесності в Університеті на сьогодні НПП кафедр, які забезпечують підготовку аспірантів на ОНП, не виявлено порушень академічної доброчесності.

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОНП?

Сильні сторони ОНП:

ОНП відповідає тенденціям розвитку спеціальності та ринку праці, враховує галузевий і регіональний контекст, досвід аналогічних вітчизняних та іноземних ОНП; має чітко сформульовані цілі, які визначені з урахуванням позицій і потреб стейкхолдерів та відповідають місії і стратегії Університету. ОНП передбачає практичну підготовку аспірантів та набуття ними необхідних hard skills та soft skills навичок.

ОНП включає складові, передбачені Порядком підготовки здобувачів вищої освіти ступеня доктора філософії та доктора, затвердженого Постановою КМУ №261 від 23.03.2016.

Зміст ОНП відповідає науковим інтересам аспірантів і забезпечує їхню підготовку до дослідницької та викладацької діяльності.

Викладання на ОНП тісно пов'язано з інтернаціоналізацією освіти. Викладачі та аспіранти активно беруть участь у міжнародних стажуваннях та програмах академічної мобільності.

Якісний підхід до представлення навчальних матеріалів у системі Moodle сприяє безперервності ефективного освітнього процесу в кризових умовах пандемії і воєнного стану.

Тематика досліджень аспірантів входить до наукових інтересів наукових керівників.

Залучення аспірантів до участі у наукових заходах.

Дотримання правил і процедур, що регулюють права та обов'язки всіх учасників освітнього процесу у ході реалізації ОНП.

Відпрацювання процедур системного залучення аспірантів до моніторингу якості ОНП.

Правила прийому та правила визнання результатів навчання за ОНП є чіткими, прозорими і зрозумілими. Форми навчання і викладання є студентоцентричними, 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 ОНП в цілому.

Політики, стандарти і процедури дотримання академічної доброчесності за ОНП є чіткими і зрозумілими.

Академічна і професійна кваліфікація НПП, задіяних в реалізації ОНП, забезпечує досягнення визначених програмою цілей та РН. Добір НПП здійснюється на конкурсній основі. До освітнього процесу Університет активно залучає роботодавців.

Наявність унікальної матеріально-технічної бази для забезпечення ОНП.

Водночас, поруч із зазначеними сильними сторонами ОНП, існує низка проблемних питань, вирішення яких сприятиме удосконаленню ОНП:

Варто активізувати участь здобувачів та викладачів у програмах міжнародної академічної мобільності, міжнародних наукових проектах, у т.ч. грантових.

Якими є перспективи розвитку ОП упродовж найближчих 3 років? Які конкретні заходи ЗВО планує здійснити задля реалізації цих перспектив?

Перспективи розвитку ОНП «Інформаційна безпека держави» перш за все пов'язані з очікуванням затвердження стандарту за спеціальністю 125 Кібербезпека для третього (освітньо-наукового) рівня вищої освіти, що буде вимагати створення нової редакції ОНП через приведення ОНП у відповідність до нього.

З метою розвитку ОНП відповідно до вимог сучасного наукового простору плануються наступні заходи:

Найближчою перспективою розвитку ОНП є підготовка першої когорти випускників ОНП до успішного захисту дисертацій за новими вимогами МОНУ та Національного агентства із забезпечення якості вищої освіти.

Розширення міжнародної співпраці та академічної мобільності здобувачів та їх керівників.

Безперервне удосконалення програмного забезпечення і технічного оснащення, збагачення інформаційних ресурсів освітнього процесу.

Актуалізація змісту навчальних дисциплін в ході постійного моніторингу міжнародних та вітчизняних тенденцій підготовки докторів філософії в межах ОНП.

Залучення іноземних фахівців до проведення гостьових лекцій, практичних занять, круглих столів, семінарів.

Популяризація науки та необхідності наукового зростання серед здобувачів другого (магістерського) рівня вищої освіти задля їх подальшого розвитку як компетентних науковців (дослідників) на третьому рівні вищої освіти.

Запевнення

Запевняємо, що уся інформація, наведена у відомостях та доданих до них матеріалах, є достовірною.

Гарантуємо, що ЗВО за запитом експертної групи надасть будь-які документи та додаткову інформацію, яка стосується освітньої програми та/або освітньої діяльності за цією освітньою програмою.

Надаємо згоду на опрацювання та оприлюднення цих відомостей про самооцінювання та усіх доданих до них матеріалів у повному обсязі у відкритому доступі.

Додатки:

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

Таблиця 2. Зведена інформація про викладачів ОП

Таблиця 3. Матриця відповідності програмних результатів навчання, освітніх компонентів, методів навчання та оцінювання

Шляхом підписання цього документа запевняю, що я належним чином уповноважений на здійснення такої дії від імені закладу вищої освіти та за потреби надам документ, який посвідчує ці повноваження.

Документ підписаний кваліфікованим електронним підписом/кваліфікованою електронною печаткою.

Інформація про КЕП

ПІБ: ТУРУНЦЕВ ОЛЕКСАНДР ПЕТРОВИЧ

Дата: 05.04.2023 р.

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

| Назва освітнього компонента | Вид компонента | Силабус або інші навчально-методичні матеріали | | Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього* |
|--|----------------------|--|--|---|
| | | Назва файла | Хеш файла | |
| Прикладні аспекти протидії кібератакам в соціотехнічних системах | навчальна дисципліна | 125_PAPKSS_NP2020.pdf | yNALge987/zYXnDo2Acwo8/R9v6ukYZmWfNQYK37Wfc= | <p>Прикладні аспекти протидії кібератакам в соціотехнічних системах Навчальна дисципліна Коршун Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням електронного навчального курсу у системі e-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. З метою проведення практичних та/або лабораторних занять, експериментальної частини дослідження здобувачам надано доступ до Лабораторії безпеки інформаційних активів:</p> <p>Сервер Dell PE R530 Сервер Dell PE R530 Сервер HP ProLiant КВМ-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 min#1 Dell OptiPlex 3050 Micro Form Factor – 15 шт. Комп'ютер min#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</p> |

| | | | | |
|--|----------------------|--|---|---|
| | | | | <i>NetworkSniffer та EndpointSniffer Контур управління інформаційною безпекою «Digital Security» у складі DS Office та DS LifeCycle Management System.</i> |
| Технології безпеки складних соціотехнічних систем | навчальна дисципліна | <i>125_tbsss_2020.pdf</i> | <i>LjPqz/1iWvuXwvFJ MtCkf+CKob96CMG 9Kx6EkSzzGT0=</i> | <i>Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. З метою проведення практичних та/або лабораторних занять, експериментальної частини дослідження здобувачам надано доступ до Лабораторії безпеки інформаційних активів: Сервер Dell PE R530 Сервер Dell PE R530 Сервер HP ProLiant КВМ-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 «SearchInfort» у складі NetworkSniffer та EndpointSniffer Контур управління інформаційною безпекою «Digital Security» у складі DS Office та DS LifeCycle Management System.</i> |
| Прикладні аспекти управління інформаційною та кібербезпекою об'єктів | навчальна дисципліна | <i>125_PA_upravlinny a_IKB_OKI_NP202 o.pdf</i> | <i>PfvGAFIgaKcQzBMK otHFiVhXz3dqwtqizw kozBoGxFU=</i> | <i>Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне</i> |

критичної
інфраструктури

забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. З метою проведення практичних та/або лабораторних занять, експериментальної частини дослідження здобувачам надано доступ до:

Лабораторії безпеки інформаційних активів:
Сервер Dell PE R530
Сервер Dell PE R530
Сервер HP ProLiant
КВМ-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 min#1 Dell OptiPlex 3050 Micro Form Factor – 15 шт.
Комп'ютер min#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
Контур управління інформаційною безпекою «Digital Security» у складі DS Office та DS LifeCycle Management System.
Лабораторії комп'ютерних мереж:
Комп'ютер min#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. |
|--|----------------------|----------------------|--|--|
| Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів | навчальна дисципліна | 125_zboki_NP2020.pdf | sTYDeFci8m1xYz9Vp1W3cpph6+cJqCl66/lrkNBzP7A= | <p>Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. З метою проведення практичних та/або лабораторних занять, експериментальної частини дослідження здобувачам надано доступ до:</p> <p>Лабораторії безпеки інформаційних активів: Сервер Dell PE R530 Сервер Dell PE R530 Сервер HP ProLiant КВМ-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 min#1 Dell OptiPlex 3050 Micro Form Factor – 15 шт. Комп'ютер min#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 «SearchInfort» у складі NetworkSniffer та EndpointSniffer Контур управління інформаційною безпекою «Digital Security» у складі DS Office та DS LifeCycle Management System. Лабораторії комп'ютерних мереж: Комп'ютер min#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</p> |

| | | | | |
|---|-----------------------------|--|---|--|
| | | | | <p>w/SEC license Інтерфейсна карта Cisco HWIC-2T Комутатори Catalyst 3650 24 Fast 4x1 G Інтерактивна дошка SMART Board.</p> |
| <p>Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем</p> | <p>навчальна дисципліна</p> | <p>125_PA_monit_ta_audyt_ZIKS_NP2020.pdf</p> | <p>22PF6V3MsJm5b0DPLng5hQS2ZWfPuN1fPuUjF/SVnQY=</p> | <p>Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. З метою проведення практичних та/або лабораторних занять, експериментальної частини дослідження здобувачам надано доступ до:</p> <p>Лабораторії безпеки інформаційних активів: Сервер Dell PE R530 Сервер Dell PE R530 Сервер HP ProLiant КВМ-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 min#1 Dell OptiPlex 3050 Micro Form Factor – 15 шт. Комп'ютер min#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 «SearchInfort» у складі NetworkSniffer та EndpointSniffer Контур управління інформаційною безпекою «Digital Security» у складі DS Office та DS LifeCycle Management System. Лабораторії комп'ютерних мереж:</p> |

| | | | | |
|--|-----------------------------|---------------------------|--|---|
| | | | | <p>Комп'ютер min#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.</p> |
| <p>Організація захисту розподілених інформаційних ресурсів</p> | <p>навчальна дисципліна</p> | <p>125_ozrir_2020.pdf</p> | <p>FUoRvZbBoJ+ED5JMDMAiiXtfr13uaqne aCd9BJ8RBMg=</p> | <p>Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. З метою проведення практичних та/або лабораторних занять, експериментальної частини дослідження здобувачам надано доступ до:</p> <p>Лабораторії безпеки інформаційних активів: Сервер Dell PE R530 Сервер Dell PE R530 Сервер HP ProLiant КВМ-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 min#1 Dell OptiPlex 3050 Micro Form Factor – 15 шт. Комп'ютер min#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 «SearchInfort» у складі NetworkSniffer та EndpointSniffer Контур управління</p> |

| | | | | |
|---|-----------------------------|---------------------------------|---|--|
| | | | | <p>інформаційною безпекою «Digital Security» у складі DS Office та DS LifeCycle Management System. Лабораторії комп'ютерних мереж: Комп'ютер min#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.</p> |
| <p>Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем</p> | <p>навчальна дисципліна</p> | <p>125_PAAEZIKS_NP2 020.pdf</p> | <p>2ofXklEyQE7P6qN8 hQgwctG6enTDQb74 zRD8I51/Ydw=</p> | <p>Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. З метою проведення практичних та/або лабораторних занять, експериментальної частини дослідження здобувачам надано доступ до: Лабораторії безпеки інформаційних активів: Сервер Dell PE R530 Сервер Dell PE R530 Сервер HP ProLiant КВМ-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 min#1 Dell OptiPlex 3050 Micro Form Factor – 15 шт. Комп'ютер min#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</p> |

| | | | | |
|--|----------------------|---------------------|--|---|
| | | | | <p>Мережеве сховище Internet Download Manager Synology DS718+</p> <p>Контур інформаційної безпеки «SearchInform» у складі NetworkSniffer та EndpointSniffer</p> <p>Контур управління інформаційною безпекою «Digital Security» у складі DS Office та DS LifeCycle Management System.</p> <p>Лабораторії комп'ютерних мереж:</p> <p>Комп'ютер min#1 Intel Core i3 3.0GHz, 4GB RAM, 1000GB HDD, 22" LED. Кількість: 12+1 ПК</p> <p>Міжмережевий екран ASA5506-K8</p> <p>Комутатор WS-C2960+24TC-L</p> <p>Роутер Cisco ISR 4321 Sec bundle w/SEC license</p> <p>Інтерфейсна карта Cisco HWIC-2T</p> <p>Комутатори Catalyst 3650 24 Fast 4x1 G</p> <p>Інтерактивна дошка SMART Board.</p> |
| Проектування і впровадження захищених інформаційно-комунікаційних систем | навчальна дисципліна | 125_pzviks_2020.pdf | EgIscYkCyY9pYbIoz/rSEfSYSUIзMW9LaE6j4HIObQQ= | <p>Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. З метою проведення практичних та/або лабораторних занять, експериментальної частини дослідження здобувачам надано доступ до:</p> <p>Лабораторії безпеки інформаційних активів:</p> <p>Сервер Dell PE R530 Сервер Dell PE R530</p> <p>Сервер HP ProLiant</p> <p>КВМ-перемикач з підтримкою USB-периферії</p> <p>Міжмережевий екран FG-100E-BDL-EU – 1 шт.</p> <p>Комутатор TP-Link T2600G-52TS</p> <p>Комутатор Mikrotik Cloud Smart Switch CSS326-24G-2S+</p> <p>Маршрутизатор (router) Cisco</p> <p>Точка доступу Cisco</p> <p>Комп'ютер min#1 Dell OptiPlex 3050 Micro Form Factor – 15 шт.</p> <p>Комп'ютер min#2 Dell Precision Tower 3620 XCTO BASE – 1 шт.</p> <p>Дошка магнітна крейдова-маркерна обертова на колесах</p> <p>Точка wi-fi доступу Linksys Cisco SB WAP 121 (WAP 121-E-K9-G5).</p> <p>Екран для проектора настінний Walfix з механізмом повернення 150" (4:3) 300x225 см</p> <p>Проектор на стелю мережевий</p> |

| | | | | |
|---|----------------------|----------------------------------|--|---|
| | | | | <p>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 «SearchInfort» у складі NetworkSniffer та EndpointSniffer Контур управління інформаційною безпекою «Digital Security» у складі DS Office та DS LifeCycle Management System. Лабораторії комп'ютерних мереж: Комп'ютер min#1 Intel Core i3 3.0GHz, 4GB RAM, 1000GB HDD, 22" LED. Кількість: 12+1 ПК Міжмережвий 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.</p> |
| Дослідницька практика | практика | 125-dosl-prakt_2022.pdf | Q/ITdIdUPRYPbOeVK/SOfSX/iGccVQ4U0013RsWIOoI= | Дослідницька практика здійснюється на базі Київського університету імені Бориса Грінченка. |
| Науково-викладацька практика | практика | 125-nauk-vykl-prakt_2022.pdf | iaI2hOgimbMuARoK Fvdgt3uhAk5e2w7eq b2RIU/eXqg= | Науково-викладацька практика здійснюється на базі Київського університету імені Бориса Грінченка. |
| Прикладні аспекти теорій ризиків, конфліктів і катастроф в системах безпеки | навчальна дисципліна | 125_PATRKK_sys_b ezpeky_2020.pdf | MhTsmpphMr8ErB2 oKwOWpQ1roDERU jTHkXEApF6jbWA= | <p>Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. З метою проведення практичних та/або лабораторних занять, експериментальної частини дослідження здобувачам надано доступ до Лабораторії безпеки інформаційних активів: Сервер Dell PE R530 Сервер Dell PE R530 Сервер HP ProLiant КВМ-перемикач з підтримкою USB-периферії Міжмережвий екран FG-100E-BDL-EU – 1 шт. Комутатор TP-Link T2600G-52TS Комутатор Mikrotik Cloud Smart</p> |

Switch CSS326-24G-2S+
 Маршрутизатор (router) Cisco
 Точка доступу Cisco
 Комп'ютер min#1 Dell OptiPlex
 3050 Micro Form Factor – 15 шт.
 Комп'ютер min#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
 Контур управління
 інформаційною безпекою «Digital
 Security» у складі DS Office та DS
 LifeCycle Management System.
 Лабораторії комп'ютерних
 мереж:
 Комп'ютер min#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.

Прикладні аспекти
 створення та
 застосування систем
 криптографічного
 захисту

навчальна
 дисципліна

125_PASZS_krypt_z
 ahystu_NP2020.pdf

xtYkhuO81GVGpdN
 NU2LY5MQPjjQIKR
 BbUgH4k6XEMIo=

Навчальні аудиторії обладнані
 мультимедійним комплексом
 (проектор, SMART-дошка,
 комп'ютер, відповідне програмне
 забезпечення, акустична
 система). Навчання відбувається
 з використанням розробленого
 для дисципліни електронного
 навчального курсу у системі e-
 навчання Університету у
 поєднанні з корпоративним
 Google Meet та/або ліцензованим
 Zoom. Є доступ до
 наукометричних баз Scopus і Web
 of Science (віддалений та з
 локальної мережі), ScienceDirect,
 Research4Life, бази нормативних
 документів БУДСТАНДАРТ
 Online, «Інформаційного ресурсу»
 LIBRARIA™ та Онлайн-
 бібліотеки видавництва «Центр
 учбової літератури»,
 комп'ютеризованої читальної
 зали з бібліотечним фондом.
 З метою проведення практичних
 та/або лабораторних занять,
 експериментальної частини
 дослідження здобувачам надано
 доступ до Лабораторії
 криптографічного захисту
 інформації:
 Ноутбук min#1 Dell Inspiron
 15/500 Series IntelCore i5-8250u
 cpi, 1.8 Ghz, 8 Gb ОЗУ
 Програмно-апаратний комплекс

| | | | | |
|---|----------------------|-----------------------------------|--|---|
| | | | | <p>“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.</p> |
| Прикладні аспекти створення та застосування систем технічного захисту | навчальна дисципліна | 125_PASZS_tech_zahystu_NP2020.pdf | 94f6rAamsDEyZZ8WDc97bZ1/i9E/YQ8/iVD7WH2baHE= | <p>Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. З метою проведення практичних та/або лабораторних занять, експериментальної частини дослідження здобувачам надано доступ до Лабораторії технічного захисту інформації: Детектор (індикатор) поля PROTECT 1210і Детектор (індикатор) поля PROTECT 1206і Скануючий приймач IC-R20 Багатофункціональний пошуковий прилад ST-033 «Піранія» Виявник прихованих відеокамер Антена рамкова жорстка "PIAC-1AJ" Генератор акустичного шуму "PIAC-2ГС" Вібровипромінювач п'єзоелектричний "PIAC-2ВІІ" Випромінювач акустичний "PIAC-2ВА" Квадрокоптер DJI Mavic PRO Контролер Matrix-II Net.</p> |
| Інформаційно-аналітичні процеси в системах безпеки державних інформаційних ресурсів | навчальна дисципліна | 125_IA_protsey_NP2020.pdf | B+r1NGPrkp4VN2JwLWiv6BiCfl74IgToIiVJobEgmXo= | <p>Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web</p> |

of Science (віддаленій та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. З метою проведення практичних та/або лабораторних занять, експериментальної частини дослідження здобувачам надано доступ до:

Лабораторії безпеки інформаційних активів:
Сервер Dell PE R530
Сервер Dell PE R530
Сервер HP ProLiant
КВМ-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 min#1 Dell OptiPlex 3050 Micro Form Factor – 15 шт.
Комп'ютер min#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
Контур управління інформаційною безпекою «Digital Security» у складі DS Office та DS LifeCycle Management System.
Лабораторії комп'ютерних мереж:
Комп'ютер min#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.

Наукова комунікація іноземною мовою (за ОНП 2019, зі змінами 2020)

навчальна дисципліна

Nauk_komunikatsiy a_inozemnoy_movo u_NP2020.pdf

6kHTBJXOfLis5ifsOs 9lh9ORDFnB2FQL8 PBlZKOfb5I=

Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Функціонує лінгафонний комплекс Sanako Lab 90 (інтерактивна дошка SMART

| | | | | |
|--|-----------------------------|--|--|--|
| | | | | <p>Board – 1 шт.; ПК Intel Core 2 Duo, 512 МБ, 230 Гб, – 1шт.; ПЕОМ: Intel Celeron CPU 1.80 GHz., навушники Sven GD- 010 MV – 1шт.). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом.</p> |
| <p>Стратегії наукових досліджень (Сучасні технології інформаційної і кібербезпеки та захисту інформації)</p> | <p>навчальна дисципліна</p> | <p>125_strategii_nauk_doslidzhen_STIKZI_NP2020.pdf</p> | <p>Z7EAvYiz2yaJMNsIoZ5v08jX8n6LpVAoO d10zmgpDZA=</p> | <p>Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. З метою проведення практичних та/або лабораторних занять, експериментальної частини дослідження здобувачам надано доступ до Лабораторії безпеки інформаційних активів: Сервер Dell PE R530 Сервер Dell PE R530 Сервер HP ProLiant КВМ-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 min#1 Dell OptiPlex 3050 Micro Form Factor – 15 шт. Комп'ютер min#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</p> |

| | | | | |
|---|----------------------|--|--|--|
| | | | | <p>(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 Контур управління інформаційною безпекою «Digital Security» у складі DS Office та DS LifeCycle Management System.</p> |
| Системний аналіз та прийняття рішень в інформаційній і кібербезпеці | навчальна дисципліна | 125_syst_analiz_ta_pryinyattya_rish_v_inf_i_kibbezp_NP2022.pdf | JsO6ICGGJdt93Hd25m98MBYKOATM7rffURmKlWaj708= | <p>Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційого ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. З метою проведення практичних та/або лабораторних занять, експериментальної частини дослідження здобувачам надано доступ до Лабораторії вбудованих систем та 3-D моделювання:</p> <p>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</p> <p>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 Display 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 MIO283AV2 Adapter v2 Плата Intel Galileo Плата Altium NanoBoard 3000 Двоколійна демонстраційна модель Formula Flowcode Buggy Макет лабіринту (Maze walls).</p> |
| Наукова комунікація | навчальна | Nauk_komunikatsiy | SMiYBxUbD6SkjflN | Навчальні аудиторії обладнані |

| | | | | |
|--|----------------------|--|---|---|
| іноземною мовою (за ОНП 2022) | дисципліна | <i>a_inozemnou_movo_u_NP2022.pdf</i> | Xx6WWpNwUH5qh UXQORyyCPx2X7c= | мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Функціонує лінгафонний комплекс Sapako Lab 90 (інтерактивна дошка SMART Board – 1 шт.; ПК Intel Core 2 Duo, 512 МБ, 230 Гб, – 1шт.; ПЕОМ: Intel Celeron CPU 1.80 GHz., навушники Sven GD- 010 MV – 1шт.). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. |
| Стратегії наукових досліджень (Інтернаціоналізація науки: Змістовий модуль 2. Інформаційна грамотність; Змістовий модуль 3. Наукові публікації в цифровому середовищі) | навчальна дисципліна | <i>strategii_nauk_dosli_dzhen_Internats_2022.pdf</i> | HdrmWHcFdxA2116 /pbC6Hf4MalEKOT nc51oTvqarOE= | Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. |
| Стратегії наукових досліджень (Інтернаціоналізація науки: Змістовий модуль 1. Основи інтернаціоналізації вищої освіти і науки) | навчальна дисципліна | <i>strategii_nauk_dosli_dzhen_Internats_2022.pdf</i> | HdrmWHcFdxA2116 /pbC6Hf4MalEKOT nc51oTvqarOE= | Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. |

| | | | | |
|--|----------------------|--|--|---|
| Стратегії наукових досліджень (Нормативно-правова база наукових досліджень та наукової діяльності) | навчальна дисципліна | <i>strategii_nauk_doslidzhen_norm_praw_baza_2022.pdf</i> | GsXDzducW99blpLv h7ghprTT26oO9W+I jhPmOhq1QAM= | Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. |
| Філософія і методологія наукової діяльності (Наукова етика) | навчальна дисципліна | <i>fil_zagalnauk_metod_NP2022.pdf</i> | GNPFehw99eiqLHpd K4Ji/mioMAkWqsZC OCZopQgN6MI= | Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. |
| Філософія і методологія наукової діяльності (Філософія науки; Загальнонаукова методологія) | навчальна дисципліна | <i>fil_zagalnauk_metod_NP2022.pdf</i> | GNPFehw99eiqLHpd K4Ji/mioMAkWqsZC OCZopQgN6MI= | Навчальні аудиторії обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер, відповідне програмне забезпечення, акустична система). Навчання відбувається з використанням розробленого для дисципліни електронного навчального курсу у системі е-навчання Університету у поєднанні з корпоративним Google Meet та/або ліцензованим Zoom. Є доступ до наукометричних баз Scopus і Web of Science (віддалений та з локальної мережі), ScienceDirect, Research4Life, бази нормативних документів БУДСТАНДАРТ Online, «Інформаційного ресурсу» LIBRARIA™ та Онлайн-бібліотеки видавництва «Центр учбової літератури», комп'ютеризованої читальної зали з бібліотечним фондом. |

* наводяться відомості, як мінімум, щодо наявності відповідного матеріально-технічного забезпечення, його достатності для реалізації ОП; для обладнання/устаткування – також кількість, рік введення в експлуатацію, рік останнього ремонту; для програмного забезпечення – також кількість ліцензій та версія програмного забезпечення

Таблиця 2. Зведена інформація про викладачів ОП

| ID викладача | ПІБ | Посада | Структурний підрозділ | Кваліфікація викладача | Стаж | Навчальні дисципліни, що їх викладає викладач на ОП | Обґрунтування |
|--------------|-----------------------------|------------------------------|--|--|------|--|--|
| 288692 | Аносов Андрій Олександрович | Доцент, Основне місце роботи | Факультет інформаційних технологій та математики | Диплом кандидата наук ДК 029855, виданий 30.06.2005, Атестат доцента 12ДЦ 044758, виданий 15.12.2015 | 39 | Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем | <p>Відповідність освіти:</p> <ol style="list-style-type: none"> Національна академія оборони України, 1999 р., спеціальність «Організація бойового та оперативного забезпечення військ (сил)», кваліфікація «Офіцер військового управління оперативно-тактичного рівня». Кандидат військових наук, 2005 р., 20.01.12 – Радіоелектронна боротьба, способи та засоби. Тема дисертації «Методика обґрунтування раціональних способів радіоелектронного подавлення супутникових систем зв'язку» (ДК № 029855, 30.06.2005, Вища атестаційна комісія України). Доцент кафедри інформаційної та кібернетичної безпеки (12ДЦ № 044758, 15.12.2015, Міністерство освіти і науки України). Наявність публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: <ol style="list-style-type: none"> Brzhevska, Zoreslava и Haidur, Halyna и Dovzhenko, Nadiia и Anosov, Andrii и Vorokhob, Maksym (2021) Recurrent Estimation of the Information State Vector and the Correlation of Measuring Impact Matrix using a Multi-Agent Model Cybersecurity Providing in Information and Telecommunication Systems 2021, 2963. С. 272-276. ISSN 1613-0073 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing» |

Services».

2. Черненко, Роман Миколайович и Рябчун, Олена Петрівна и Ворохоб, Максим Віталійович и Аносов, Андрій Олександрович и Козачок, Валерій Анатолійович (2021) Підвищення рівня захищеності систем мережі інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 3 (11) 2021. С. 124-135. ISSN 2663-4023 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

3. Бурячок, Володимир Леонідович и Аносов, Андрій Олександрович и Платоненко, Артем Вадимович (2019) Генерування паролю для бездротових мереж з використанням змінного правила ускладнення Захист інформації, 21 (1). 2019 С. 52-59. ISSN 2221-5212 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

4. Saunanova, K и Sagyndykova, S и Buriachok, Volodymyr и Mazur, Natalia и Anosov, A и Smirnov, S и Malyukov, V (2019) Development of a model of cyber security management for automated systems International Journal of Civil Engineering and Technology, 10 (3). 2019 С. 454-463. ISSN 0976-6308 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

5. Бржевська, Зореслава Михайлівна и Довженко, Надія Михайлівна и

індексується в «Scopus».

9. Chernenko, Roman та Anosov, Andrii та Kyrychok, Roman та Brzhevska, Zoreslava та Spasiteleva, Svitlana (2022) Encryption Method for Systems with Limited Computing Resources Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 142-148. ISSN 1613-0073 Журнал індексується в «Scopus».

Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії:

1. Бурячок, Володимир Леонідович и Аносов, Андрій Олександрович и Семко, Віктор Володимирович и Соколов, Володимир Юрійович и Складанний, Павло Миколайович Технології забезпечення безпеки мережевої інфраструктури: підручник; – Київ : Вид-во Київський університет імені Бориса Грінченка, 2019. – 218 с.

Участь у міжнародних наукових та/або освітніх проектах:

1. У 2013 – 2018 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).

Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/місячних вказівок/рекомендацій/робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування:

1. Бржевська З.М. Гайдур Г.І. Аносов

А.О. Вплив на достовірність інформації як загроза для інформаційного простору.
Кібербезпека: освіта, наука, техніка 2018. №2 (2). С. 105-112.
2. Бржевська З.М. Довженко Н.М. Гайдур Г.І. Аносова.О. Критерії моніторингу достовірності інформації в інформаційному просторі
Кібербезпека: освіта, наука, техніка, 2019. №1 (5). С. 53-60.
3. Бржевська З.М. Довженко Н.М. Киричок Р.М. Гайдур Г.І. Аносова.О. Інформаційні війни: проблеми, загрози та протидія
Кібербезпека: освіта, наука, техніка, 2019. №3 (3). С. 88-96.
4. Saunova, K и Sagyndykova, S и Buriachok, Volodymyr и Mazur, Natalia и Anosov, A и Smirnov, S и Malyukov, V (2019) Development of a model of cyber security management for automated systems International Journal of Civil Engineering and Technology, 2019. №10 (3). С. 454-463.
5. Brzhevska, Zoreslava и Haidur, Halyna и Dovzhenko, Nadiia и Anosov, Andrii и Vorokhob, Maksym (2021) Recurrent Estimation of the Information State Vector and the Correlation of Measuring Impact Matrix using a Multi-Agent Model Cybersecurity Providing in Information and Telecommunication Systems 2021, № 2963. С. 272-276.
Підвищення кваліфікації:
1. ТОВ «РДЛ», курс «Робота зі шлюзом перехоплення для PS core компанії Huawei» (144 год.). Сертифікат .№ 015/2018, 01.09-01.11.2018.
2. Київський університет імені Бориса Грінченка, наказ про результати сертифікації ЕНК від 06.12.2021 № 811 (підвищення кваліфікації за розробку електронного

| | | | | | | | |
|-------|---------------------------------|--------------------------------|---------------------------------------|--|----|--|--|
| | | | | | | | навчального курсу «Моніторинг, аудит та адміністрування захищених ІТ систем та мереж» (5 курс, КБ, денна), 120 год. |
| 37135 | Горбань Олександр Володимирович | Професор, Основне місце роботи | Факультет суспільно-гуманітарних наук | Диплом доктора наук ДД 000355, виданий 22.12.2011, Атестат професора 12ПР 008094, виданий 26.10.2012 | 25 | Філософія і методологія наукової діяльності (Філософія науки; Загальнонаукова методологія) | Відповідність освіти: 1. Доктор філософських наук, 09.00.03 – соціальна філософія та філософія історії. Тема дисертації: «Громадянське суспільство: ідея та механізм її реалізації (соціально-філософський аналіз)» (ДД № 000355, 22.12.2011, Вища атестаційна комісія України). 2. Професор кафедри філософії та права (12ПР 008094, 26.12.2012, Міністерство освіти і науки, молоді та спорту України). Наявність публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. O. Horban, R. Martych. The basic approaches to the value of life in bioethical discourse. Studia Warمیnskie. 2022. № 59. P. 87-96. https://doi.org/10.31648/sw.8328 . Web of Science 2. O. Horban, R. Martych, L. Soha, T. Lohvyniuk. Socio-Philosophical Phenomenon of the Intelligentsia: The Genesis of the Formation of the Concept. Wisdom. 2022. № 2(22). P. 40-49 https://doi.org/10.24234/wisdom.v22i2.609 Scopus 3. O. Horban, M. Maletska. Space Age Grand Narratives in Videogames. Philosophy and Cosmology, Volume 28, 2022. P. 63-72. https://doi.org/10.29202/philcosm/28/6 Web of Science. 4. O. Horban, O. Protsenko, V. Tytarenko, O. Bulvinska, O. Melnychenko (2022) Cultural economics: the role of higher education |

institution in shaping the value systems. Scientific Bulletin of National Mining University. №1. P. 128-132.
<https://doi.org/10.33271/nvngu/2022-1/128>
Scopus

5. O. Horban, H. Lavrynenko. The “Legitimation Trap” of Political Power in the Context of the Philosophy of Universalism of Political Existence. Studia Warmińskie. 2021. № 58. P. 161-171. DOI:
<https://doi.org/10.31648/sw.7012>. Web of Science

6. O. Horban, L. Babenko, I. Lomachinska, O. Hura, R. Martych. (2021) A knowledge management culture in the European higher education system. Scientific Bulletin of National Mining University. №1. P. 173-177.
<https://doi.org/10.33271/nvngu/2021-3/173>
Scopus

7. O. Horban, R. Martych. The idea of living in religious-philosophical discourse. Studia Warmińskie. 2020. № 57. P. 101-115. DOI:
<https://doi.org/10.31648/sw.6008>. Web of Science.

8. O. Horban, T. Kuprii, R. Martych, L. Panasiuk. Implications of total quality management in Ukrainian higher education institutions: international experience. Scientific Bulletin of National Mining University. 2020. № 2. P. 126-130. DOI:
<https://doi.org/10.33271/nvngu/2020-2/126>
Scopus.

9. O. Horban, T. Havryliuk, R. Martych, T. Tymoshenko, A. Shapoval. Theological anthropology: Open questions of the Greek spiritual tradition. ASTRA Salvensis, Supplement 2020. (1). C. 25-36.
<https://clck.ru/32n7Pf>
Scopus.

10. O. Horban, O. Kravchenko, R. Martych, N. Yukhymenko. The regulatory functions of

education in behavioral models. Scientific Bulletin of National Mining University. 2019. № 3. P. 152-157. DOI: <https://doi.org/10.29202/nvngu/2019-3/23>. Scopus.

Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії:

1. Oleksandr Horban. The problem of the quality of higher education in the context of knowledge management. Contemporary challenges in education. – Warsaw - Lviv, 2022. – P. 51-66.
2. Александрова О.С., Горбань О.В., Лавриненко Г.А. Філософія політики: Навчальний посібник. – К.: КУБГ, 2020. – 176 с.
3. Trudne pytania pamięci historycznej w paradygmacie dialogu kulturowego: Monografia zbiorowa / Kijów Uniwersytet im. Borisa Hrinchenka. Białystok: Białoruskie Towarzystwo Historyczne, 2019. S. 10-23.
4. Александрова О.С., Горбань О.В. Філософія права: Навчальний посібник. – К.: КУБГ, 2019. – 256 с.
5. Горбань О.В. Вітчизняна інтелігенція як ідеолог національного патріотизму. Формування патріотичної та громадянської свідомості учнів: теорія і практика: монографія. За заг. ред. проф. Левігаса Ф.Л.; наук. ред. Александрової О.С., Салати О.О. – К.: Київ. ун-т ім. Б. Грінченка, 2018. – 172 с. – С. 33-47.

Участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена разових спеціалізованих вчених рад:

1. Член спеціалізованої Вченої ради Д.26.133.07 Київського

університету імені Бориса Грінченка із захисту дисертацій за спеціальністю 09.00.03 – соціальна філософія та філософія історії (2017 – 2021 рр.).

2. Член разової спеціалізованої вченої ради ДФ 11.051.041 у Донецькому національному університеті імені Василя Стуса, офіційний опонент на захисті дисертації Гуржи Ксенії Леонідівни «Європейське місто як модус соціальної реальності та категорія культури», подану на здобуття наукового ступеня доктора філософії за спеціальністю 033 Філософія, галузь знань 03 Гуманітарні науки (2022 р.).

3. Офіційний опонент на захисті дисертації Фітьо Віктора Ярославовича «Соціальний вимір феномену розуміння у неklasичній пізнавальній парадигмі», подану на здобуття наукового ступеня кандидата філософських наук за спеціальністю 09.00.03 соціальна філософія та філософія історії у спеціалізованій Вченій раді К. 27.053.05 Університета Григорія Сковороди в Переяславі (2021 р.).

Виконання функцій (повноважень, обов'язків) головного редактора/члена редакційної колегії наукового видання, включеного до переліку фахових видань України:

1. Голова редакційної колегії фахового наукового електронного видання «Освітологічний дискурс» (2019-2022 рр.).

2. Член редакційної колегії фахового інформаційно-аналітичного журналу «Схід» (2018 р. – донині).

3. Член редакційної колегії наукового фахового журналу «Освітологія» (2017 р. – донині).

Наявність апробаційних

публікацій з наукової або професійної тематики:

1. Горбань О.В. Місто як елемент соціальної системи / О. Горбань А. Нестеровський // Київські філософські студії-2021. Матеріали Всеукраїнської наукової конференції з міжнародною участю (м. Київ, 21 травня 2021 р.): тези доповідей / за заг. ред. проф. Р.О. Додонова. – К.: КУБГ, 2021. – С. 13-17.
2. Горбань О.В. Роль гри в освіті: світоглядно-методологічні засади / О. Горбань // Київські філософські студії-2020. Матеріали Всеукраїнської наукової конференції з міжнародною участю (м. Київ, 19 травня 2020 р.): тези доповідей / за заг. ред. проф. Р.О. Додонова. – К.: КУБГ, 2020. – С. 452-457.
3. Горбань О.В. Поведінкові стратегії освіти в контексті миротворення / О. Горбань // Матеріали ІХ Міжнародної наукової конференції «Соціальне прогнозування та проектування майбутнього країни: проблеми мира та ненасильства в змінах глобального порядку» (12 квітня 2019 року, м. Запоріжжя) / Т.Ф. Бірюкова (гол. ред.). - Запоріжжя: КСК-Альянс, 2019. – С. 16-18.
4. Горбань О.В. Освітні аспекти відеоігор / О. Горбань, М. Малецька // Київські філософські студії-2019. Матеріали наукової конференції (м. Київ, 16-17 травня 2019 р.): тези доповідей / за заг. ред. проф. Р.О. Додонова. – Київ: Київський університет імені Бориса Грінченка, 2019. – С. 304-307.
5. Горбань О.В. Трансформація консолідуючих ціннісних орієнтацій сучасного українського студентства / О. Горбань, Т. Купрій, Л. Овсянкіна // Освітологічний дискурс: Електронне

наукове фахове видання. – 2019. - № 1-2 (24-25). – С. 1-21.

6. Горбань О.В. Проблеми аксіології та термінології в сучасних культурологічних дослідженнях / О. В. Горбань // Схід. – 2018. - № 5 (157). – С. 108-109.

Робота у складі організаційного комітету / журі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт):

1. Член організаційного комітету Всеукраїнського студентського турніру з філософії (2018, 2019, 2020 рр.).

Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях:

1. Член Асоціації релігієзнавців України (2017 р. – донині).

Відомості про підвищення кваліфікації викладача:

1. Інститут філософії ім. Г.С. Сковороди НАН України, Відділ історії зарубіжної філософії, з 17.10.2022 по 01.12.2022, довідка про проходження стажування від 15.12.2022 № 124/165.

2. Advanced International Training Course: “The culture and politics of modern Muslim education (practical oriented teachers training)”, Sinan Pasha Cultural Centre, Istanbul, Turkey, 15.08.2021-21.08.2021. Certificate RS № 2021-09-001; 2 кредити ECTS (60 год.).

3. International postgraduate practical internship “Internationalization of Higher Education. Organization of the educational process and innovative teaching methods in higher education institutions in Poland”, Collegium Civitas, Warsaw, 09.11.2020-18.12.2020. Certificate NR 143/2020; 6 кредитів ECTS (180 год.).

4. Київський

| | | | | | | | |
|--------|-----------------------------|--------------------------------|--|---|----|--|---|
| | | | | | | <p>університет імені Бориса Грінченка, наказ про результати сертифікації ЕНК від 05.03.2021 № 181 (підвищення кваліфікації за розробку електронного навчального курсу «Філософські студії» (3 курс, ІФН, денна)), 120 год.</p> <p>5. Київський університет імені Бориса Грінченка, наказ про зарахування підвищення кваліфікації за дослідницьким модулем від 25.11.2019 № 807, 1 кредит ECTS (30 год.).</p> | |
| 315458 | Коршун Наталя Володимирівна | Професор, Основне місце роботи | Факультет інформаційних технологій та математики | <p>Диплом спеціаліста, Державний університет телекомунікацій, рік закінчення: 2017, спеціальність: 7.17010101 безпека інформаційних і комунікаційних систем, Диплом магістра, Державний університет інформаційно-комунікаційних технологій, рік закінчення: 2005, спеціальність: 092402 Інформаційні мережі зв'язку, Диплом доктора наук ДД 088403, виданий 05.03.2019, Диплом кандидата наук ДК 019188, виданий 17.01.2014, Атестат доцента 12ДЦ 044759, виданий 15.12.2015, Атестат професора АП 003430, виданий 30.11.2021</p> | 16 | <p>Прикладні аспекти протидії кібератакам в соціотехнічних системах</p> | <p>Відповідність освіти:</p> <ol style="list-style-type: none"> 1. Державний університет інформаційно-комунікаційних технологій, 2005 р., спеціальність: «Інформаційні мережі зв'язку», кваліфікація: «Магістр телекомунікацій». Державний університет телекомунікацій, 2017 р., спеціальність: «Безпека інформаційних і комунікаційних систем», кваліфікація: «Інженер із захисту інформації в інформаційних і комунікаційних системах». 2. Доктор технічних наук, 05.12.13 – радіотехнічні пристрої та засоби телекомунікацій. Тема дисертації: «Методологія побудови наземного радіотехнічного комплексу управління супутниковим телекомунікаційним кластером» (ДД № 008403, 05.03.2019, Міністерство освіти і науки України). 3. Професор кафедри інформаційно та кібернетичної безпеки (АП № 003430, 30.11.2021, Міністерство освіти і науки України). Наявність публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: |

1. Задача синтезу алгоритмів оптимальної обробки складених сигналів широкосмугових систем зв'язку / А.П. Бондарчук, О.Г. Варфоломєєва, Н.В. Коршун, О.І. Чумак, Г.О. Дударєва // Наукові записки УНДІЗ. – 2018. – №1(49). – С.12-22.
2. Отримання та обробка геопросторових даних за допомогою MATLAB MAPPING TOOLBOX / Мехтієва Б.Г., Гулузаде Р.К., Іванова Л.В., Коршун Н.В., Складанний П.М. // Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка», 2019. – Вип. 2(6). С. 94-104.
3. TECHNOLOGY FOR INFORMATION AND CYBER SECURITY IN HIGHER EDUCATION INSTITUTIONS OF UKRAINE / Nashynets-Naumova A.Y., Buriachok V.L., Korshun N.V., Zhyltsov O.V., Skladanniy P.M., Kuzmenko, L.V. // Information Technologies and Learning Tools, 2020. - №77(3). -Рр. 337-354. Журнал індексується в Web of Science.
4. Застосування середовища NI Multisim при формуванні практичних навичок студентів спеціальності 125 «Кібербезпека» / Бурячок В.Л., Коршун Н.В., Шевченко С.М., Складанний П.М. // Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка», 2020. – Вип. 1(9). С. 159-169.
5. Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1» / Літвінчук І.С., Корчомний Р.О., Коршун Н.В., Ворохоб М.В. // Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка», 2020. – Вип. 2(10). С. 98-112.
6. Спосіб оцінювання інтегрованих систем безпеки на об'єкті інформаційної

діяльності. / Літвінчук І.С., Коршун Н.В., Ворохов М.В. // Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка», 2020. – Вип. 2(10). С. 135-143.

7. D.Berestov, O.Kurchenko, Y.Shcheblanin, T.Opryshko, N.Korshun. Analysis of Features and Prospects of Application of Dynamic Iterative Assessment of Information Security Risks // Cybersecurity Providing in Information and Telecommunication Systems 2021. CEUR Workshop Proceedings, Vol-2923. Pp. 329–335. (наукове видання, включене до наукометричної бази Scopus)

8. O. Shevchenko, A. Bondarchuk, O. Polonevych, B. Zhurakovskiy, N. Korshun. Methods of the Objects Identification and Recognition Research in the Networks with the IoT Concept Support // Cybersecurity Providing in Information and Telecommunication Systems 2021. CEUR Workshop Proceedings, Vol-2923. Pp. 277–282. (наукове видання, включене до наукометричної бази Scopus)

11. Коршун Н.В., Літвінчук І.С., Корчомний Р.О., Борисов І.В. Розробка рекомендацій щодо мінімізації ризиків зломів облікових записів на основі аналізу найпоширеніших методів злому // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – №4 (12). – К.: КУБГ, 2021. – С.136–143.

12. Zhurakovskiy, Bohdan та Fedorova, Nataliia та Pliushch, Oleksandr та Polishchuck, Mikhail та Korshun, Natalia (2022) Modifications of the Correlation Method of Face Detection in Biometric Identification Systems Cybersecurity Providing in Information and

Telecommunication Systems 2022, 3288 (1). c. 55-63. ISSN 1613-0073 Журнал індексується в «Scopus».

13. Grechaninov, Viktor та Hulak, Hennadii та Sokolov, V. Y. та Skladannyi, Pavlo та Korshun, Natalia (2022) Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center Emerging Technology Trends on the Smart Industry and the Internet of Things 2022, 3149. c. 107-117. ISSN 1613-0073 Журнал індексується в «Scopus».

Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора):

1. Козачок В.А., Коршун Н.В., Мазур Н.П., Платоненко А.В., Складаний П.М. Прикладні аспекти аналізу та синтезу політик безпеки. Навчальний посібник для студентів галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека – Київ: Вид-во КУБГ. 2021. - 160 с.

Захист дисертації на здобуття наукового ступеня:

1. Захист докторської дисертації на тему «Методологія побудови наземного радіотехнічного комплексу управління супутниковим телекомунікаційним кластером» (05.12.13 – радіотехнічні пристрої та засоби телекомунікацій), 2019 р.

Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента)

наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах:

1. Член редакційної колегії електронного науково-технічного видання “Кібербезпека: освіта, наука, техніка” Київського університету імені Бориса Грінченка (включено до переліку фахових видань України) (2020 р. – донині).

2. 2017 – 2018рр. - брала участь у науково-дослідній роботі «Розробка методу підвищення якості функціонування космічних навігаційних радіолокаційних систем на основі застосування нелінійних адаптивних компенсаторів» (Державний університет телекомунікацій), номер державної реєстрації № 0117U001334.

3. Керівник науково-дослідної теми «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури», Київський університет імені Бориса Грінченка (номер державної реєстрації 0122U200483), 2022-2027 рр.

Наукове консультування підприємств, установ, організацій не менше трьох років, що здійснювалося на підставі договору із закладом вищої освіти (науковою установою):

1. Консультант ТОВ “СКС ПРОЕКТ” (2016 – 2023, м. Київ) з питань побудови телекомунікаційних мереж та їх захисту від стороннього кібернетичного впливу.

Підвищення

| | | | | | | | |
|--------|--|---|---|---|----|--|--|
| | | | | | | <p>кваліфікації:</p> <ol style="list-style-type: none"> 1. Захист докторської дисертації, 2019 р. 2. Отримання вченого звання професора, 2021 р. 3. Київський університет імені Бориса Грінченка, сертифікат про підвищення кваліфікації за модулем "ІКТ" від 04.05.2020 № 1300, 1 кредит ECTS (30 год.). 4. Київський університет імені Бориса Грінченка, сертифікат про підвищення кваліфікації за Дослідницьким модулем від 04.12.2020 № 1455/41, 1 кредит ECTS (30 год.). 5. Київський університет імені Бориса Грінченка, сертифікат про підвищення кваліфікації за Лідерським модулем від 05.02.2021 № 1511/41, 1 кредит ECTS (30 год.). 6. Київський університет імені Бориса Грінченка, сертифікат про підвищення кваліфікації за Дидактичним модулем від 26.02.2021 № 1500/41, 1 кредит ECTS (30 год.). | |
| 315458 | Коршун Наталія Володимирів на | Професор, Основне місце роботи | Факультет інформаційних технологій та математики | <p>Диплом спеціаліста, Державний університет телекомунікацій, рік закінчення: 2017, спеціальність: 7.17010101 безпека інформаційних і комунікаційних систем, Диплом магістра, Державний університет інформаційно-комунікаційних технологій, рік закінчення: 2005, спеціальність: 092402 Інформаційні мережі зв'язку, Диплом доктора наук ДД 088403, виданий 05.03.2019,</p> | 16 | Технології безпеки складних соціотехнічних систем | <p>Відповідність освіти:</p> <ol style="list-style-type: none"> 1. Державний університет інформаційно-комунікаційних технологій, 2005 р., спеціальність: «Інформаційні мережі зв'язку», кваліфікація: «Магістр телекомунікацій». Державний університет телекомунікацій, 2017 р., спеціальність: «Безпека інформаційних і комунікаційних систем», кваліфікація: «Інженер із захисту інформації в інформаційних і комунікаційних системах». 2. Доктор технічних наук, 05.12.13 – радіотехнічні пристрої та засоби телекомунікацій. Тема дисертації: «Методологія побудови наземного радіотехнічного |

Диплом
кандидата наук
ДК 019188,
виданий
17.01.2014,
Атестат
доцента 12ДЦ
044759,
виданий
15.12.2015,
Атестат
професора АП
003430,
виданий
30.11.2021

комплексу управління
спутниковим
телекомунікаційним
кластером» (ДД №
008403, 05.03.2019,
Міністерство освіти і
науки України).
3. Професор кафедри
інформаційно та
кібернетичної безпеки
(АП № 003430,
30.11.2021,
Міністерство освіти і
науки України).
Наявність публікацій
у періодичних
наукових виданнях,
що включені до
переліку фахових
видань України, до
наукометричних баз,
зокрема Scopus, Web
of Science Core
Collection:
1. Задача синтезу
алгоритмів
оптимальної обробки
складених сигналів
ширококутових
систем зв'язку / А.П.
Бондарчук,
О.Г.Варфоломеева,
Н.В. Коршун,
О.І.Чумак, Г.О.
Дударева // Наукові
записки УНДІЗ. –
2018. – №1(49). –
С.12-22.
2. Отримання та
обробка
геопросторових даних
за допомогою
MATLAB MAPPING
TOOLBOX / Мехтієва
Б.Г., Гулузаде Р.К.,
Іванова Л.В., Коршун
Н.В., Складанний
П.М. // Електронне
фахове наукове
видання
"Кібербезпека: освіта,
наука, техніка», 2019.
– Вип. 2(6). С. 94-104.
3. TECHNOLOGY FOR
INFORMATION AND
CYBER SECURITY IN
HIGHER EDUCATION
INSTITUTIONS OF
UKRAINE / Nashynets-
Naumova A.Y.,
Buriachok V.L.,
Korshun N.V., Zhyltsov
O.B., Skladanniy P.M.,
Kuzmenko, L.V. //
Information
Technologies and
Learning Tools, 2020. -
№77(3). -Рр. 337-354.
Журнал індексується в
Web of Science.
4. Застосування
середовища NI
Multisim при
формуванні
практичних навичок
студентів
спеціальності 125
«Кібербезпека» /
Бурячок В.Л., Коршун
Н.В., Шевченко С.М.,
Складанний П.М. //

Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка», 2020. – Вип. 1(9). С. 159-169.

5. Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1» / Літвінчук І.С., Корчомний Р.О., Коршун Н.В., Ворохоб М.В. // Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка», 2020. – Вип. 2(10). С. 98-112.

6. Спосіб оцінювання інтегрованих систем безпеки на об'єкті інформаційної діяльності. / Літвінчук І.С., Коршун Н.В., Ворохоб М.В. // Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка», 2020. – Вип. 2(10). С. 135-143.

7. D.Berestov, O.Kurchenko, Y.Shcheblanin, T.Opryshko, N.Korshun. Analysis of Features and Prospects of Application of Dynamic Iterative Assessment of Information Security Risks // Cybersecurity Providing in Information and Telecommunication Systems 2021. CEUR Workshop Proceedings, Vol-2923. Pp. 329–335. (наукове видання, включене до наукометричної бази Scopus)

8. O. Shevchenko, A. Bondarchuk, O. Polonevych, B. Zhurakovskiy, N. Korshun. Methods of the Objects Identification and Recognition Research in the Networks with the IoT Concept Support // Cybersecurity Providing in Information and Telecommunication Systems 2021. CEUR Workshop Proceedings, Vol-2923. Pp. 277–282. (наукове видання, включене до наукометричної бази Scopus)

11. Коршун Н.В., Літвінчук І.С., Корчомний Р.О., Борисов І.В. Розробка рекомендацій щодо мінімізації ризиків

зломів облікових записів на основі аналізу найпоширеніших методів злomu // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – №4 (12). – К.: КУБГ, 2021. – С.136–143.

12. Zhurakovskiy, Bohdan та Fedorova, Nataliia та Pliushch, Oleksandr та Polishchuck, Mikhail та Korshun, Natalia (2022) Modifications of the Correlation Method of Face Detection in Biometric Identification Systems Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 55-63. ISSN 1613-0073 Журнал індексується в «Scopus».

13. Grechaninov, Viktor та Hulak, Hennadii та Sokolov, V. Y. та Skladannyi, Pavlo та Korshun, Natalia (2022) Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center Emerging Technology Trends on the Smart Industry and the Internet of Things 2022, 3149. с. 107-117. ISSN 1613-0073 Журнал індексується в «Scopus».

Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора):

1. Козачок В.А., Коршун Н.В., Мазур Н.П., Платоненко А.В., Складанний П.М. Прикладні аспекти аналізу та синтезу політик безпеки. Навчальний посібник для студентів галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека – Київ: Вид-во КУБГ. 2021. - 160 с.

Захист дисертації на здобуття наукового ступеня:

1. Захист докторської

дисертації на тему «Методологія побудови наземного радіотехнічного комплексу управління супутниковим телекомунікаційним кластером» (05.12.13 – радіотехнічні пристрої та засоби телекомунікацій), 2019 р.

Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах:

1. Член редакційної колегії електронного науково-технічного видання “Кібербезпека: освіта, наука, техніка” Київського університету імені Бориса Грінченка (включено до переліку фахових видань України) (2020 р. – донині).
2. 2017 – 2018рр. - брала участь у науково-дослідній роботі «Розробка методу підвищення якості функціонування космічних навігаційних радіолокаційних систем на основі застосування нелінійних адаптивних компенсаторів” (Державний університет телекомунікацій), номер державної реєстрації № 0117U001334.
3. Керівник науково-дослідної теми «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури», Київський університет імені Бориса

| | | | | | | | |
|--------|-----------------------------|------------------------------|--|--|----|--|--|
| | | | | | | <p>Грінченка (номер державної реєстрації 0122U200483), 2022-2027 рр. Наукове консультування підприємств, установ, організацій не менше трьох років, що здійснювалося на підставі договору із закладом вищої освіти (науковою установою):</p> <ol style="list-style-type: none"> 1. Консультант ТОВ "СКС ПРОЕКТ" (2016 – 2023, м. Київ) з питань побудови телекомунікаційних мереж та їх захисту від стороннього кібернетичного впливу. Підвищення кваліфікації: <ol style="list-style-type: none"> 1. Захист докторської дисертації, 2019 р. 2. Отримання вченого звання професора, 2021 р. 3. Київський університет імені Бориса Грінченка, сертифікат про підвищення кваліфікації за модулем "ІКТ" від 04.05.2020 № 1300, 1 кредит ECTS (30 год.). 4. Київський університет імені Бориса Грінченка, сертифікат про підвищення кваліфікації за Дослідницьким модулем від 04.12.2020 № 1455/41, 1 кредит ECTS (30 год.). 5. Київський університет імені Бориса Грінченка, сертифікат про підвищення кваліфікації за Лідерським модулем від 05.02.2021 № 1511/41, 1 кредит ECTS (30 год.). 6. Київський університет імені Бориса Грінченка, сертифікат про підвищення кваліфікації за Дидактичним модулем від 26.02.2021 № 1500/41, 1 кредит ECTS (30 год.). | |
| 288692 | Аносов Андрій Олександрович | Доцент, Основне місце роботи | Факультет інформаційних технологій та математики | Диплом кандидата наук ДК 029855, виданий 30.06.2005, Атестат доцента 12ДЦ 044758, виданий 15.12.2015 | 39 | Прикладні аспекти управління інформаційною та кібербезпекою об'єктів критичної інфраструктури | Відповідність освіти: <ol style="list-style-type: none"> 1. Національна академія оборони України, 1999 р., спеціальність «Організація бойового та оперативного забезпечення військ (сил)», кваліфікація «Офіцер військового |

управління оперативно-тактичного рівня».

2. Кандидат військових наук, 2005 р., 20.01.12 – Радіоелектронна боротьба, способи та засоби. Тема дисертації «Методика обґрунтування раціональних способів радіоелектронного подавлення супутникових систем зв'язку» (ДК № 029855, 30.06.2005, Вища атестаційна комісія України).

3. Доцент кафедри інформаційної та кібернетичної безпеки (12ДЦ № 044758, 15.12.2015, Міністерство освіти і науки України).
Наявність публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection:

1. Brzhevska, Zoreslava и Haidur, Halyna и Dovzhenko, Nadiia и Anosov, Andrii и Vorokhob, Maksym (2021) Recurrent Estimation of the Information State Vector and the Correlation of Measuring Impact Matrix using a Multi-Agent Model Cybersecurity Providing in Information and Telecommunication Systems 2021, 2963. С. 272-276. ISSN 1613-0073 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

2. Черненко, Роман Миколайович и Рябчун, Олена Петрівна и Ворохоб, Максим Віталійович и Аносов, Андрій Олександрович и Козачок, Валерій Анатолійович (2021) Підвищення рівня захищеності систем мережі інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами Електронне фахове наукове видання

"Кібербезпека: освіта, наука, техніка", 3 (11) 2021. С. 124-135. ISSN 2663-4023 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

3. Бурячок, Володимир Леонідович и Аносов, Андрій Олександрович и Платоненко, Артем Вадимович (2019) Генерування паролю для бездротових мереж з використанням змінного правила ускладнення Захист інформації, 21 (1). 2019 С. 52-59. ISSN 2221-5212 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

4. Saunova, K и Sagundykova, S и Buriachok, Volodymyr и Mazur, Natalia и Anosov, A и Smirnov, S и Malyukov, V (2019) Development of a model of cyber security management for automated systems International Journal of Civil Engineering and Technology, 10 (3). 2019 С. 454-463. ISSN 0976-6308 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

5. Бржевська, Зореслава Михайлівна и Довженко, Надія Михайлівна и Киричок, Роман Васильович и Гайдур, Галина Іванівна и Аносов, Андрій Олександрович (2019) Інформаційні війни: проблеми, загрози та протидія Кібербезпека: освіта, наука, техніка, 3 (3). 2019 С. 88-96. ISSN 2663-4023 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

6. Бржевська, Зореслава Михайлівна

и Довженко, Надія Михайлівна и Гайдур, Галина Іванівна и Аносов, Андрій Олександрович (2019) Критерії моніторингу достовірності інформації в інформаційному просторі
Кібербезпека: освіта, наука, техніка, 1 (5). 2019 С. 53-60. ISSN 2663-4023 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

7. Бржевська, Зореслава Михайлівна и Гайдур, Галина Іванівна и Аносов, Андрій Олександрович (2018) Вплив на достовірність інформації як загроза для інформаційного простору
Кібербезпека: освіта, наука, техніка (2). 2018 С. 105-112. ISSN 2663-4023 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

8. Brzhevska, Zoreslava та Kyrychok, Roman та Anosov, Andrii та Skladannyi, Pavlo та Vorokhob, Maksym (2021) Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3188 (2). с. 257-264. ISSN 1613-0073 Журнал індексується в «Scopus».

9. Chernenko, Roman та Anosov, Andrii та Kyrychok, Roman та Brzhevska, Zoreslava та Spasiteleva, Svitlana (2022) Encryption Method for Systems with Limited Computing Resources Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 142-148. ISSN 1613-0073 Журнал індексується в «Scopus».

Наявність виданого підручника чи

навчального посібника (включаючи електронні) або монографії:
1. Бурячок, Володимир Леонідович и Аносов, Андрій Олександрович и Семко, Віктор Володимирович и Соколов, Володимир Юрійович и Складанний, Павло Миколайович
Технології забезпечення безпеки мережевої інфраструктури: підручник; – Київ : Вид-во Київський університет імені Бориса Грінченка, 2019. – 218 с.
Участь у міжнародних наукових та/або освітніх проектах:
1. У 2013 – 2018 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).
Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/місячних вказівок/рекомендацій/робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування:
1. Бржевська З.М. Гайдур Г.І. Аносов А.О. Вплив на достовірність інформації як загроза для інформаційного простору. Кібербезпека: освіта, наука, техніка 2018. №2 (2). С. 105-112.
2. Бржевська З.М. Довженко Н.М. Гайдур Г.І. Аносов А.О. Критерії моніторингу достовірності інформації в інформаційному просторі Кібербезпека: освіта, наука, техніка, 2019. №1 (5). С. 53-60.
3. Бржевська З.М. Довженко Н.М.

| | | | | | | | |
|--------|-----------------------------|------------------------------|--|--|----|--|--|
| | | | | | | <p>Киричок Р.М. Гайдур Г.І. Аносов А.О. Інформаційні війни: проблеми, загрози та протидія Кібербезпека: освіта, наука, техніка, 2019. №3 (3). С. 88-96.</p> <p>4. Saunanova, K и Sagyndykova, S и Buriachok, Volodymyr и Mazur, Natalia и Anosov, A и Smirnov, S и Malyukov, V (2019) Development of a model of cyber security management for automated systems International Journal of Civil Engineering and Technology, 2019. №10 (3). С. 454-463.</p> <p>5. Brzhevska, Zoreslava и Haidur, Halyna и Dovzhenko, Nadiia и Anosov, Andrii и Vorokhob, Maksym (2021) Recurrent Estimation of the Information State Vector and the Correlation of Measuring Impact Matrix using a Multi-Agent Model Cybersecurity Providing in Information and Telecommunication Systems 2021, № 2963. С. 272-276.</p> <p>Підвищення кваліфікації:</p> <p>1. ТОВ «РДЛ», курс «Робота зі шлюзом законного перехоплення для PS core компанії Huawei» (144 год.). Сертифікат .№ 015/2018, 01.09-01.11.2018.</p> <p>2. Київський університет імені Бориса Грінченка, наказ про результати сертифікації ЕНК від 06.12.2021 № 811 (підвищення кваліфікації за розробку електронного навчального курсу «Моніторинг, аудит та адміністрування захищених ІТ систем та мереж» (5 курс, КБ, денна), 120 год.</p> | |
| 288692 | Аносов Андрій Олександрович | Доцент, Основне місце роботи | Факультет інформаційних технологій та математики | Диплом кандидата наук ДК 029855, виданий 30.06.2005, Атестат доцента 12ДЦ 044758, виданий 15.12.2015 | 39 | Забезпечення безпеки об'єктів критичної інфраструктур і в умовах ведення кібердій і кіберконфлікті в | Відповідність освіти: 1. Національна академія оборони України, 1999 р., спеціальність «Організація бойового та оперативного забезпечення військ (сил)», кваліфікація «Офіцер військового управління оперативно-тактичного рівня». |

2. Кандидат військових наук, 2005 р., 20.01.12 – Радіоелектронна боротьба, способи та засоби. Тема дисертації «Методика обґрунтування раціональних способів радіоелектронного подавлення супутникових систем зв'язку» (ДК № 029855, 30.06.2005, Вища атестаційна комісія України).

3. Доцент кафедри інформаційної та кібернетичної безпеки (12/ДЦ № 044758, 15.12.2015, Міністерство освіти і науки України). Наявність публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection:

1. Brzhevska, Zoreslava и Haidur, Halyna и Dovzhenko, Nadiia и Anosov, Andrii и Vorokhob, Maksym (2021) Recurrent Estimation of the Information State Vector and the Correlation of Measuring Impact Matrix using a Multi-Agent Model Cybersecurity Providing in Information and Telecommunication Systems 2021, 2963. С. 272-276. ISSN 1613-0073 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

2. Черненко, Роман Миколайович и Рябчун, Олена Петрівна и Ворохоб, Максим Віталійович и Аносов, Андрій Олександрович и Козачок, Валерій Анатолійович (2021) Підвищення рівня захищеності систем мережі інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 3 (11) 2021. С. 124-135. ISSN

2663-4023 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

3. Бурячок, Володимир Леонідович и Аносов, Андрій

Олександрович и Платоненко, Артем Вадимович (2019) Генерування паролю для бездротових мереж з використанням змінного правила ускладнення Захист інформації, 21 (1).

2019 С. 52-59. ISSN

2221-5212 Журнал

індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

4. Saunova, K и Sagundykova, S и Buriachok, Volodymyr и Mazur, Natalia и Anosov, A и Smirnov, S и Maluykov, V (2019)

Development of a model of cyber security management for automated systems International Journal of Civil Engineering and Technology, 10 (3).

2019 С. 454-463. ISSN

0976-6308 Журнал

індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

5. Бржевська, Зореслава Михайлівна и Довженко, Надія

Михайлівна и Киричок, Роман Васильович и Гайдур, Галина Іванівна и Аносов, Андрій

Олександрович (2019)

Інформаційні війни: проблеми, загрози та протидія

Кибербезпека: освіта, наука, техніка, 3 (3).

2019 С. 88-96. ISSN

2663-4023 Журнал

індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

6. Бржевська, Зореслава Михайлівна и Довженко, Надія Михайлівна и Гайдур, Галина Іванівна и

Аносов, Андрій
Олександрович (2019)
Критерії моніторингу
достовірності
інформації в
інформаційному
просторі
Кібербезпека: освіта,
наука, техніка, 1 (5).
2019 С. 53-60. ISSN
2663-4023 Журнал
індексується в
«IndexCopernicus»,
«CiteFactor», «Google
Scholar», «Polska
Bibliografia Naukowa»
та «Scientific Indexing
Services».

7. Бржевська,
Зореслава Михайлівна
и Гайдур, Галина
Іванівна и Аносов,
Андрій
Олександрович (2018)
Вплив на
достовірність
інформації як загроза
для інформаційного
простору
Кібербезпека: освіта,
наука, техніка (2).
2018 С. 105-112. ISSN
2663-4023 Журнал
індексується в
«IndexCopernicus»,
«CiteFactor», «Google
Scholar», «Polska
Bibliografia Naukowa»
та «Scientific Indexing
Services».

8. Brzhevska, Zoreslava
та Kyrychok, Roman та
Anosov, Andrii та
Skladannyi, Pavlo та
Vorokhob, Maksym
(2021) Analysis of the
Process of Information
Transfer from the
Source-to-User in
Terms of Information
Impact Cybersecurity
Providing in
Information and
Telecommunication
Systems II 2021, 3188
(2). с. 257-264. ISSN
1613-0073 Журнал
індексується в
«Scopus».

9. Chernenko, Roman
та Anosov, Andrii та
Kyrychok, Roman та
Brzhevska, Zoreslava та
Spasiteleva, Svitlana
(2022) Encryption
Method for Systems
with Limited
Computing Resources
Cybersecurity Providing
in Information and
Telecommunication
Systems 2022, 3288 (1).
с. 142-148. ISSN 1613-
0073 Журнал
індексується в
«Scopus».

Наявність виданого
підручника чи
навчального
посібника
(включаючи

електронні) або монографії:
1. Бурячок, Володимир Леонідович и Аносов, Андрій Олександрович и Семко, Віктор Володимирович и Соколов, Володимир Юрійович и Складанний, Павло Миколайович Технології забезпечення безпеки мережевої інфраструктури: підручник; – Київ : Вид-во Київський університет імені Бориса Грінченка, 2019. – 218 с.
Участь у міжнародних наукових та/або освітніх проектах:
1. У 2013 – 2018 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).
Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування:
1. Бржевська З.М. Гайдур Г.І. Аносов А.О. Вплив на достовірність інформації як загроза для інформаційного простору. Кібербезпека: освіта, наука, техніка 2018. №2 (2). С. 105-112.
2. Бржевська З.М. Довженко Н.М. Гайдур Г.І. Аносова А.О. Критерії моніторингу достовірності інформації в інформаційному просторі Кібербезпека: освіта, наука, техніка, 2019. №1 (5). С. 53-60.
3. Бржевська З.М. Довженко Н.М. Киричок Р.М. Гайдур Г.І. Аносова А.О. Інформаційні війни:

| | | | | | | | |
|--------|----------------------------|------------------------------|--|--|----|---|---|
| | | | | | | <p>проблеми, загрози та протидія</p> <p>Кібербезпека: освіта, наука, техніка, 2019. №3 (3). С. 88-96.</p> <p>4. Saunova, K и Sagyndykova, S и Buriachok, Volodymyr и Mazur, Natalia и Anosov, A и Smirnov, S и Malyukov, V (2019) Development of a model of cyber security management for automated systems International Journal of Civil Engineering and Technology, 2019. №10 (3). С. 454-463.</p> <p>5. Brzhevska, Zoreslava и Haidur, Halyna и Dovzhenko, Nadiia и Anosov, Andrii и Vorokhob, Maksym (2021) Recurrent Estimation of the Information State Vector and the Correlation of Measuring Impact Matrix using a Multi-Agent Model Cybersecurity Providing in Information and Telecommunication Systems 2021, № 2963. С. 272-276.</p> <p>Підвищення кваліфікації:</p> <p>1. ТОВ «РДЛ», курс «Робота зі шлюзом законного перехоплення для PS core компанії Huawei» (144 год.). Сертифікат № 015/2018, 01.09-01.11.2018.</p> <p>2. Київський університет імені Бориса Грінченка, наказ про результати сертифікації ЕНК від 06.12.2021 № 811 (підвищення кваліфікації за розробку електронного навчального курсу «Моніторинг, аудит та адміністрування захищених ІТ систем та мереж» (5 курс, КБ, денна), 120 год.</p> | |
| 288814 | Соколов Володимир Юрійович | Доцент, Основне місце роботи | Факультет інформаційних технологій та математики | Диплом магістра, Національний технічний університет України "Київський політехнічний інститут", рік закінчення: 2005, спеціальність: 090803 Електронні системи, Диплом кандидата наук ДК 055193, | 16 | Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем | Відповідність освіти: 1. Національний технічний університет України «Київський політехнічний інститут», 2005 р., спеціальність «Електронні системи», кваліфікація «Магістр електроніки». 2. Кандидат технічних наук, 2019 р. 05.13.06 – інформаційні технології. Тема дисертації «Методи і засоби підвищення інформаційної та |

виданий
16.12.2019,
Атестат
доцента АД
009225,
виданий
30.11.2021

функціональної безпеки безпроводових мереж передавання даних» (ДК № 055193, 16.12.2019, Міністерство освіти і науки України).
3. Доцент кафедри інформаційної та кібернетичної безпеки (АД № 009225, 30.11.2021, Міністерство освіти і науки України).
Наявність публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection:
1. Taj Dini, M. Penetration Tests for Bluetooth Low Energy and Zigbee using the Software-Defined Radio / Mahyar Taj Dini, V. Yu. Sokolov // Сучасний захист інформації. — №1. — К.: ДУТ, 2018. — С. 82–89. [Фахове видання.]
2. Buryachok, V. L. Low-Cost Spectrum Analyzers for Channel Allocation in Wireless Networks 2.4 GHz Range / V. L. Buryachok, V. Yu. Sokolov // World Science. — #3 (31). — Vol. 1. — Warsaw : RS Global Sp. z O. O., 2018. — P. 9–16. [Фахове видання.]
3. Buryachok, V. L. Using 2.4 GHz Wireless Botnets to Implement Denial-of-Service Attacks / V. L. Buryachok, V. Yu. Sokolov // Web of Scholar. — #6 (24). — Vol. 1. — Warsaw : RS Global Sp. z O. O., 2018. — P. 14–21. [Фахове видання.]
4. Bogachuk, I. Monitoring Subsystem for Wireless Systems based on Miniature Spectrum Analyzers / I. Bogachuk, V. Yu. Sokolov, V. Buriachok // Proceedings of the V International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T'2018), October 9–12, 2018: abstracts. — Kharkiv : IEEE, 2018. — P. 581–585. [Індексується в Scopus і WoS.]

5. Соколов, В. Ю. Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності / В. Ю. Соколов, Д. М. Курбанмурадов // Кібербезпека: освіта, наука, техніка. — №1. — К. : КУБГ, 2018. — С. 6–16. [Фахове видання категорії Б.]
6. Владимиренко, М. А. Дослідження стійкості роботи однорангових безпроводових мереж із самоорганізацією / М. А. Владимиренко, В. Ю. Соколов, В. М. Астапеня // Кібербезпека: освіта, наука, техніка. — №3. — К. : КУБГ, 2019. — С. 6–26. [Фахове видання категорії Б.]
7. Buriachok, V. Security Rating Metrics for Distributed Wireless Systems / V. Buriachok, V. Sokolov, P. Skladannyi // 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. [Індексується в Scopus.]
8. TajDini, M. Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio / M. TajDini, V. Sokolov, V. Buriachok // 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. [Індексується в Scopus.]
9. Астапеня, В. М. Результати та засоби оцінки ефективності систем фокусування для підвищення доступності в безпроводових мережах / В. М. Астапеня, В. Ю. Соколов, М. Таджіні // Кібербезпека:

освіта, наука, техніка.
— №4. — К. : КУБГ,
2019. — С. 90–103.
[Фахове видання
категорії Б.]

10. Kuzminykh, I.
Investigation of the IoT
Device Lifetime with
Secure Data
Transmission / I.
Kuzminykh, A.
Carlsson, M.
Yevdokymenko, V.
Sokolov // Proceedings
of the Internet of
Things, Smart Spaces,
and Next Generation
Networks and Systems
(NEW2AN'2019,
ruSMART'2019).
Lecture Notes in
Computer Science,
September 12, 2019:
abstracts. — Vol. 11660.
— Cham : Springer,
2019. — P. 16–27.
[Індексується в Scopus
і WoS.]

11. Vladymyrenko, M.
Analysis of
Implementation Results
of the Distributed
Access Control System /
M. Vladymyrenko, V.
Sokolov, V. Buriachok,
A. Platonenko, D.
Ageyev // Proceedings
of the VI International
Scientific and Practical
Conference Problems of
Infocommunications.
Science and Technology
(PIC S&T'2019),
October 8–11, 2019:
abstracts. — Kyiv :
IEEE, 2019. — P. 39–
44. [Індексується в
Scopus.]

12. Kipchuk, F.
Investigation of
Availability of Wireless
Access Points based on
Embedded Systems / F.
Kipchuk, V. Sokolov, V.
Buriachok, L.
Kuzmenko //
Proceedings of the VI
International Scientific
and Practical
Conference Problems of
Infocommunications.
Science and Technology
(PIC S&T'2019),
October 8–11, 2019:
abstracts. — Kyiv :
IEEE, 2019. — P. 246–
250. [Індексується в
Scopus.]

13. Buriachok, V.
Implantation of
Indexing Optimization
Technology for Highly
Specialized Terms
based on Metaphone
Phonetical Algorithm /
V. Buriachok, M.
Hadzhyiev, V. Sokolov,
P. Skladannyi, L.
Kuzmenko // Eastern-
European Journal of
Enterprise

Technologies. — Vol. 5, no. 2 (101). — Kharkiv, 2019. — P. 64–71.
[Індексується в Scopus.]

14. Курбанмурадов, Д. М. Реалізація протоколу шифрування ХТЕА на базі безпроводових систем стандарту IEEE 802.15.4 / Д. М. Курбанмурадов, В. Ю. Соколов, В. М. Астапеня // Кібербезпека: освіта, наука, техніка. — №2 (6). — К. : КУБГ, 2019. — С. 32–45. [Фахове видання категорії Б.]

15. Buriachok, V. Research of Caller ID Spoofing Launch, Detection, and Defense / V. Buriachok, V. Sokolov, M. Taj Dini // Cybersecurity: Education, Science, Technique. — #1 (7). — К. : ВГКУ, 2020. — P. 6–16. [Фахове видання категорії Б.]

16. Carlsson, A. Sustainability Research of the Secure Wireless Communication System with Channel Reservation / A. Carlsson, D. Ageyev, Y. Sadykov, V. Sokolov // Proceedings of the 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET'2020), February 25–29, 2020: abstracts. — Lviv-Slavske : IEEE, 2020. — P. 973–977.
[Індексується в Scopus і WoS.]

17. Hu, Z. Bandwidth Research of Wireless IoT Switches / Z. Hu, B. Vovkotrub, V. Buriachok, Y. Zotkin, V. Sokolov // Proceedings of the 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET'2020), February 25–29, 2020: abstracts. — Lviv-Slavske : IEEE, 2020. — P. 546–550.
[Індексується в Scopus і WoS.]

18. Bessalov, A. 3- and 5-Isogenies of Supersingular Edwards Curves / A. Bessalov, E. Grubiyani, V. Sokolov,

P. Skladannyi // Cybersecurity: Education, Science, Technique. — #4 (8). — К. : BGKU, 2020. — P. 6–21. [Фахове видання категорії Б.]

19. Bessalov, A. Modeling of 3- and 5- Isogenies of Supersingular Edwards Curves / A. Bessalov, V. Sokolov, P. Skladannyi // Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS'2020), June 2–3, 2020: abstracts. — No. I, vol. 2631. — Aachen : CEUR, 2020. — P. 30–39. [Індексується в Scopus.]

20. Iosifova, O. Techniques Comparison for Natural Language Processing / O. Iosifova, I. Iosifov, O. Rolik, V. Sokolov // Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS'2020), June 2–3, 2020: abstracts. — No. I, vol. 2631. — Aachen : CEUR, 2020. — P. 57–67. [Індексується в Scopus.]

21. Hu, Z. Development and Operation Analysis of Spectrum Monitoring Subsystem 2.4–2.5 GHz Range / Z. Hu, V. Buriachok, I. Bogachuk, V. Sokolov, D. Ageyev // Data-Centric Business and Applications. — Vol. 48. — Cham : Springer, 2020. — P. 675–709. [Індексується в Scopus.]

22. Hu, Z. B. Implementation of Social Engineering Attack at Institution of Higher Education / Z. B. Hu, V. Buriachok, V. Sokolov // Proceedings of the 1th International Workshop on Cyber Hygiene & Conflict Management in Global Information Networks (CybHyg), October 29–30, 2019: abstracts. — Vol. 2654. — Aachen : CEUR, 2020. — P. 155–164. [Індексується в Scopus.]

23. Astapenya, V. Experimental Evaluation of an Accelerating Lens on Spatial Field Structure

and Frequency Spectrum / V. Astapenya, V. Sokolov, D. Ageyev // Proceedings of the IEEE Ukrainian Microwave Week (UkrMW), September 21–25, 2020: abstracts. — Vol. 1. — Kharkiv : IEEE, 2020. — P. 203–206. [Індексується в Scopus.]

24 Bessalov, A. Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves / A. Bessalov, L. Kovalchuk, V. Sokolov, P. Skladannyi, T. Radivilova // Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS'2020), July 7, 2020: abstracts. — Vol. 2746. — Aachen : CEUR, 2020. — P. 1–13. [Індексується в Scopus.]

25. Buriachok, V. Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies / V. Buriachok, D. Ageyev, O. Zhyltsov, P. Skladannyi, V. Sokolov // Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS'2020), July 7, 2020: abstracts. — Vol. 2746. — Aachen : CEUR, 2020. — P. 23–32. [Індексується в Scopus.]

Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора):

1. Buriachok, V. Increase the Speed of Spectrum Analyzers based on Atmel Atmega328 and ARM Cortex-M3 RISC Processors / V. Buriachok, V. Sokolov ; [ed. M. Kozinski] // Bezpieczeństwo w Cyberprzestrzeni Społeczna Przestrzeń Internetu w Kontekście Wartości i Zagrożeń. — Kharkiv : NUCPU, 2019. — P. 283–297.

[Колективна монографія.]
2. Buriachok, V. Implementation of Active Learning in the Master's Program on Cybersecurity / V. Buriachok, V. Sokolov // Advances in Computer Science for Engineering and Education II. — Vol. 938. — Cham : Springer, 2019. — P. 610–624. [Колективна монографія. Індукується в Scopus.]

3. Бурячок, В. Л. Технології забезпечення безпеки мережевої інфраструктури : Підручник / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складаний. — К. : КУБГ, 2019. — 218 с. [Підручник.]

4. Бурячок, В. Л. Безпека безпроводових і мобільних мереж : Навчальний посібник / В. Л. Бурячок, В. Ю. Соколов, М. М. Тадждіні. — 2 вид., доп. — К. : КУБГ, 2020. — 144 с. [Посібник.]

5. Бурячок, В. Л. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів : Монографія / В. Л. Бурячок, В. Ю. Соколов. — К. : КУБГ, 2019. — 164 с. [Монографія.]

6. Hu, Z. V. Deduplication Method for Ukrainian Last Names, Medicinal Names, and Toponyms Based on Metaphone Phonetic Algorithm / Z. V. Hu, V. Buriachok, V. Sokolov // Advances in Computer Science for Engineering and Education III. — Vol. 1247. — Cham : Springer, 2020. — P. 518–533. [Колективна монографія. Індукується в Scopus.]

7. Marusenko, R. Experimental Evaluation of Phishing Attack on High School Students / R. Marusenko, V. Sokolov, V. Buriachok // Advances in Computer Science for Engineering

and Education III. — Vol. 1247. — Cham : Springer, 2020. — P. 668–680. [Колективна монографія. Індукується в Scopus.]

8. Sokolov, V. Development of Low-Budget Spectrum Analyzers for IoT and Sensor Networks / V. Sokolov, A. Platonenko, L. Kuzmenko, V. Buriachok // Projektowanie, badania i eksploatacja. — Bielsku-Białej : NATH, 2020. — P. 331–342. [Колективна монографія.]

Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування:

1. Соколов, В. Ю. Безпека безпроводових і мобільних мереж : Лабораторний практикум / В. Ю. Соколов, М. Тадж-Діні / ред. перекл. О. П. Райтер. — К. : ДУТ, 2018. — 122 с. [Практикум.]

2. Ініціатива SDIO / перекл. В. Ю. Соколов, ред. В. Л. Бурячок. — Версія 2.1. — К. : КУБГ, 2019. — 34 с. [Методичні вказівки.]

3. Керівництво по eduScrum : «Правила гри» / перекл. В. Ю. Соколов, ред. В. Л. Бурячок. — Версія 1.2. — К. : КУБГ, 2019. — 36 с. [Методичні вказівки.]

Захист дисертації на здобуття наукового ступеня:

1. Захист кандидатської/докторської дисертації на тему «Методи і засоби підвищення інформаційної та функціональної безпеки безпроводових мереж передавання даних»

(05.13.06 – інформаційні технології, 2019 р.)
Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах:

1. Член редколегії фахових видань «Кібербезпека: освіта, наука, техніка» (ISSN: 2663-4023) і «Космос. Технології. Суспільство» (ISSN: 2709-1503).
2. Член організаційного комітету міжнародної конференції «IEEE International Scientific-Practical Conference on Problems of Infocommunications Science and Technology» (індексується в Scopus).
3. Технічний редактор міжнародної конференції «Workshop on Cybersecurity Providing in Information and Telecommunication Systems» (індексується в Scopus).

Участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання "суддя міжнародної категорії":

1. «Research of Natural Language Processing» (01.04.2020–01.04.2021 pp.) – грант Ender Turing OÜ № 32-041120 (координатор проекту).
2. «Real-Time Consolidation of Wireless Communication Network Data» (01.08.2019–01.08.2020 pp.) – грант International Center of Informatics and Computer Science

№ CCNU19TS022 (виконавець).
3. «Educating the Next Generation Experts in Cyber Security: the New EU-Recognized Master's Program» (01.12.2013–01.11. 2017 рр.) – грант European Commission № 544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR (виконавець).
Наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій:
1. Vyshnivskiy, V. Laboratory Complex “Cyber Range” / V. Vyshnivskiy, V. Sokolov // Repots of the Regional Workshop of the International Telecommunication Union for Europe and CIS Region “Digi-tal Future Powered by 4G/5G”, 14–16 травня 2018 р.: тези доповіді // Сучасний захист інформації. – №2. – К. : ДУТ, 2018. – С. 105–107. [Огляд.]
2. Соколов, В. Ю. Порівняння можливих підходів щодо розробки низькобюджетних аналізаторів спектру для сенсорних мереж діапазону 2,4–2,5 ГГц / В. Ю. Соколов // Кібербезпека: освіта, наука, техніка. – №2. – К. : КУБГ, 2018. – С. 31–46. [Фахове видання категорії Б.]
3. Sokolov, V. Y. Analysis of Recent Attacks based on Social Engineering Techniques / V. Y. Sokolov, O. Y. Korzhenko // Матеріали Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених «Комп'ютерна інженерія і кібербезпека: досягнення та інновації», 27–29 листопада 2018 р.: тези доповіді. – Кропивницький : ЦНТУ, 2018. – С. 361–363. [Огляд.]
4. Yevdokymenko, M. Overview of the Course

in “Wireless and Mobile Security” / М. Yevdokymenko, V. Sokolov // Educating the Next Generation MSc in Cyber Security. — Sweden : BTH, 2019. — P. 104–119. [Огляд.]

5. Соколов, В. Ю. Порівняльний аналіз пропускної здатності малопотужних безпроводових IoT-комутаторів / В. Ю. Соколов, Б. В. Вовкотруб, Є. О. Зоткін // Кібербезпека: освіта, наука, техніка. — №1 (5). — К. : КУБГ, 2019. — С. 16–30. [Фахове видання категорії Б.]

7. Бурячок, В. Л. Дослідження продуктивності безпроводових вбудованих систем / В. Л. Бурячок, В. Ю. Соколов, Ф. В. Кіпчук // Матеріали I Міжнародної науково-практичної конференції «Безпека ресурсів інформаційних систем», 16, 17 квітня 2020 р.: тези доповіді. — Чернігів : НУЧП, 2020. — С. 65–71. [Огляд.]

8. TajDini, M. Wireless Sensors for Brain Activity — A Survey / M. TajDini, V. Sokolov, I. Kuzminykh, S. Shiaeles, B. Ghita // Electronics. — Vol. 9(12), iss. 2092. — Basel : MDPI, 2020. — P. 1–26. [Індексується в Scopus і WoS.]

Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях:

1. Член «European Microwave Association (EuMA)» (з 2019 р.)
2. Член «Center for Internet Security (CIS)» (з 2018 р.)
3. Член «Malware Information Sharing Platform (MISP)» (з 2018 р.)
4. Член «International Telecommunication Union (ITU)» (з 2017 р.)
5. Член «Internet Society (IS)» (з 2017 р.)

Досвід практичної роботи за спеціальністю:
04.2020—05.2021 — бізнес-аналітик, ТОВ «Comrito»
Організаційна робота у закладах освіти на посадах керівника

| | | | | | | | |
|--------|----------------------------|------------------------------|--|---|----|---|---|
| | | | | | | <p>(заступника керівника) закладу освіти/ інституту/ факультету/ відділення (наукової установи)/ філії/ кафедри або іншого відповідального за підготовку здобувачів вищої освіти підрозділу/ відділу (наукової установи)/ навчально:</p> <p>З 1 вересня 2018 року по цей час – завідувач лабораторії «Безпеки інформаційних активів» кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка за суміщенням.</p> <p>Підвищення кваліфікації:</p> <ol style="list-style-type: none"> 1. Київський університет імені Бориса Грінченка, наказ про результати сертифікації ЕНК від 06.30.2021 № 448 (підвищення кваліфікації за розробку електронного навчального курсу «Основи ОС та сучасних Інтернет-технологій» (4 курс, КБ, денна), 120 год. 2. Київський університет імені Бориса Грінченка, підвищення кваліфікації за дослідницьким модулем від 03.12.2021, 1 кредит ECTS (30 год.). | |
| 288814 | Соколов Володимир Юрійович | Доцент, Основне місце роботи | Факультет інформаційних технологій та математики | <p>Диплом магістра, Національний технічний університет України "Київський політехнічний інститут", рік закінчення: 2005, спеціальність: 090803 Електронні системи, Диплом кандидата наук ДК 055193, виданий 16.12.2019, Атестат доцента АД 009225, виданий 30.11.2021</p> | 16 | Організація захисту розподілених інформаційних ресурсів | <p>Відповідність освіти:</p> <ol style="list-style-type: none"> 1. Національний технічний університет України «Київський політехнічний інститут», 2005 р., спеціальність «Електронні системи», кваліфікація «Магістр електроніки». 2. Кандидат технічних наук, 2019 р. 05.13.06 – інформаційні технології. Тема дисертації «Методи і засоби підвищення інформаційної та функціональної безпеки безпроводових мереж передавання даних» (ДК № 055193, 16.12.2019, Міністерство освіти і науки України). 3. Доцент кафедри інформаційної та кібернетичної безпеки (АД № 009225, 30.11.2021, |

Міністерство освіти і науки України).
Наявність публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection:

1. Taj Dini, M. Penetration Tests for Bluetooth Low Energy and Zigbee using the Software-Defined Radio / Mahyar Taj Dini, V. Yu. Sokolov // Сучасний захист інформації. — №1. — К.: ДУТ, 2018. — С. 82–89. [Фахове видання.]
2. Buryachok, V. L. Low-Cost Spectrum Analyzers for Channel Allocation in Wireless Networks 2.4 GHz Range / V. L. Buryachok, V. Yu. Sokolov // World Science. — #3 (31). — Vol. 1. — Warsaw : RS Global Sp. z O. O., 2018. — P. 9–16. [Фахове видання.]
3. Buryachok, V. L. Using 2.4 GHz Wireless Botnets to Implement Denial-of-Service Attacks / V. L. Buryachok, V. Yu. Sokolov // Web of Scholar. — #6 (24). — Vol. 1. — Warsaw : RS Global Sp. z O. O., 2018. — P. 14–21. [Фахове видання.]
4. Bogachuk, I. Monitoring Subsystem for Wireless Systems based on Miniature Spectrum Analyzers / I. Bogachuk, V. Yu. Sokolov, V. Buriachok // Proceedings of the V International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T'2018), October 9–12, 2018: abstracts. — Kharkiv : IEEE, 2018. — P. 581–585. [Індексується в Scopus і WoS.]
5. Соколов, В. Ю. Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності / В. Ю. Соколов, Д. М. Курбанмуратов // Кібербезпека: освіта, наука, техніка. — №1. — К. : КУБГ, 2018. — С. 6–16. [Фахове видання]

категорії Б.]
6. Владимиренко, М. А. Дослідження стійкості роботи однорангових безпроводових мереж із самоорганізацією / М. А. Владимиренко, В. Ю. Соколов, В. М. Астапеня // Кібербезпека: освіта, наука, техніка. — №3. — К. : КУБГ, 2019. — С. 6–26. [Фахове видання категорії Б.]
7. Buriachok, V. Security Rating Metrics for Distributed Wireless Systems / V. Buriachok, V. Sokolov, P. Skladannyi // 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. [Індексується в Scopus.]
8. TajDini, M. Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio / M. TajDini, V. Sokolov, V. Buriachok // 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. [Індексується в Scopus.]
9. Астапеня, В. М. Результати та засоби оцінки ефективності систем фокусування для підвищення доступності в безпроводових мережах / В. М. Астапеня, В. Ю. Соколов, М. Таджіні // Кібербезпека: освіта, наука, техніка. — №4. — К. : КУБГ, 2019. — С. 90–103. [Фахове видання категорії Б.]
10. Kuzminykh, I. Investigation of the IoT Device Lifetime with Secure Data Transmission / I. Kuzminykh, A. Carlsson, M. Yevdokymenko, V.

Sokolov // Proceedings of the Internet of Things, Smart Spaces, and Next Generation Networks and Systems (NEW2AN'2019, ruSMART'2019). Lecture Notes in Computer Science, September 12, 2019: abstracts. — Vol. 11660. — Cham : Springer, 2019. — P. 16–27. [Індексується в Scopus і WoS.]

11. Vladymyrenko, M. Analysis of Implementation Results of the Distributed Access Control System / M. Vladymyrenko, V. Sokolov, V. Buriachok, A. Platonenko, D. Ageyev // Proceedings of the VI International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T'2019), October 8–11, 2019: abstracts. — Kyiv : IEEE, 2019. — P. 39–44. [Індексується в Scopus.]

12. Kipchuk, F. Investigation of Availability of Wireless Access Points based on Embedded Systems / F. Kipchuk, V. Sokolov, V. Buriachok, L. Kuzmenko // Proceedings of the VI International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T'2019), October 8–11, 2019: abstracts. — Kyiv : IEEE, 2019. — P. 246–250. [Індексується в Scopus.]

13. Buriachok, V. Implantation of Indexing Optimization Technology for Highly Specialized Terms based on Metaphone Phonetical Algorithm / V. Buriachok, M. Hadzhyiev, V. Sokolov, P. Skladannyi, L. Kuzmenko // Eastern-European Journal of Enterprise Technologies. — Vol. 5, no. 2 (101). — Kharkiv, 2019. — P. 64–71. [Індексується в Scopus.]

14. Курбанмурадов, Д. М. Реалізація протоколу шифрування ХТЕА на базі безпроводових систем стандарту IEEE 802.15.4 / Д. М. Курбанмурадов, В. Ю.

Соколов, В. М.
Астапеня // Кібербезпека: освіта, наука, техніка. — №2 (6). — К. : КУБГ, 2019. — С. 32–45. [Фахове видання категорії Б.]

15. Buriachok, V. Research of Caller ID Spoofing Launch, Detection, and Defense / V. Buriachok, V. Sokolov, M. Taj Dini // Cybersecurity: Education, Science, Technique. — #1 (7). — К. : BGKU, 2020. — P. 6–16. [Фахове видання категорії Б.]

16. Carlsson, A. Sustainability Research of the Secure Wireless Communication System with Channel Reservation / A. Carlsson, D. Ageyev, Y. Sadykov, V. Sokolov // Proceedings of the 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET'2020), February 25–29, 2020: abstracts. — Lviv-Slavske : IEEE, 2020. — P. 973–977. [Індексується в Scopus і WoS.]

17. Hu, Z. Bandwidth Research of Wireless IoT Switches / Z. Hu, B. Vovkotrub, V. Buriachok, Y. Zotkin, V. Sokolov // Proceedings of the 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET'2020), February 25–29, 2020: abstracts. — Lviv-Slavske : IEEE, 2020. — P. 546–550. [Індексується в Scopus і WoS.]

18. Bessalov, A. 3- and 5-Isogenies of Supersingular Edwards Curves / A. Bessalov, E. Grubiyani, V. Sokolov, P. Skladannyi // Cybersecurity: Education, Science, Technique. — #4 (8). — К. : BGKU, 2020. — P. 6–21. [Фахове видання категорії Б.]

19. Bessalov, A. Modeling of 3- and 5-Isogenies of Supersingular Edwards Curves / A. Bessalov, V. Sokolov, P. Skladannyi

// Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS'2020), June 2–3, 2020: abstracts. — No. I, vol. 2631. — Aachen : CEUR, 2020. — P. 30–39. [Индексується в Scopus.]

20. Iosifova, O. Techniques Comparison for Natural Language Processing / O. Iosifova, I. Iosifov, O. Rolik, V. Sokolov // Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS'2020), June 2–3, 2020: abstracts. — No. I, vol. 2631. — Aachen : CEUR, 2020. — P. 57–67. [Индексується в Scopus.]

21. Hu, Z. Development and Operation Analysis of Spectrum Monitoring Subsystem 2.4–2.5 GHz Range / Z. Hu, V. Buriachok, I. Bogachuk, V. Sokolov, D. Ageyev // Data-Centric Business and Applications. — Vol. 48. — Cham : Springer, 2020. — P. 675–709. [Индексується в Scopus.]

22. Hu, Z. B. Implementation of Social Engineering Attack at Institution of Higher Education / Z. B. Hu, V. Buriachok, V. Sokolov // Proceedings of the 1th International Workshop on Cyber Hygiene & Conflict Management in Global Information Networks (CybHyg), October 29–30, 2019: abstracts. — Vol. 2654. — Aachen : CEUR, 2020. — P. 155–164. [Индексується в Scopus.]

23. Astapenya, V. Experimental Evaluation of an Accelerating Lens on Spatial Field Structure and Frequency Spectrum / V. Astapenya, V. Sokolov, D. Ageyev // Proceedings of the IEEE Ukrainian Microwave Week (UkrMW), September 21–25, 2020: abstracts. — Vol. 1. — Kharkiv : IEEE, 2020. — P. 203–206. [Индексується в Scopus.]

24 Bessalov, A. Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves / A. Bessalov, L. Kovalchuk, V. Sokolov, P. Skladannyi, T. Radivilova // Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS'2020), July 7, 2020: abstracts. — Vol. 2746. — Aachen : CEUR, 2020. — P. 1–13. [Індексується в Scopus.]

25. Buriachok, V. Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies / V. Buriachok, D. Ageyev, O. Zhyltsov, P. Skladannyi, V. Sokolov // Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS'2020), July 7, 2020: abstracts. — Vol. 2746. — Aachen : CEUR, 2020. — P. 23–32. [Індексується в Scopus.]

Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора):

1. Buriachok, V. Increase the Speed of Spectrum Analyzers based on Atmel Atmega328 and ARM Cortex-M3 RISC Processors / V. Buriachok, V. Sokolov ; [ed. M. Kozinski] // Bezpieczeństwo w Cyberprzestrzeni Społeczna Przestrzeń Internetu w Kontekście Wartości i Zagrożeń. — Kharkiv : NUCPU, 2019. — P. 283–297. [Колективна монографія.]

2. Buriachok, V. Implementation of Active Learning in the Master's Program on Cybersecurity / V. Buriachok, V. Sokolov // Advances in Computer Science for Engineering and Education II. — Vol. 938. — Cham :

Springer, 2019. — P. 610–624. [Колективна монографія. Індукується в Scopus.]

3. Бурячок, В. Л. Технології забезпечення безпеки мережевої інфраструктури : Підручник / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складаний. — К. : КУБГ, 2019. — 218 с. [Підручник.]

4. Бурячок, В. Л. Безпека безпроводових і мобільних мереж : Навчальний посібник / В. Л. Бурячок, В. Ю. Соколов, М. М. Тадждіні. — 2 вид., доп. — К. : КУБГ, 2020. — 144 с. [Посібник.]

5. Бурячок, В. Л. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів : Монографія / В. Л. Бурячок, В. Ю. Соколов. — К. : КУБГ, 2019. — 164 с. [Монографія.]

6. Hu, Z. B. Deduplication Method for Ukrainian Last Names, Medicinal Names, and Toponyms Based on Metaphone Phonetic Algorithm / Z. B. Hu, V. Buriachok, V. Sokolov // Advances in Computer Science for Engineering and Education III. — Vol. 1247. — Cham : Springer, 2020. — P. 518–533. [Колективна монографія. Індукується в Scopus.]

7. Marusenko, R. Experimental Evaluation of Phishing Attack on High School Students / R. Marusenko, V. Sokolov, V. Buriachok // Advances in Computer Science for Engineering and Education III. — Vol. 1247. — Cham : Springer, 2020. — P. 668–680. [Колективна монографія. Індукується в Scopus.]

8. Sokolov, V. Development of Low-Budget Spectrum Analyzers for IoT and Sensor Networks / V. Sokolov, A. Platonenko,

L. Kuzmenko, V. Buriachok // Projektowanie, badania i eksploatacja. — Bielsku-Białej : NATH, 2020. — P. 331–342. [Коллективна монографія.]
Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування:
1. Соколов, В. Ю. Безпека безпроводових і мобільних мереж : Лабораторний практикум / В. Ю. Соколов, М. Тадж-Діні / ред. перекл. О. П. Райтер. — К. : ДУТ, 2018. — 122 с. [Практикум.]
2. Ініціатива CDIO / перекл. В. Ю. Соколов, ред. В. Л. Бурячок. — Версія 2.1. — К. : КУБГ, 2019. — 34 с. [Методичні вказівки.]
3. Керівництво по eduScrum : «Правила гри» / перекл. В. Ю. Соколов, ред. В. Л. Бурячок. — Версія 1.2. — К. : КУБГ, 2019. — 36 с. [Методичні вказівки.]
Захист дисертації на здобуття наукового ступеня:
1. Захист кандидатської/докторської дисертації на тему «Методи і засоби підвищення інформаційної та функціональної безпеки безпроводових мереж передавання даних» (05.13.06 — інформаційні технології, 2019 р.)
Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної

колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах:

1. Член редколегії фахових видань «Кібербезпека: освіта, наука, техніка» (ISSN: 2663-4023) і «Космос. Суспільство» (ISSN: 2709-1503).
2. Член організаційного комітету міжнародної конференції «IEEE International Scientific-Practical Conference on Problems of Infocommunications Science and Technology» (індексується в Scopus).
3. Технічний редактор міжнародної конференції «Workshop on Cybersecurity Providing in Information and Telecommunication Systems» (індексується в Scopus).

Участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії”:

1. «Research of Natural Language Processing» (01.04.2020–01.04.2021 pp.) — грант Ender Turing OÜ № 32-041120 (координатор проекту).
2. «Real-Time Consolidation of Wireless Communication Network Data» (01.08.2019–01.08.2020 pp.) — грант International Center of Informatics and Computer Science № CCNU19TS022 (виконавець).
3. «Educating the Next Generation Experts in Cyber Security: the New EU-Recognized Master’s Program» (01.12.2013–01.11. 2017 pp.) — грант European Commission № 544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR (виконавець).

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

1. Vyshnivskiy, V. Laboratory Complex "Cyber Range" / V. Vyshnivskiy, V. Sokolov // Repots of the Regional Workshop of the International Telecommunication Union for Europe and CIS Region "Digi-tal Future Powered by 4G/5G", 14–16 травня 2018 р.: тези доповіді // Сучасний захист інформації. — №2. — К. : ДУТ, 2018. — С. 105–107. [Огляд.]
2. Соколов, В. Ю. Порівняння можливих підходів щодо розробки низькобюджетних аналізаторів спектру для сенсорних мереж діапазону 2,4–2,5 ГГц / В. Ю. Соколов // Кібербезпека: освіта, наука, техніка. — №2. — К. : КУБГ, 2018. — С. 31–46. [Фахове видання категорії Б.]
3. Sokolov, V. Y. Analysis of Recent Attacks based on Social Engineering Techniques / V. Y. Sokolov, O. Y. Korzhenko // Матеріали Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених «Комп'ютерна інженерія і кібербезпека: досягнення та інновації», 27–29 листопада 2018 р.: тези доповіді. — Кропивницький : ЦНТУ, 2018. — С. 361–363. [Огляд.]
4. Yevdokymenko, M. Overview of the Course in "Wireless and Mobile Security" / M. Yevdokymenko, V. Sokolov // Educating the Next Generation MSc in Cyber Security. — Sweden : ВТН, 2019. — Р. 104–119. [Огляд.]
5. Соколов, В. Ю. Порівняльний аналіз пропускну здатності малопотужних безпроводових IoT-

комутаторів / В. Ю. Соколов, Б. В. Вовкотруб, Є. О. Зоткін // Кібербезпека: освіта, наука, техніка. — №1 (5). — К. : КУБГ, 2019. — С. 16–30. [Фахове видання категорії Б.]

7. Бурячок, В. Л. Дослідження продуктивності безпроводових вбудованих систем / В. Л. Бурячок, В. Ю. Соколов, Ф. В. Кіпчук // Матеріали I Міжнародної науково-практичної конференції «Безпека ресурсів інформаційних систем», 16, 17 квітня 2020 р.: тези доповіді. — Чернігів : НУЧП, 2020. — С. 65–71. [Огляд.]

8. TajDini, M. Wireless Sensors for Brain Activity — A Survey / M. TajDini, V. Sokolov, I. Kuzminykh, S. Shiaeles, B. Ghita // Electronics. — Vol. 9(12), iss. 2092. — Basel : MDPI, 2020. — P. 1–26. [Індексується в Scopus і WoS.]

Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях:

1. Член «European Microwave Association (EuMA)» (з 2019 р.)
2. Член «Center for Internet Security (CIS)» (з 2018 р.)
3. Член «Malware Information Sharing Platform (MISP)» (з 2018 р.)
4. Член «International Telecommunication Union (ITU)» (з 2017 р.)
5. Член «Internet Society (IS)» (з 2017 р.)

Досвід практичної роботи за спеціальністю:
04.2020—05.2021 — бізнес-аналітик, ТОВ «Comrito»

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:

| | | | | | | | |
|--------|------------------------------|------------------------------|--|---|----|--|---|
| | | | | | | <p>З 1 вересня 2018 року по цей час – завідувач лабораторії «Безпеки інформаційних активів» кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка за суміщенням.</p> <p>Підвищення кваліфікації:</p> <ol style="list-style-type: none"> 1. Київський університет імені Бориса Грінченка, наказ про результати сертифікації ЕНК від 06.30.2021 № 448 (підвищення кваліфікації за розробку електронного навчального курсу «Основи ОС та сучасних Інтернет-технологій» (4 курс, КБ, денна), 120 год. 2. Київський університет імені Бориса Грінченка, підвищення кваліфікації за дослідницьким модулем від 03.12.2021, 1 кредит ECTS (30 год.). | |
| 276988 | Шевченко Світлана Миколаївна | Доцент, Основне місце роботи | Факультет інформаційних технологій та математики | <p>Диплом спеціаліста, Державний університет телекомунікацій, рік закінчення: 2017, спеціальність: 7.17010101 безпека інформаційних і комунікаційних систем, Диплом кандидата наук ДК 020164, виданий 14.02.2014, Атестат доцента 12ДЦ 043926, виданий 29.09.2015</p> | 34 | <p>Прикладні аспекти теорій ризиків, конфліктів і катастроф в системах безпеки</p> | <p>Відповідність освіти:</p> <ol style="list-style-type: none"> 1. Харківський державний університет ім. О.М. Горького, 1987 р., спеціальність «Математика», кваліфікація «Математик. Викладач». Державний університет телекомунікацій, 2017 р., спеціальність: «Безпека інформаційних і комунікаційних систем», кваліфікація: «Інженер із захисту інформації в інформаційних і комунікаційних системах». 2. Кандидат педагогічних наук, 2014 р. 13.00.02 – теорія та методика навчання (математика). Тема дисертації «Розвиток аналітичного мислення студентів вищих технічних навчальних закладів у процесі вивчення математичних дисциплін» (ДК № 20164, 14.02.2014, Міністерство освіти і науки України). 3. Доцент кафедри вищої математики (12ДЦ № 043926, 29.09.2015, Міністерство освіти і |

науки України).
Наявність публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection:
1. Viktoriia Onyshchenko, Svitlana Shevchenko and Olena Negodenko. Models of Information Processing in IoT Networks on the Basis of Fundamental Trigonometric Splines. – 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications. Science and Technology PIC S&T`2019. С. 613-616. ISSN ISBN 978-1-7281-4184-8. Індексуються в Scopus.
2. Shevchenko Svitlana, Burov Oleksandr, Lytvynova Svitlana, Lavrov Evgeniy, Krylova-Grek Yuliya, Orlyk Olena, Petrenko Sergiy, Tkachenko Oleksii. (2020) Cybersecurity in Educational Networks Intelligent Human Systems Integration 2020 - Proceedings of the 3rd International Conference on Intelligent Human Systems Integration (IHSI 2020): Integrating People and Intelligent Systems, February 19-21, 2020, Modena, Italy, 1131. С. 359-364. ISSN 2194-5365 (electronic)/ 978-3-030-39512-4 (eBook). Індексуються в Scopus.
3. Pinchuk Olga, Sokolyuk Oleksandra, Burov Oleksandr, Lavrov Evgeniy, Shevchenko Svitlana, Aksakovska Valeriia (2020) ICT for training and evaluation of the solar impact on aviation safety ICT in Education, Research, and Industrial Applications. Proc. 16 th Int. Conf. ICTERI 2020. Volume II: Workshops. Kharkiv, Ukraine, October 6-10, 2020, CEUR-WS.org,. С. 786-792. ISSN 1613-0073 Індексуються в Scopus.
4. Шевченко С.М. Автоматизація процесу генерування і перевірки індивідуальних навчальних завдань

для студентів з теми «дії в кільці многочленів» / Ю.Д. Жданова, С.О. Спасітелєва, С.М.Шевченко // Фізико-математична освіта: науковий журнал. – 2017. – Випуск 1(11). – С. 42-47. Журнал індексується в CrossRef, Index Copernicus, Google Scholar, Natsional'na Biblioteka Ukrayiny Imeni V.I. Vernads'koho, Abstract database "Ukrainian Science".

5. Шевченко С.М. Формування у студентів ІТ-спеціальностей компетентностей в області захисту інформації з використанням криптографічних служб .NET FRAMEWORK / С.О. Спасітелєва, С.М. Шевченко // Фізико-математична освіта: науковий журнал. – 2019. – Випуск 1(19). – С. 48-54. Журнал індексується в CrossRef, Index Copernicus, Google Scholar, Natsional'na Biblioteka Ukrayiny Imeni V.I. Vernads'koho, Abstract database "Ukrainian Science".

6. Шевченко С.М. Застосування бібліотеки класів Security.Cryptography для практичної підготовки спеціалістів з кібербезпеки / С.О. Спасітелєва, С.М. Шевченко // Кібербезпека: освіта, наука, техніка. – 2019, Том 4 № 4. – С.44-53. Журнал індексується в Directory of Open Access Journals, Index Copernicus, Google Scholar, Open Ukrainian Citation Index, Journal Factor, Reasearch Bible.

7. Шевченко С.М. Математичні методи в кібербезпеці: фрактали та їх застосування в інформаційній та кібернетичній безпеці / С.М. Шевченко, Ю.Д. Жданова, С.О. Спасітелєва, О.В. Негоденко, Н.П. Мазур, К.В. Кравчук // Кібербезпека: освіта, наука, техніка.

– 2019, Том 1 № 5. – С.31-39. Журнал індексується в Directory of Open Access Journals, Index Copernicus, Google Scholar, Open Ukrainian Citation Index, Journal Factor, Reasearch Bible.

8. Шевченко С.М. Аналіз та дослідження характеристик антивірусного програмного забезпечення, стандартизованого в Україні / С.М. Шевченко, П.М. Складанний, М.С. Марценюк // Кібербезпека: освіта, наука, техніка. – 2019, (4). – С. 62-71. Журнал індексується в Directory of Open Access Journals, Index Copernicus, Google Scholar, Open Ukrainian Citation Index, Journal Factor, Reasearch Bible.

9. Шевченко С.М. Прикладні та методичні аспекти застосування хеш-функцій в інформаційній безпеці / Ю.Д. Жданова, С.О. Спасітелєва, С.М. Шевченко, К.В. Кравчук // Кібербезпека: освіта, наука, техніка. – 2020, Том 4, № 8. – С.85-96. Журнал індексується в Directory of Open Access Journals, Index Copernicus, Google Scholar, Open Ukrainian Citation Index, Journal Factor, Reasearch Bible.

10. Шевченко С.М. Застосування середовища Nt Multisim при формуванні практичних навичок студентів спеціальності 125 «Кібербезпека» / В.Л. Бурячок, Н.В. Коршун С.М. Шевченко, П.М. Складанний // Кібербезпека: освіта, наука, техніка. – 2020, 9 (1). – С. 159-196. Журнал індексується в Directory of Open Access Journals, Index Copernicus, Google Scholar, Open Ukrainian Citation Index, Journal Factor, Reasearch Bible.

11. Шевченко С.М. Проведення SWOT-аналізу оцінювання інформаційних

ризиків як засіб формування практичних навичок студентів спеціальності 125 Кібербезпека / Ю.Д. Жданова, С.М. Шевченко, С.О. Спасітелєва, П.М. Складаний // Кібербезпека: освіта, наука, техніка. – 2020, Том 2, № 10. – С. 158-168. Журнал індексується в Directory of Open Access Journals, Index Copernicus, Google Scholar, Open Ukrainian Citation Index, Journal Factor, Reasearch Bible.

12. Шевченко С.М. Міждисциплінарний підхід до формування навичок управління ризиками ІБ на засадах теорії прийняття рішень / В.Л. Бурячок, Ю.Д. Жданова, С.М. Шевченко, П.М. Складаний // Кібербезпека: освіта, наука, техніка. – 2021, Том 3, № 11. – С. 155-165. Журнал індексується в Directory of Open Access Journals, Index Copernicus, Google Scholar, Open Ukrainian Citation Index, Journal Factor, Reasearch Bible.

Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії:

1. 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. –155 с.

Наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики:

1. Жданова Ю.Д., Спасітелєва С.О., Шевченко С.М. Застосування комп'ютерних технологій до процесу організації самостійної роботи

студентів. Теоретико-практичні проблеми використання математичних методів і комп'ютерно-орієнтованих технологій в освіті та науці: зб. матеріалів II Всеукраїнської науково-практичної конференції, 28 березня 2018 р., м. Київ / Київ. ун-т ім. Б. Грінченка. – К.: Київ. ун-т ім. Б. Грінченка, 2018. – 235 с. – С. 43-47.

2. Жданова Ю.Д., Спасітелєва С.О., Шевченко С.М. Формування практичних навичок студентів спеціальності 125 Кібербезпека за допомогою віртуальних лабораторій. Математика в сучасному технічному університеті: Матеріали VII Міжнар. наук.-практ. конф. (Київ, 27-28 грудня 2018 р.). – Київ.: КПІ ім. Ігоря Сікорського, 2019. – 382 с. – С.253-255.

3. Жданова Ю.Д., Спасітелєва С.О., Шевченко С.М. Застосування фракталів в інформаційній та кібернетичній безпеці. Математика в сучасному технічному університеті: Матеріали VIII Міжнар. наук.-практ. конф. «Математика в сучасному технічному університеті», Київ, 27–28 грудня 2019 р. – Вінниця: Видавець ФОП Кушнір Ю. В., 2020. – 336 с. – С.67-71.

4. Жданова Ю.Д., Спасітелєва С.О., Шевченко С.М. Активні методи навчання у вивченні ризиків інформаційної безпеки. Математика в сучасному технічному університеті : Матеріали IX Міжнар. наук.-практ. конф. «Математика в сучасному технічному університеті», Київ, 28–29 грудня 2020 р. – Вінниця: Видавець ФОП Кушнір Ю. В., 2021. – 330 с. – С.291-294.

5. Жданова Ю.Д., Спасітелєва С.О.,

| | | | | | | | |
|--------|-----------------------------|------------------------------|--|--|----|---|---|
| | | | | | | <p>Шевченко С.М. Особливості застосування технологій захисту інформації в корпоративних освітніх мережах. Теоретико-практичні проблеми використання математичних методів і комп'ютерно-орієнтованих технологій в освіті та науці: зб. матеріалів III Всеукраїнської науково-практичної конференції, 28 квітня 2021 р., м. Київ / Київ. ун-т ім. Б. Грінченка. – К.: Київ. ун-т ім. Б. Грінченка, 2021. – 203 с. – С. 183-185.</p> <p>Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях:</p> <p>Член міжнародного товариства «Internet Society» https://admin.internetsociety.org/622619/Entity/Details?entityTypeId=d601a3bf-efa2-4bb7-907b-269e91ee1bc5&EntityId=37188942-23bf-4bdd-8943-d649b7009eb1 Member ID 2186776</p> <p>Підвищення кваліфікації:</p> <ol style="list-style-type: none"> «TEACHERS`SMARTU P». Sigma Software University, сертифікат № 10431, 24.01.22-28.01.22. «Управління науковими та освітніми проектами». Національний університет «Одеська юридична академія», Центр українсько-європейського наукового співробітництва, сертифікат ADV-240279-OLA dated 06.03.2022, 24.01.22-06.03.22 | |
| 288692 | Аносів Андрій Олександрович | Доцент, Основне місце роботи | Факультет інформаційних технологій та математики | Диплом кандидата наук ДК 029855, виданий 30.06.2005, Атестація доцента 12ДЦ 044758, виданий 15.12.2015 | 39 | Проектування і впровадження захищених інформаційно-комунікаційних систем | <p>Відповідність освіти:</p> <ol style="list-style-type: none"> Національна академія оборони України, 1999 р., спеціальність «Організація бойового та оперативного забезпечення військ (сил)», кваліфікація «Офіцер військового управління оперативно-тактичного рівня». Кандидат військових наук, 2005 р., 20.01.12 – Радіоелектронна боротьба, способи та |

засоби. Тема дисертації «Методика обґрунтування раціональних способів радіоелектронного подавлення супутникових систем зв'язку» (ДК № 029855, 30.06.2005, Вища атестаційна комісія України).

3. Доцент кафедри інформаційної та кібернетичної безпеки (12ДЦ № 044758, 15.12.2015, Міністрство освіти і науки України). Наявність публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection:

1. Brzhevska, Zoreslava и Haidur, Halyna и Dovzhenko, Nadiia и Anosov, Andrii и Vorokhob, Maksym (2021) Recurrent Estimation of the Information State Vector and the Correlation of Measuring Impact Matrix using a Multi-Agent Model Cybersecurity Providing in Information and Telecommunication Systems 2021, 2963. С. 272-276. ISSN 1613-0073 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

2. Черненко, Роман Миколайович и Рябчун, Олена Петрівна и Ворохоб, Максим Віталійович и Аносов, Андрій Олександрович и Козачок, Валерій Анатолійович (2021) Підвищення рівня захищеності систем мережі інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 3 (11) 2021. С. 124-135. ISSN 2663-4023 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google

Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

3. Бурячок, Володимир Леонідович и Аносов, Андрій Олександрович и Платоненко, Артем Вадимович (2019) Генерування паролю для бездротових мереж з використанням змінного правила ускладнення Захист інформації, 21 (1). 2019 С. 52-59. ISSN 2221-5212 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

4. Sauanova, K и Sagundykova, S и Buriachok, Volodymyr и Mazur, Natalia и Anosov, A и Smirnov, S и Malyukov, V (2019) Development of a model of cyber security management for automated systems International Journal of Civil Engineering and Technology, 10 (3). 2019 С. 454-463. ISSN 0976-6308 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

5. Бржевська, Зореслава Михайлівна и Довженко, Надія Михайлівна и Киричок, Роман Васильович и Гайдур, Галина Іванівна и Аносов, Андрій Олександрович (2019) Інформаційні війни: проблеми, загрози та протидія Кібербезпека: освіта, наука, техніка, 3 (3). 2019 С. 88-96. ISSN 2663-4023 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

6. Бржевська, Зореслава Михайлівна и Довженко, Надія Михайлівна и Гайдур, Галина Іванівна и Аносов, Андрій Олександрович (2019) Критерії моніторингу достовірності

інформації в інформаційному просторі
Кібербезпека: освіта, наука, техніка, 1 (5). 2019 С. 53-60. ISSN 2663-4023 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

7. Бржезька, Зореслава Михайлівна и Гайдур, Галина Іванівна и Аносов, Андрій Олександрович (2018) Вплив на достовірність інформації як загроза для інформаційного простору
Кібербезпека: освіта, наука, техніка (2). 2018 С. 105-112. ISSN 2663-4023 Журнал індексується в «IndexCopernicus», «CiteFactor», «Google Scholar», «Polska Bibliografia Naukowa» та «Scientific Indexing Services».

8. Brzhevska, Zoreslava та Kyrychok, Roman та Anosov, Andrii та Skladannyi, Pavlo та Vorokhob, Maksym (2021) Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3188 (2). с. 257-264. ISSN 1613-0073 Журнал індексується в «Scopus».

9. Chernenko, Roman та Anosov, Andrii та Kyrychok, Roman та Brzhevska, Zoreslava та Spasiteleva, Svitlana (2022) Encryption Method for Systems with Limited Computing Resources Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 142-148. ISSN 1613-0073 Журнал індексується в «Scopus».

Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії:
1. Бурячок, Володимир Леонідович и Аносов,

Андрій
Олександрович и
Семко, Віктор
Володимирович и
Соколов, Володимир
Юрійович и
Складанний, Павло
Миколайович
Технології
забезпечення безпеки
мережевої
інфраструктури:
підручник; – Київ :
Вид-во Київський
університет імені
Бориса Грінченка,
2019. – 218 с.
Участь у міжнародних
наукових та/або
освітніх проектах:
1. У 2013 – 2018 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).
Наявність виданих
навчально-
методичних
посібників/посібників
для самостійної
роботи здобувачів
вищої освіти та
дистанційного
навчання,
електронних курсів на
освітніх платформах
ліцензіатів,
конспектів
лекцій/практикумів/м
єтичних вказівок/
рекомендацій/
робочих програм,
інших друкованих
навчально-
методичних праць
загальною кількістю
три найменування:
1. Бржевська З.М.
Гайдур Г.І. Аносов
А.О. Вплив на
достовірність
інформації як загроза
для інформаційного
простору.
Кібербезпека: освіта,
наука, техніка 2018.
№2 (2). С. 105-112.
2. Бржевська З.М.
Довженко Н.М.
Гайдур Г.І. Аносова.О.
Критерії моніторингу
достовірності
інформації в
інформаційному
просторі
Кібербезпека: освіта,
наука, техніка, 2019.
№1 (5). С. 53-60.
3. Бржевська З.М.
Довженко Н.М.
Киричок Р.М. Гайдур
Г.І. Аносова.О.
Інформаційні війни:
проблеми, загрози та
протидія
Кібербезпека: освіта,
наука, техніка, 2019.

| | | | | | | | |
|--------|----------------------------|------------------------------|--|---|----|---|--|
| | | | | | | <p>№3 (3). С. 88-96.</p> <p>4. Saunova, K и Sagyndykova, S и Buriachok, Volodymyr и Mazur, Natalia и Anosov, A и Smirnov, S и Malukov, V (2019) Development of a model of cyber security management for automated systems International Journal of Civil Engineering and Technology, 2019. №10 (3). С. 454-463.</p> <p>5. Brzhevska, Zoreslava и Haidur, Halyna и Dovzhenko, Nadiia и Anosov, Andrii и Vorokhob, Maksym (2021) Recurrent Estimation of the Information State Vector and the Correlation of Measuring Impact Matrix using a Multi-Agent Model Cybersecurity Providing in Information and Telecommunication Systems 2021, № 2963. С. 272-276.</p> <p>Підвищення кваліфікації:</p> <p>1. ТОВ «РДЛ», курс «Робота зі шлюзом законного перехоплення для PS core компанії Huawei» (144 год.). Сертифікат .№ 015/2018, 01.09-01.11.2018 року.</p> <p>2. Київський університет імені Бориса Грінченка, наказ про результати сертифікації ЕНК від 06.12.2021 № 811 (підвищення кваліфікації за розробку електронного навчального курсу «Моніторинг, аудит та адміністрування захищених ІТ систем та мереж» (5 курс, КБ, денна), 120 год.</p> | |
| 365957 | Козачок Валерій Аналійович | Доцент, Основне місце роботи | Факультет інформаційних технологій та математики | <p>Диплом магістра, Національна академія оборони України, рік закінчення: 2006, спеціальність: Організація бойового та оперативного забезпечення військ (за видами та родами військ і сил), Диплом кандидата наук КН 014905, виданий 17.06.1997, Аттестат</p> | 38 | <p>Прикладні аспекти створення та застосування систем технічного захисту</p> | <p>Відповідність освіти:</p> <p>1. Київське вище інженерне радіотехнічне училище ППО, 1988 р., спеціальність: «Радіотехнічні засоби», кваліфікація: радіоінженер. Національна академія оборони України, 2006 р., спеціальність: «Організація бойового та оперативного забезпечення військ (за видами та родами військ і сил)», кваліфікація: магістр військового управління, офіцер військового управління</p> |

доцента 12ДЦ
046343,
виданий
25.02.2016

оперативно-тактичного рівня.
2. Кандидат технічних наук, 20.02.14 – озброєння та військова техніка. Тема дисертації: спеціальна. (КН № 014905, 17.06.1997, Вища атестаційна комісія України).
3. Доцент кафедри інформаційної та кібернетичної безпеки (12 ДЦ № 046343, 25.02.2016, Міністерство освіти і науки України).
Наявність публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection:
1. Козачок В.А. Information security and development problems egovernment systems in Ukraine / Kozachok V., Khmelevskoy R., Khmelevskoy Y., Semko V., Ilin O. // К., ДУТ, Збірник наукових праць «Сучасний захист інформації», 2018 р., вип. №3 (35), с. 71-77.
2. Козачок В.А. Підвищення захищеності інформаційно-телекомунікаційних систем шляхом використання ТРМ-модулів / В.А. Козачок, Г.І. Гайдур, Р.М. Хмелевський, В.Є. Дмитрієв // К., ДУТ, Збірник наукових праць «Сучасний захист інформації», 2019 р., вип. №1 (36). с. 51-59.
3. Козачок В.А. Спосіб організації оцінки стану кіберзахисту критичної інформаційної інфраструктури в режимі реального часу з урахуванням індикаторів кіберзагроз / В.А. Козачок, І.В. Ткаченко // К., ДУТ, Збірник наукових праць «Сучасний захист інформації», 2019 р., вип. №4. с. 88-93.
4. Козачок В.А. Оцінка стану кібербезпеки критичної інформаційної інфраструктури в ході виявлення та відслідкування

кризових індикаторів / В.А. Козачок, І.В. Ткаченко, С.О. Гахов, В.Є. Дмитрієв // К., ДУТ, Збірник наукових праць «Сучасний захист інформації», 2020 р., вип. №1 (41). с. 54-57.

5. Zybin S., Khoroshko V., Khokhlov Y., Kozachok V. Approach of the attack analysis to reduce omissions in the risk management //CEUR Workshop Proceedings, Volume 2923, Pages 318 – 328/ Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS 2021

6. Козачок В.А. Підвищення рівня захищеності систем мережі Інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами / В.А. Козачок, Р. М. Черненко, О.П. Рябчун, М.В. Ворохоб, А.О. Аносов // Кібербезпека: освіта, наука, техніка. – №3 (11). – К. : КУБГ, 2021. – С. 124–133.

Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії:

1. Козачок В.А., Коршун Н.В., Мазур Н.П., Платоненко А.В., Складанний П.М. Прикладні аспекти аналізу та синтезу політик безпеки. Навчальний посібник для студентів галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека – Київ: Вид-во КУБГ. 2021. - 160 с.

Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що

| | | | | | | | |
|--------|----------------------------|--------------------------------|--|---|----|---|--|
| | | | | | | <p>індексуються в бібліографічних базах:</p> <p>1. Член редакційної колегії електронного фахового наукового видання Київського університету імені Бориса Грінченка "КІБЕРБЕЗПЕКА: ОСВІТА, НАУКА, ТЕХНІКА".</p> <p>Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях:</p> <p>Internet Society (IS): Reston, VA, US.</p> <p>Підвищення кваліфікації:</p> <p>1. Центральний інститут післядипломної освіти ДЗВО «Університет менеджменту освіти» Національної академії педагогічних наук України, свідоцтво про підвищення кваліфікації за категорією «Науково-педагогічні працівники університетів, академій, інститутів» від 25.10.2019 № СП 35830447 / 2653-19, 7 кредитів ECTS (210 год.).</p> | |
| 401940 | Гулак Геннадій Миколайович | Професор, Основне місце роботи | Факультет інформаційних технологій та математики | <p>Диплом спеціаліста, Вища школа КДБ СРСР, рік закінчення: 1977, спеціальність: прикладна математика, Диплом доктора наук ДД 011796, виданий 29.06.2021, Диплом кандидата наук ДК 047448, виданий 02.07.2008, Аттестат доцента 12ДЦ 030734, виданий 17.05.2012</p> | 40 | Інформаційно-аналітичні процеси в системах безпеки державних інформаційних ресурсів | <p>Відповідність освіти:</p> <p>1. Вища школа КДБ СРСР, 1977 р., спеціальність «Прикладна математика».</p> <p>2. Доктор технічних наук, 05.13.06 – інформаційні технології. Тема дисертації спеціальна (ДД № 011796, 29.06.2021, Міністерство освіти і науки України)</p> <p>3. Доцент кафедри інформаційних систем і технологій (12 ДЦ № 030734, 17.05.2012, Вища атестаційна колегія України).</p> <p>Наявність публікацій у наукових виданнях, які включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection:</p> <p>1. Гулак Г.М. Аналіз операцій модульного та покомпонентного додавання у блокових шифрах. Безпека інформації. 2020. Т. 26, № 2. С. 87-98. Журнал індексується в «EBSCO Information Services», «Google Scholar», «Bielefeld</p> |

Academic Search Engine (BASE)»
2. Гулак Г.М. Методологічні засади побудови захищених гарантоздатних інформаційних систем дистанційного навчання закладів вищої освіти. Математичні машини і системи. 2020. № 4. С. 148-162. Журнал індексується в «CrossRef», «Google Scholar», «WorldCat», «Open Ukrainian Citation Index (OUCI)»..
3. Гулак Г.М., Лахно В.А., Адилжанова С.А. Метод раціонального керування системами кіберзахисту та забезпечення гарантоздатності радіотехнічних систем. Вісник НТУУ "КПІ". Серія радіотехніка. Радіоапаратобудуванн я. 2020. №83. С. 62-68. Журнал індексується в Web of Science Core Collection.
4. Formation of requirements for the electronic record-book in guaranteed information systems of distance learning
Hulak, H., Kriuchkova, L., Skladannyi, P., Opriskyu, I. CEUR Workshop Proceedings, 2021, 2923, стр. 137–142 . Журнал індексується в Scopus.
5. V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption. 5-th International Workshop on Computer Modelling and Intelligent Systems (CMIS-2022). Zaporizhzhia, Ukraine, May 12, 2022. vol. 3137. p.p. 227-237. ISSN: 1613-0073. Періодичне видання, індексується в наукометричній базі Scopus.
6. V. Grechaninov, H. Hulak, V. Sokolov, P. Skladannyi, N. Korshun, Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center. Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, January 19, 2022, vol. 3149, p.p. 107-117. ISSN: 1613-0073. Періодичне видання,

індексується в наукометричній базі Scopus.

7. Гулак Г., Жданова Ю., Складанний П., Гулак Є., Корнієць В. Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Кібербезпека: освіта, наука, техніка. 2022. 1(17), С. 145-158. Електронне наукове видання, індексується в наукометричній базі Index Copernicus

8. S. Obushnyi, D. Virovets, H. Hulak, B. Zhurakovskiy, Autonomy of Economic Agents in Peer-to-Peer Systems. Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2022), October 13, 2022, Kyiv, Ukraine, vol. 3288, p.p. 125–133. ISSN: 1613-0073. Періодичне видання, індексується в наукометричній базі Scopus.

9. V. Grechaninov, O. Khoshaba, H. Hulak, Y. Zhdanova, I. Melnyk Models and Methods for Determining Application Performance Estimates in Distributed Structures. Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2022), October 13, 2022, Kyiv, Ukraine, vol. 3288, p.p. 134–141, ISSN: 1613-0073. Періодичне видання, індексується в наукометричній базі Scopus.

Захист дисертації на здобуття наукового ступеня:

1. Захист докторської дисертації на тему «Методологія побудови захищених гарантоздатних систем дистанційного навчання закладів вищої освіти сектору національної безпеки» (05.13.06 – Інформаційні технології, 2021 р.) Наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня (прізвище, ім'я, по

батькові дисертанта, здобутий науковий ступінь, спеціальність, назва дисертації, рік захисту, серія, номер, дата, ким виданий диплом):

1. Кузьменко Л.В. Інформаційна технологія для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури: Дис. канд.тех.наук: 05.13.06 / Інститут телекомунікацій і глобального інформаційного простору НАН України. – Київ, 2021.

2. Складаний П.М. Моделі і методи імітостійкості та конфіденційності в системах обробки інформації: Дис. канд.тех.наук: 05.13.06 / Інститут телекомунікацій і глобального інформаційного простору НАН України. – Київ, 2021.

Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах:

1. Керівник науково-дослідної теми шифр «Норін» (номер державної реєстрації 0118U00001дс) 2017-2018 рр.

2. Член редакційної колегії електронного фахового наукового видання «Кибербезпека: освіта, наука, техніка».

Участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання «суддя міжнародної категорії»:

1. «Research of Natural Language Processing.

| | | | | | | | |
|-------|-------------------------------|-----------------------------|--|--|----|---|--|
| | | | | | | <p>Stage 3» (продовження програми «Research of Natural Language Processing», №32-041120 та «Research of Natural Language Processing. Stage 2» №43-070121) за грантом №67-090121 від Ender Turing OÜ (Таллін, Естонія) з 01.09.2022 по 31.12.2023.</p> <p>2. «Methods for determining the investment attractiveness of Decentralized Autonomous Organizations» з 01.05.2022 по 31.07.2022.</p> <p>3. «Design of DAO for economy of University Community» з 01.09.2022 по 31.12.2022.</p> <p>Підвищення кваліфікації:</p> <p>1. Київський університет імені Бориса Грінченка, наказ про результати сертифікації ЕНК від 06.12.2021 № 811 (підвищення кваліфікації за розробку електронного навчального курсу «Інфраструктура відкритих ключів» (4 курс, КБ, денна), 120 год.</p> <p>2. Київський університет імені Бориса Грінченка, підвищення кваліфікації за дослідницьким модулем від 30.11.2021, 1 кредит ECTS (30 год.).</p> | |
| 25839 | Якуба Валентина Володимирівна | Декан, Основне місце роботи | Факультет романо-германської філології | Диплом кандидата наук ДК 041421, виданий 14.06.2007, Атестат доцента 12ДЦ 028546, виданий 10.11.2011 | 22 | Наукова комунікація іноземною мовою (за ОНП 2019, зі змінами 2020) | <p>Відповідність освіти:</p> <p>1. Ніжинський державний педагогічний інститут ім. М. В. Горького, 1997 р., спеціальність: «Англійська, німецька мови», кваліфікація: «Вчитель англійської, німецької мов».</p> <p>2. Кандидат філологічних наук, 10.02.04 – германські мови. Тема дисертації «Мовні засоби вираження ситуації. Зміна матримоніального стану в англійській художній прозі ХХ століття (лінгвокогнітивний та комунікативнопрагматичний аспекти)» (ДК 041421, 14.06.2007,</p> |

Вища атестаційна комісія України).
3. Доцент кафедри англійської філології (12 ДЦ 028546, 10.11.2011, Міністерство освіти і науки, молоді та спорту України).
Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора):
1. Цапро Г.Ю., Якуба В.В. A Step to Perfection for Linguists and Translators: навчальний посібник з першої іноземної мови (англійська) для студентів IV курсу спеціальностей «філологія» та «переклад» // Г.Ю. Цапро, В.В. Якуба. – Част. I. – К: Типографія Алюр, 2019. – 370 с.
(Рекомендовано МОН України як навчальний посібник для вищих навчальних закладів (лист №1/11-312 від 17.01.11р.)
2. Цапро Г.Ю., Якуба В.В. A Step to Perfection for Linguists and Translators: навчальний посібник з першої іноземної мови (англійська) для студентів IV курсу спеціальностей «філологія» та «переклад» // Г.Ю. Цапро, В.В. Якуба. – Част. II. – К: Типографія Алюр, 2019. – 250 с.
(Рекомендовано МОН України як навчальний посібник для вищих навчальних закладів (лист №1/11-312 від 17.01.11р.)
Наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня: Рожков Ю.Г.
Вербалізація хвороб тварин засобами англійської мови: лінгвокогнітивний і структурно-семантичний аспекти. ДФ 26.133.014. –

Дисертація на здобуття ступеня доктора філософії зі спеціальності 035 Філологія, Київський університет імені Бориса Грінченка, червень, 2021 р.
Участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад:
Член спеціалізованої Вченої ради К 26.133.08 в Київському університеті імені Бориса Грінченка з правом прийняття до розгляду та проведення захисту дисертацій на здобуття наукового ступеня кандидата філологічних наук за спеціальностями 10.02.04 «Германські мови» та 10.02.15 «Загальне мовознавство» (по грудня 2019 р.)
Опонування: 2018 р. – Чумак, Людмила Миколаївна, дисертація на здобуття ступеня кандидата філологічних наук, 10.02.04 – германські мови, «Лексичні інновації в англomовному медійному дискурсі початку ХХІ століття: структурний і лінгвопрагматичний аспекти».
Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах:
Член редколегії наукового журналу «Crossroads», Польща (індексується в Index Copernicus) (2018 - 2020 рр.).
Участь у міжнародних наукових та/або

освітніх проектах, залучення до міжнародної експертизи, наявність звання «суддя міжнародної категорії»:
Регіональний представник, член Наглядової ради міжнародної фундації Co-Serve International (США, м. Портленд) (з 2017 по тепер).
«Шкільний вчитель нового покоління» Міністерства освіти і науки України та Британської Ради в Україні (2014 –2019 рр.)
Наукове консультування підприємств, установ, організацій не менше трьох років, що здійснювалося на підставі договору із закладом вищої освіти (науковою установою) 2017 по теперішній час, 2022 р.: УЦОЯО – експертиза тестових завдань з англійської мови.
Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях:
Член ІА TEFL-Ukraine (з 2018 р.).
Відомості про підвищення кваліфікації викладача:
1. English Programmes Manager British Council Ukraine (сертифікат) 21-27.01.2017 (36 год.).
2. Київський університет імені Бориса Грінченка, наказ про результати підвищення кваліфікації за Дослідницьким модулем (23.03 - 11.05.2021) від 24.05.2021 № 356, 1 кредит ECTS (30 год.).
3. Київський університет імені Бориса Грінченка, підвищення кваліфікації (02.11. - 05.11.2021) сертифікат від 08.11.2021, 1 кредит ECTS (30 год.).
4. Київський університет імені Бориса Грінченка, наказ про результати підвищення кваліфікації за Дослідницьким модулем (поглиблений рівень) (22.10 - 30.11.2021) від

| | | | | | | | |
|--------|----------------------------|--------------------------------|--|--|----|--|---|
| | | | | | | <p>03.12.2021 № 1759/41, 1 кредит ECTS (30 год.).</p> <p>5. Київський університет імені Бориса Грінченка, наказ про результати підвищення кваліфікації за Дослідницьким модулем (поглиблений рівень) (21.04 - 27.05.2022) від 01.06.2022 № 1987/41, 1 кредит ECTS (30 год.).</p> <p>6. Ніжинський державний університет імені Миколи Гоголя, кафедра прикладної лінгвістики, підвищення кваліфікації (стажування) 26.05 – 25.06. 2022, свідоцтво від 25.06.2022 № 95/21-22 СТ, 4 кредит ECTS (120 год.). Фахівець з навчання науковому письму за пакетом матеріалів Манчестерського університету. Пройшла низку закордонних стажувань в кількох університетах США.</p> | |
| 401940 | Гулак Геннадій Миколайович | Професор, Основне місце роботи | Факультет інформаційних технологій та математики | <p>Диплом спеціаліста, Вища школа КДБ СРСР, рік закінчення: 1977, спеціальність: прикладна математика, Диплом доктора наук ДД 011796, виданий 29.06.2021, Диплом кандидата наук ДК 047448, виданий 02.07.2008, Атестат доцента 12ДЦ 030734, виданий 17.05.2012</p> | 40 | <p>Стратегії наукових досліджень (Сучасні технології інформаційної і кібербезпеки та захисту інформації)</p> | <p>Відповідність освіти:</p> <ol style="list-style-type: none"> 1. Вища школа КДБ СРСР, 1977 р., спеціальність «Прикладна математика». 2. Доктор технічних наук, 05.13.06 – інформаційні технології. Тема дисертації спеціальна (ДД № 011796, 29.06.2021, Міністерство освіти і науки України) 3. Доцент кафедри інформаційних систем і технологій (12 ДЦ № 030734, 17.05.2012, Вища атестаційна колегія України). Наявність публікацій у наукових виданнях, які включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: <p>1. Гулак Г.М. Аналіз операцій модульного та покомпонентного додавання у блокових шифрах. Безпека інформації. 2020. Т. 26, № 2. С. 87-98. Журнал індексується в «EBSCO Information Services», «Google Scholar», «Bielefeld Academic Search Engine (BASE)»</p> |

2. Гулак Г.М. Методологічні засади побудови захищених гарантоздатних інформаційних систем дистанційного навчання закладів вищої освіти. Математичні машини і системи. 2020. № 4. С. 148-162. Журнал індексується в «CrossRef», «Google Scholar», «WorldCat», «Open Ukrainian Citation Index (OUCI)»..

3. Гулак Г.М., Лахно В.А., Адилжанова С.А. Метод раціонального керування системами кіберзахисту та забезпечення гарантоздатності радіотехнічних систем. Вісник НТУУ "КПІ". Серія радіотехніка. Радіоапаратобудуванн я. 2020. №83. С. 62-68. Журнал індексується в Web of Science Core Collection.

4. Formation of requirements for the electronic record-book in guaranteed information systems of distance learning Hulak, H., Kriuchkova, L., Skladannyi, P., Oprisky, I. CEUR Workshop Proceedings, 2021, 2923, стр. 137–142 . Журнал індексується в Scopus.

5. V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption. 5-th International Workshop on Computer Modelling and Intelligent Systems (CMIS-2022). Zaporizhzhia, Ukraine, May 12, 2022. vol. 3137. p.p. 227-237. ISSN: 1613-0073. Періодичне видання, індексується в наукометричній базі Scopus.

6. V. Grechaninov, H. Hulak, V. Sokolov, P. Skladannyi, N. Korshun, Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center. Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, January 19, 2022, vol. 3149, p.p. 107-117. ISSN: 1613-0073. Періодичне видання, індексується в наукометричній базі

Scopus.
7. Гулак Г., Жданова Ю., Складаний П., Гулак Є., Корнієць В. Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Кібербезпека: освіта, наука, техніка. 2022. 1(17), С. 145-158. Електронне наукове видання, індексується в наукометричній базі Index Copernicus

8. S. Obushnyi, D. Virovets, H. Hulak, B. Zhurakovskiy, Autonomy of Economic Agents in Peer-to-Peer Systems. Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2022), October 13, 2022, Kyiv, Ukraine, vol. 3288, p.p. 125–133. ISSN: 1613-0073. Періодичне видання, індексується в наукометричній базі Scopus.

9. V. Grechaninov, O. Khoshaba, H. Hulak, Y. Zhdanova, I. Melnyk Models and Methods for Determining Application Performance Estimates in Distributed Structures. Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2022), October 13, 2022, Kyiv, Ukraine, vol. 3288, p.p. 134–141, ISSN: 1613-0073. Періодичне видання, індексується в наукометричній базі Scopus.

Захист дисертації на здобуття наукового ступеня:
1. Захист докторської дисертації на тему «Методологія побудови захищених гарантоздатних систем дистанційного навчання закладів вищої освіти сектору національної безпеки» (05.13.06 – Інформаційні технології, 2021 р.)
Наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня (прізвище, ім'я, по батькові дисертанта, здобутий науковий

ступінь, спеціальність, назва дисертації, рік захисту, серія, номер, дата, ким виданий диплом):

1. Кузьменко Л.В. Інформаційна технологія для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури: Дис. канд.тех.наук: 05.13.06 / Інститут телекомунікацій і глобального інформаційного простору НАН України. – Київ, 2021.

2. Складанний П.М. Моделі і методи імітостійкості та конфіденційності в системах обробки інформації: Дис. канд.тех.наук: 05.13.06 / Інститут телекомунікацій і глобального інформаційного простору НАН України. – Київ, 2021.

Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах:

1. Керівник науково-дослідної теми шифр «Норін» (номер державної реєстрації 0118U00001дс) 2017-2018 рр.

2. Член редакційної колегії електронного фахового наукового видання «Кібербезпека: освіта, наука, техніка». Участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання «суддя міжнародної категорії»:

1. «Research of Natural Language Processing. Stage 3» (продовження

| | | | | | | | |
|--------|-----------------------------|---------------------------------|--|--|---|--|--|
| | | | | | | <p>програми «Research of Natural Language Processing», №32-041120 та «Research of Natural Language Processing, Stage 2» №43-070121) за грантом №67-090121 від Ender Turing OU (Таллін, Естонія) з 01.09.2022 по 31.12.2023.</p> <p>2. «Methods for determining the investment attractiveness of Decentralized Autonomous Organizations» з 01.05.2022 по 31.07.2022.</p> <p>3. «Design of DAO for economy of University Community» з 01.09.2022 по 31.12.2022.</p> <p>Підвищення кваліфікації:</p> <p>1. Київський університет імені Бориса Грінченка, наказ про результати сертифікації ЕНК від 06.12.2021 № 811 (підвищення кваліфікації за розробку електронного навчального курсу «Інфраструктура відкритих ключів» (4 курс, КБ, денна), 120 год.</p> <p>2. Київський університет імені Бориса Грінченка, підвищення кваліфікації за дослідницьким модулем від 30.11.2021, 1 кредит ECTS (30 год.).</p> | |
| 241373 | Складаний Павло Миколайович | Завідувач, Основне місце роботи | Факультет інформаційних технологій та математики | Диплом кандидата наук ДК 061086, виданий 29.06.2021, Атестат доцента АД 011358, виданий 10.10.2022 | 9 | Системний аналіз та прийняття рішень в інформаційній і кібербезпеці | <p>Відповідність освіти:</p> <p>1. Державний університет телекомунікацій, 2014 р, спеціальність «Безпека інформаційних і комунікаційних систем», кваліфікація «Професіонал із організації інформаційної безпеки».</p> <p>2. Кандидат технічних наук, 05.13.06 – інформаційні технології. Тема дисертації: «Моделі і методи забезпечення імітостійкості та конфіденційності в системах обробки інформації», (ДК № 061086, 29.06.2021, Міністерство освіти і науки України).</p> <p>3. Доцент кафедри інформаційної та</p> |

кібернетичної безпеки (АД № 011358, 10.10.2022, Міністерство освіти і науки України).
Наявність публікацій у наукових виданнях, які включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection:

1. Bessalov A., Kovalchuk L., Sokolov V., Skladannyi P., Radivilova T. (2020) Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves
Cybersecurity Providing in Information and Telecommunication Systems, 2746. с. 1-13. ISSN 1613-0073. (Scopus)
2. Buriachok, V., Ageyev D., Zhyltsov O., Skladannyi P., Sokolov V. (2020) Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies
Cybersecurity Providing in Information and Telecommunication Systems, 2746. с. 23-32. ISSN 1613-0073. (Scopus)
3. Nashynets-Naumova A., Buriachok V., Korshun N., Zhyltsov O., Skladannyi P., Kuzmenko L. (2020) Technology for information and cyber security in higher education institutions of Ukraine
Інформаційні технології і засоби навчання, 77 (3). с. 337-354. ISSN 2076-8184. (Web of Science Core Collection)
4. Bessalov, Anatoly та Sokolov, V. Y. та Skladannyi, Pavlo (2020) Modeling of 3- and 5-Isogenies of Supersingular Edwards Curves MoMLeT&DS, 2631 (1). с. 30-39. ISSN 1613-0073. (Scopus)
5. Buriachok, Volodymyr and Hadzhyiev, M. and Sokolov, V. Y. and Skladannyi, Pavlo and Kuzmenko, L. (2019) Implementation of an index optimize technology for highly specialized terms based on the phonetic algorithm Metaphone Eastern-European Journal of Enterprise

Technologies, 5 (2(101)). pp. 64-71. ISSN 1729-406. (Scopus)

6. Buriachok, Volodymyr and Sokolov, V. Y. and Skladannyi, Pavlo (2019) Security Rating Metrics for Distributed Wireless Systems MoMLeT&DS. pp. 222-233. ISSN 1613-0073. (Scopus)

7. Martyniuk, Hanna and Lazarenko, Serhii and Kozlovskiy, Valeriy and Balanyuk, Yuriy and Yakoviv, Ivan and Skladannyi, Pavlo (2019) Data Mining Usage for Social Networks Proceedings of the International Workshop on Cyber Hygiene (CybHyg-2019), 2654. pp. 432-443. ISSN 1613-0073. (Scopus)

8. Solomentsev, Oleksandr and Zaliskyi, Maksym and Skladannyi, Pavlo (2019) Operation System for Modern Unmanned Aerial Vehicles Proceedings of the International Workshop on Cyber Hygiene (CybHyg-2019), 2654. pp. 363-374. ISSN 1613-0073. (Scopus)

9. Lakhno, V and Buriachok, Volodymyr and Parkhuts, L and Tarasova, H and Kydyralina, L and Skladannyi, Pavlo and Skrypnyk, M and Shostakovska, A (2018) Development of a conceptual model of adaptive access rights management with using the apparatus of Petri nets International Journal of Civil Engineering and Technology, 11 (9). pp. 95-104. ISSN 0976-630. (Scopus)

10. V. L. Buriachok, Bogush V. M., Y. V. Borsukovskii, P. M. Skladannyi, and V. Y. Borsukovska, "Training Model for Professionals in the Field of Information and Cyber Security in the Higher Educational Institutions of Ukraine", ITLT, vol. 67, no. 5, pp. 277-291, Oct. 2018. (Web of Science Core Collection)

11. Mekhdiyeva, B., Rustam, G., Ivanova, L., Korshun, N., & Skladannyi, P. (2019).

GETTING AND PROCESSING GEOPRODITIONAL DATA WITH MATLAB MAPPING TOOLBOX. Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique» 2(6), 94-104. <https://doi.org/10.28925/2663-4023.2019.6.94104> Index Copernicus, Master List, Cite Factor, Google Scholar, Crossref.

12. Shevchenko, S., Zhdanova Y., Spasiteleva, S., & Skladannyi, P. (2020). CONDUCTING A SWOT-ANALYSIS OF INFORMATION RISK ASSESSMENT AS A MEANS OF FORMATION OF PRACTICAL SKILLS OF STUDENTS SPECIALTY 125 CYBER SECURITY. Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique» 2(10), 158-168. <https://doi.org/10.28925/2663-4023.2020.10.158168> Index Copernicus, Master List, Cite Factor, Google Scholar, Crossref.

13. Bessalov, A., Grubiyani, E., Sokolov, V., & Skladannyi, P. (2020). 3- AND 5- ISOGENIES OF SUPERSINGULAR EDWARDS CURVES. Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique» 4(8), 6-21. <https://doi.org/10.28925/2663-4023.2020.8.621> Index Copernicus, Master List, Cite Factor, Google Scholar, Crossref.

14. Hulak, H., Buriachok, V., Skladannyi, P., & Kuzmenko, L. (2020). CRYPTOVIROLOGY: SECURITY THREATS TO GUARANTEED INFORMATION SYSTEMS AND MEASURES TO COMBAT ENCRYPTION VIRUSES. Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique» 2(10), 6-28. <https://doi.org/10.28925/2663->

4023.2020.10.628
Index Copernicus,
Master List, Cite Factor,
Google Scholar,
Crossref.

15. Roy, Y. V., Mazur,
N. P., & Skladannyi, P.
M. (2018). Audit of
Information Security is
the basis of Effective
Protection of the
Enterprise. Electronic
Professional Scientific
Edition «Cybersecurity:
Education, Science,
Technique» 1(1), 86-93.
<https://doi.org/10.28925/2663-4023.2018.1.8693>
Index Copernicus,
Master List, Cite Factor,
Google Scholar,
Crossref.

16. Buriachok, V. L.,
Shevchenko, S. M., &
Skladannyi, P. M.
(2018). Virtual
Laboratory for
Modeling of Processes
in Informational and
Cyber Securities as a
form of Forming
Practical Skills of
Students. Electronic
Professional Scientific
Edition «Cybersecurity:
Education, Science,
Technique» 2(2), 98-
104.
<https://doi.org/10.28925/2663-4023.2018.2.98104>
Index Copernicus,
Master List, Cite Factor,
Google Scholar,
Crossref.

17. Buriachok , V.,
Korshun , N.,
Shevchenko , S., &
Skladannyi, P. (2020).
APPLICATION OF NI
MULTISIM
ENVIRONMENT IN
THE PRACTICAL
SKILLS BUILDING
FOR STUDENTS OF
125
"CYBERSECURITY"
SPECIALTY. Electronic
Professional Scientific
Edition «Cybersecurity:
Education, Science,
Technique» 1(9), 159-
169.
<https://doi.org/10.28925/2663-4023.2020.9.159169>
Index Copernicus,
Master List, Cite Factor,
Google Scholar,
Crossref.

18. Shevchenko, S.,
Skladannyi, P., &
Martseniuk, M. (2019).
ANALYSIS AND
RESEARCH OF THE
CHARACTERISTICS
OF STANDARDIZED
IN UKRAINE
ANTIVIRUS
SOFTWARE. Electronic

Professional Scientific Edition «Cybersecurity: Education, Science, Technique» 4(4), 62-71. <https://doi.org/10.28925/2663-4023.2019.4.6271> Index Copernicus, Master List, Cite Factor, Google Scholar, Crossref.

19. Buriachok, V., Shevchenko, S., Zhdanova Y., & Skladannyi, P. (2021). INTERDISCIPLINARY APPROACH TO THE DEVELOPMENT OF IS RISK MANAGEMENT SKILLS ON THE BASIS OF DECISION-MAKING THEORY. Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique» 3(11), 155-165. <https://doi.org/10.28925/2663-4023.2021.11.155165> Index Copernicus, Master List, Cite Factor, Google Scholar, Crossref.

Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії, в тому числі видані у співавторстві:

1. Козачок В.А., Коршун Н.В., Мазур Н.П., Платоненко А.В., Складанний П.М. Прикладні аспекти аналізу та синтезу політик безпеки Навчальний посібник для студентів галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека – Київ: Вид-во КУБГ. 2021.- 160 с.

2. Бурячок В.Л., Складанний П.М., Киричок Р.В. Основи інформаційної та кібернетичної безпеки. Навчальний посібник для студентів галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека – Київ: Вид-во КУБГ. 2019. - 320 с.

3. Buriachok V.L., Duravkin Ie.V., Lukova-Chuyko N.V., Skladannyi P.M. Methods of Information Protection in Telecommunication Systems. K.: KUBG, 2019. – 74 с.

4. В. Бурячок, А. Аносов, В. Семко, В. Соколов, П. Складанний. Технології забезпечення безпеки мережевої інфраструктури. Підручник для студентів галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека – Київ: Вид-во КУБГ. 2019. - 218 с.

Захист дисертації на здобуття наукового ступеня:

1. Захист кандидатської дисертації на тему «Моделі і методи забезпечення імітостійкості та конфіденційності в системах обробки інформації» (05.13.06 – інформаційні технології), 2021 р.

Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах:

1. Головний редактор електронного фахового наукового видання "Кібербезпека: освіта, наука, техніка" (електронне видання).

2. Відповідальний секретар електронного наукового видання "Космос. Технології. Суспільство" (електронне видання).

3. Член організаційного комітету міжнародної конференції «IEEE International Scientific-Practical Conference on Problems of Infocommunications Science and Technology» (індексується в Scopus).

4. Член організаційного комітету міжнародної конференції

«Workshop on Cybersecurity Providing in Information and Telecommunication Systems» (індексується в Scopus).

Керівництво студентом, який зайняв призове місце на I або II етапі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт):

1. Керівництво Репіним В.В., який посів I місце у II турі Всеукраїнського конкурсу студентських наукових робіт зі спеціальності «Кібербезпека» (2021).
2. Керівництво Марценюком М.С., який посів I місце у II турі Всеукраїнського конкурсу студентських наукових робіт зі спеціальності «Кібербезпека» (2022).

Досвід практичної роботи за спеціальністю (спеціалізацією)/професією не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності) із зазначенням посади та строку роботи на цій посаді:

Член «Internet Society (IS)» (з 2019 р.).

Підвищення кваліфікації:

1. Захист кандидатської дисертації, 2021 р.
2. Фаховий модуль Academic innovations and online learning methodology: psychological, technological and ethical aspects, 2021р.
3. Отримання вченого звання доцента, 2022 р.
4. Київський університет імені Бориса Грінченка, підвищення кваліфікації за дослідницьким модулем від 03.12.2021, 1 кредит ECTS (30 год.).
5. Київський університет імені Бориса Грінченка, наказ про результати сертифікації ЕНК від 02.052022 № 212 (підвищення кваліфікації за

| | | | | | | | |
|-------|-------------------------------|-----------------------------|--|--|----|---|--|
| | | | | | | | розробку електронного навчального курсу «Організація науки і наукових досліджень» (5 курс, КБ, денна), 120 год. |
| 25839 | Якуба Валентина Володимирівна | Декан, Основне місце роботи | Факультет романо-германської філології | Диплом кандидата наук ДК 041421, виданий 14.06.2007, Атестат доцента 12ДЦ 028546, виданий 10.11.2011 | 22 | Наукова комунікація іноземною мовою (за ОНП 2022) | Відповідність освіти: 1. Ніжинський державний педагогічний інститут ім. М. В. Горького, 1997 р., спеціальність: «Англійська, німецька мови», кваліфікація: «Вчитель англійської, німецької мов». 2. Кандидат філологічних наук, 10.02.04 – германські мови. Тема дисертації «Мовні засоби вираження ситуації. Зміна матримоніального стану в англійській художній прозі ХХ століття (лінгвокогнітивний та комунікативнопрагматичний аспекти)» (ДК 041421, 14.06.2007, Вища атестаційна комісія України). 3. Доцент кафедри англійської філології (12 ДЦ 028546, 10.11.2011, Міністерство освіти і науки, молоді та спорту України). Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора): 1. Цапро Г.Ю., Якуба В.В. A Step to Perfection for Linguists and Translators: навчальний посібник з першої іноземної мови (англійська) для студентів IV курсу спеціальностей «філологія» та «переклад» // Г.Ю. Цапро, В.В. Якуба. – Част. I. – К: Типографія Алюр, 2019. – 370 с. (Рекомендовано МОН України як навчальний посібник для вищих навчальних закладів (лист №1/11-312 від 17.01.11р.) 2. Цапро Г.Ю., Якуба В.В. A Step to Perfection for Linguists and Translators: |

навчальний посібник з першої іноземної мови (англійська) для студентів IV курсу спеціальностей «філологія» та «переклад») // Г.Ю. Цапро, В.В. Якуба. – Част. II. – К: Типографія Алюр, 2019. – 250 с. (Рекомендовано МОН України як навчальний посібник для вищих навчальних закладів (лист №1/11-312 від 17.01.11р.)
Наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня: Рожков Ю.Г.
Вербалізація хвороб тварин засобами англійської мови: лінгвокогнітивний і структурно-семантичний аспекти. ДФ 26.133.014. – Дисертація на здобуття ступеня доктора філософії зі спеціальності 035 Філологія, Київський університет імені Бориса Грінченка, червень, 2021 р.
Участь в агестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад:
Член спеціалізованої Вченої ради К 26.133.08 в Київському університеті імені Бориса Грінченка з правом прийняття до розгляду та проведення захисту дисертацій на здобуття наукового ступеня кандидата філологічних наук за спеціальностями 10.02.04 «Германські мови» та 10.02.15 «Загальне мовознавство» (по грудня 2019 р.)
Опонування: 2018 р. – Чумак, Людмила Миколаївна, дисертація на здобуття ступеня кандидата філологічних наук, 10.02.04 – германські мови, «Лексичні інновації в англомовному медійному дискурсі початку XXI століття:

структурний і лінгвопрагматичний аспекти».

Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах:

Член редколегії наукового журналу «Crossroads», Польща (індексується в Index Copernicus) (2018 - 2020 рр.).

Участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання «суддя міжнародної категорії»:

Регіональний представник, член Наглядової ради міжнародної фундації Co-Serve International (США, м. Портленд) (з 2017 по тепер).

«Шкільний вчитель нового покоління» Міністерства освіти і науки України та Британської Ради в Україні (2014 –2019 рр.)

Наукове консультування підприємств, установ, організацій не менше трьох років, що здійснювалося на підставі договору із закладом вищої освіти (науковою установою) 2017 по теперішній час, 2022 р.: УЦОЯО – експертиза тестових завдань з англійської мови.

Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях:

Член IA TEFL-Ukraine (з 2018 р.).

Відомості про підвищення кваліфікації викладача:

1. English Programmes Manager British Council Ukraine

| | | | | | | | |
|--------|--------------------------|-----------------------|-------------------------------|--|---|--|--|
| | | | | | | <p>(сертифікат) 21-27.01.2017 (36 год.).</p> <p>2. Київський університет імені Бориса Грінченка, наказ про результати підвищення кваліфікації за Дослідницьким модулем (23.03 - 11.05.2021) від 24.05.2021 № 356, 1 кредит ECTS (30 год.).</p> <p>3. Київський університет імені Бориса Грінченка, підвищення кваліфікації (02.11. - 05.11.2021) сертифікат від 08.11.2021, 1 кредит ECTS (30 год.).</p> <p>4. Київський університет імені Бориса Грінченка, наказ про результати підвищення кваліфікації за Дослідницьким модулем (поглиблений рівень) (22.10 - 30.11.2021) від 03.12.2021 № 1759/41, 1 кредит ECTS (30 год.).</p> <p>5. Київський університет імені Бориса Грінченка, наказ про результати підвищення кваліфікації за Дослідницьким модулем (поглиблений рівень) (21.04 - 27.05.2022) від 01.06.2022 № 1987/41, 1 кредит ECTS (30 год.).</p> <p>6. Ніжинський державний університет імені Миколи Гоголя, кафедра прикладної лінгвістики, підвищення кваліфікації (стажування) 26.05 – 25.06. 2022, свідоцтво від 25.06.2022 № 95/21-22 СТ, 4 кредит ECTS (120 год.). Фахівець з навчання науковому письму за пакетом матеріалів Манчестерського університету. Пройшла низку закордонних стажувань в кількох університетах США.</p> | |
| 438034 | Опришко Тетяна Сергіївна | Викладач, Сумісництво | Факультет педагогічної освіти | Диплом магістра, Національний педагогічний університет імені М.П. Драгоманова, рік закінчення: 2010, | 0 | Стратегії наукових досліджень (Інтернаціоналізація науки: Змістовий модуль 2. Інформаційна грамотність; | Відповідність освіти: 1. Кандидат наук із соціальних комунікацій, 27.00.03 – книгознавство, бібліотекознавство, бібліографознавство. Тема дисертації: «Українська |

спеціальність:
030501
Українська
мова та
література

Змістовий
модуль 3.
Наукові
публікації в
цифровому
середовищі)

літературно-художня періодика в УСРР (1921-1934 рр.): бібліотечно-бібліографічна реконструкція, напрями розвитку, специфіка функціонування» (ДК № 030277, 29.09.2015, Вища атестаційна комісія України). Стаж науково-педагогічної роботи: з 2010 р. на умовах погодинної оплати. Розробник та викладач Програми підвищення кваліфікації для НПП та НП за Дослідницьким модулем (за базовим та поглибленим рівнями). Наявність публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection:
1. Opryshko, T., & Nazarovets, S. (2022). Case Study: Citizen Science in Digital Humanities Context. Digital Humanities Workshop, 198–203. <https://doi.org/10.1145/3526242.3526246> (Scopus)
2. Vinnikova, N. M., Aleksandrova, O. S., Kuzmenko, O. M., Opryshko, T. S., & Karpenko, A. S. (2022). Use of Digital Tools for Checking Uniqueness by Students and Academic Staff of the Borys Grinchenko Kyiv University: Problems and Solutions. Digital Humanities Workshop, 29–36. <https://doi.org/10.1145/3526242.3526250> (Scopus)
3. Опришко, Т. С., Єрескова, Т. В., Тимофєєва, Г. В., & Литвинова, А. В. (2021). Використання інноваційних інструментів у редакційному процесі наукових журналів України. Відкрите освітнє е-середовище сучасного університету, (11), 121-129. <https://doi.org/10.28925/2414-0325.2021.1110> (категорія Б Переліку фахових МОН України)

4. Berestov, D., Kurchenko, O., Shcheblanin, Y., Korshun, N., & Opryshko, T. (2021). Analysis of Features and Prospects of Application of Dynamic Iterative Assessment of Information Security Risks. In V. Buriachok, D. Ageyev, V. Lahno, & V. Sokolov (Eds.), Proceedings of Selected Papers of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021) (Vol. 2923, pp. 329–335). CEUR. <https://ceur-ws.org/Vol-2923/#paper36> (Scopus)
5. Trush, O., Trush, M., Shincaruk, O., Radzivilov, H., & Opryshko, T. (2021). Analysis of Corporate Culture Development Parameters in the Telecommunication Enterprise Informations. B A. Bessalov, D. Ageyev, V. Lahno, & V. Sokolov (Eds.), Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II. Volume II (Vol. 3188, pp. 53–62). CEUR. <https://ceur-ws.org/Vol-3188/#paper6> (Scopus)
6. Yereskova, T., Mazuryk, O., Tymofieieva, H. ., & Opryshko, T. (2020). Social Activity of Contemporary Ukrainian Society: Threat to Internal Stability or Possibility of Social Dialogue. Postmodern Openings, 11(4), 144–173. <https://doi.org/10.18662/po/11.4/227> (Web of Science)
7. Тимофєєва, Г., & Опришко, Т. (2020). Українські університети в рейтингах публікаційної активності 2019 року. Відкрите освітнє е-середовище сучасного університету, (8), 174–190. <https://doi.org/10.28925/2414-0325.2020.8.16> (категорія Б Переліку фахових МОН України)
8. Опришко, Т., & Тимофєєва, Г. (2019).

Інтернаціоналізація як стратегія розвитку академічних бібліотек. Вісник Одеського національного університету. Бібліотекознавство, бібліографознавство, книгознавство, 24(1), 155–171.
[https://doi.org/10.18524/2304-1447-2019.1\(21\).1659349](https://doi.org/10.18524/2304-1447-2019.1(21).1659349). Опришко, Т. (2017). Етика наукових публікацій. Бібліотекознавство. Документознавство. Інформологія, (3), 50-57.
<http://journals.urau.ua/bdi/article/view/150330> (категорія Б Переліку фахових МОН України)
Наявність електронних курсів на освітніх платформах:
1. Електронний навчальний курс до змістового модуля «Інтернаціоналізація науки» навчальної дисципліни «Стратегії наукових досліджень» на платформі Moodle
<https://elearning.kubg.edu.ua/course/view.php?id=22175>
Участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена разових спеціалізованих вчених рад:
Офіційний опонент на захисті дисертації Потіхи Андрія Леонідовича «Засоби масової комунікації політичних партій в інформаційно-аналітичній діяльності бібліотек України (1990 – 2010-ті рр.)», поданої на здобуття наукового ступеня кандидата наук із соціальних комунікацій за спеціальністю 27.00.03 – книгознавство, бібліотекознавство, бібліографознавство у спеціалізованій Вченій раді К. 26.165.01 Національної бібліотеки України ім. В. І. Вернадського (2018 р.).
Виконання функцій (повноважень, обов'язків) головного редактора/члена редакційної колегії

| | | | | | | | |
|--------|---------------------------|-------------------|---|---|---|--|---|
| | | | | | | <p>наукового видання, включеного до переліку фахових видань України:</p> <p>1. Голова Науково-методичної ради бібліотеки, яка координує діяльність наукових періодичних видань Університету, а також рекомендує до друку 4 наукові фахові видання Університету: «Освітологія», Освітологічний дискурс», «Неперервна професійна освіта: теорія і практика», «The Modern Higher Education Review».</p> <p>2. Член редакційної колегії електронного фахового журналу «Синopsis: текст, контекст, медіа» (2022 р. – донині). Відомості про підвищення кваліфікації :</p> <p>1. Монреальський університет (фр. Université de Montréal – UdeM) (провінція Квебек, Канада), постдоктор (Postdoctoral position), 23.07.2022 – 23.07.2023.</p> <p>2. Університет Матея Бела (м. Банська Бистриця, Словаччина), 30.06.2018 – 30.07.2018, стажування за Національною стипендіальною програмою Словацької Республіки (SATA).</p> | |
| 357752 | Виговська Ольга Сергіївна | Доцент, Суміщення | Факультет права та міжнародних відносин | <p>Диплом магістра, Київський національний університет імені Тараса Шевченка, рік закінчення: 2010, спеціальність: 030402 Міжнародне право, Диплом магістра, Київський національний університет імені Тараса Шевченка, рік закінчення: 2009, спеціальність: 030404 Міжнародна інформація, Диплом кандидата наук ДК 015537, виданий 04.07.2013</p> | 9 | <p>Стратегії наукових досліджень (Інтернаціоналізація науки: Змістовий модуль 1. Основи інтернаціоналізації вищої освіти і науки)</p> | <p>Відповідність освіти:</p> <p>1. Київський національний університет імені Тараса Шевченка, 2009 р., спеціальність: «Міжнародна інформація», кваліфікація: «Інформаційний аналітик-міжнародник, перекладач з німецької мови».</p> <p>2. Кандидат політичних наук, 23.00.04 – політичні проблеми міжнародних систем та глобального розвитку. Тема дисертації: «Зовнішньо політичні аспекти національної безпеки України в інформаційній сфері» (ДК № 015537, 04.07.2013, Вища атестаційна комісія України).</p> |

Наявність публікацій у наукових виданнях, які включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection:

1. Виговська О. С. Фінансування академічної мобільності в Україні: проблеми і шляхи вирішення. / О.С. Виговська // Вісник Маріупольського державного університету. Серія: історія, політологія., 2016. С. 186-191. ISSN 2518-1521
2. Виговська О. С. Стратегія інтернаціоналізації як ключовий пріоритет розвитку університетської освіти. / О.С. Виговська // «Неперервна професійна освіта: теорія і практика», 2018. Журнал індексується в Index Copernicus
3. O.Vyhovska, V.Zavadnyi, O.Aleksandrova, N.Vinnikova, I.Spudka (2019) European Union Enlargement in 2004: System Analysis of the Benefits and Losses. Journal of Advanced Reseach in Law and Economics (6(44)) 2019.
<http://elibrary.kubg.edu.ua/id/eprint/31624/>
4. Vyhovska O. Social media and higher education institutions: using social networks to recruit. The Modern Higher Education Review. 2020. DOI 10.28925/2518-7635.
5. Vyhovska O. Ukrainian way to provide education in pandemic. Baltic Rim Economies.2020.
<https://sites.utu.fi/bre/ukrainian-way-to-provide-education-in-pandemic/>
6. Виговська О.С. (2022) Experience of training experts in the field of decisionmaking policy in Eastern European countries Вісник Львівського університету (42). pp. 182-189. ISSN 2307-1664

Наявність виданого підручника чи навчального посібника

(включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора):

1. Виговська О.С. Інформаційна складова національної безпеки України. / О.С. Виговська, Н.Б. Белоусова // Колективна (двоосібна). Київський університет імені Бориса Грінченка, Київ, 2017. Монографія

Рамкові міжнародні науково-дослідні проекти:

1. Модуль «Державне-міжнародне-суспільне: європейські цінності та норми, що формують завдання міждисциплінарного навчального модулю (STIPENDIUM)» № 611217-EPP-1-2019-1-UAERPMO-MODULE програми Еразмус+: Жан Моне. 01.09.2019 р. – 31.08.2022 р. Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України:

1. Керівник наукової теми «Інтернаціоналізація університетської освіти у забезпеченні якості підготовки фахівців» (2016-2023 рр, реєстраційний номер 0116U002965). Відомості про підвищення кваліфікації викладача:

1. Міжнародне стажування в Університеті Кадісу (Іспанія), 14-18.03.2022.
2. Міжнародне стажування в Університеті Гранади (Іспанія), 21-25.03.2022.
3. Міжнародне стажування в Університеті Кадісу (Іспанія), 24.04-

| | | | | | | | |
|--------|---------------------------|--------------------------------|---|--|----|--|---|
| | | | | | | | 31.08.2022. 4. Міжнародне стажування в Університеті Західної Тімішоари (Румунія), 24-28.10.2022. |
| 241471 | Баклан Олег Володимирович | Професор, Основне місце роботи | Факультет права та міжнародних відносин | Диплом спеціаліста, Українська академія внутрішніх справ, рік закінчення: 1994, спеціальність: правознавство, Диплом спеціаліста, Київський орден Леніна політехнічний інститут, рік закінчення: 1982, спеціальність: промислова теплоенергетика, Диплом доктора наук ДД 003015, виданий 14.02.2014, Атестат професора 12ПР 009937, виданий 31.10.2014 | 34 | Стратегії наукових досліджень (Нормативно-правова база наукових досліджень та наукової діяльності) | Відповідність освіти: 1. Українська академія внутрішніх справ, 1994 р., спеціальність «Правознавство», кваліфікація «Юрист». 2. Доктор юридичних наук, 12.00.07 - адміністративне право і процес; фінансове право; інформаційне право. Тема дисертації: «Адміністративно-правове регулювання підприємництва в Україні (теоретико-прикладний аспект)» (ДД № 003015, 14.02.2014, Вища атестаційна комісія України). 3. Професор кафедри цивільних дисциплін та кримінально-правових дисциплін (12 ПР № 009937, 31.10.2014, Міністерство освіти і науки України). Наявність публікацій у наукових виданнях, які включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Баклан О.В. Про міжнародні нормативно-правові акти як джерела галузевих правових наук України: окремі питання. Альманах міжнародного права. 2020. Випуск № 24. С.3-10. 2. Баклан О.В. Державний вплив на економіку та підприємництво: окремі порівняльно-правові питання. Вісник Південного регіонального центру Національної академії правових наук України – № 22 (3). 2020 – с.74-82. 3. Oleh Baklan, Yuliia Zaveriukha (2020) The ways to bring Ukraine's tax legislation to European standards European political and law discourse (7). с. 305-312. ISSN 2336-5439; 2336-5447 4. Баклан О.В. До питання правової природи та структури неправових форм |

державного управління (на прикладі сфери підприємництва). Публічне право України. 2019. № 1(33). с.56-63.

5. Баклан О.В. Про розвиток науки державного управління: історико-правовий аспект. Вісник Південного регіонального центру Національної академії правових наук України. № 18 (2019). с. 14-22.

6. Баклан О.В. Про поняття, структуру та різновиди адміністративно-правових відносин. Вісник Південного регіонального центру Національної академії правових наук України. 2018. № 14. с. 80-87.

7. Баклан О.В. Деякі коментарі щодо характеристики правового статусу окремих суб'єктів адміністративного права (частина 1). Публічне право України. 2018. № 1. с. 52-59.

8. Баклан О.В. Деякі коментарі щодо характеристики правового статусу окремих суб'єктів адміністративного права (частина 2). Публічне право України. 2018. № 2. с. 89-94.

Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії:

1. Баклан, Олег Володимирович (2020) Державна присутність у господарсько-правових відносинах: монографія. Одноосібна. Видавництво Людмила, Київ, 2020. – 208 с.

Робота у складі складі галузевої експертної ради як експерта Національного агентства із забезпечення якості вищої освіти, або у складі Акредитаційної комісії, або міжгалузевої експертної ради з вищої освіти Акредитаційної комісії, або

експертних комісій
МОН/зазначеного
Агентства, або
Науково-методичної
ради/науково-
методичних комісій
(підкомісій) з вищої
або фахової
передвищої освіти
МОН,
наукових/науково-
методичних/експертн
их рад органів
державної влади та
органів місцевого
самоврядування, або у
складі комісій
Державної служби
якості освіти із
здійснення планових
(позапланових)
заходів державного
нагляду (контролю)
1. Член експертної
групи по проведенню
чергової
акредитаційної
експертизи у ПНВЗ
“Київський
міжнародний
університет”
08.12.2017 р.
Наявність
апробаційних та/або
науково-популярних,
та/або
консультаційних
(дорадчих), та/або
науково-експертних
публікацій з наукової
або професійної
тематики:
1.Баклан О.В.
Довідник
«Адміністративно-
правова наука та
освіта в персоналіях»
2020 р. /
http://lsej.org.ua/dovidnyk_admin.law.education.pdf. С. 9.
Відомості про
підвищення
кваліфікації
викладача:
1. Київський
університет імені
Бориса Грінченка,
сертифікат про
проходження
Лідерського модуля
від 03.10.2018
№867Л, 1 кредит
ECTS (30 год.).
2. Київський
університет імені
Бориса Грінченка,
сертифікат про
проходження Модуля
з ІКТ від 03.10.2018
№831Л, 1 кредит ECTS
(30 год.).
3. Київський
університет імені
Бориса Грінченка,
сертифікат про
проходження
Дидактичного модуля
від 03.10.2018
№784Л, 1 кредит
ECTS (30 год.).

| | | | | | | | |
|--------|---------------------------------|--------------------------------|--|--|----|--|--|
| | | | | | | 4. ДВНЗ «Київський національний економічний університет», довідка про проходження Фахового модуля (стажування) від 04.06.2019 №18/27-006 (з 08.04.2019 по 08.05.2019). | |
| 137352 | Бессалов Анатолій Володимирович | Професор, Основне місце роботи | Факультет інформаційних технологій та математики | Диплом доктора наук ДН 000735, виданий 24.12.1993, Атестат професора ПР 001510, виданий 22.06.1994 | 60 | Прикладні аспекти створення та застосування систем криптографічного захисту | Відповідність освіти: 1. Київське вище інженерно-авіаційне військово училище ВПС, 1968 р., спеціальність: «Радіотехнічні засоби пілотованих повітряних і космічних літальних апаратів», кваліфікація: військовий інженер з радіотехніки. 2. Доктор технічних наук, 20.02.14 – озброєння та військова техніка. Тема дисертації: спеціальна. (ДН № 000735, 24.12.1993, Вища атестаційна комісія України). 3. Професор кафедри бортових систем радіозв'язку та радіонавігації, (ПР № 001510, 22.06.1994, Міністерство освіти України). Наявність публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, 1. Бессалов А.В., Ковальчук Л.В., Кучинська Н.В., Теліженко О.Б. Безпека модифікованого цифрового підпису з відкритим ключем EDDSA // Радіотехніка, 198. (2019) с. 209-215. 2. Бессалов А.В., Котенко А.М., Третьяков Д.Б. (2019) Складність обчислення 3- і 5-ізогеній суперсингулярних кривих Едвардса Сучасний захист інформації (4(40)). с. 63-69. 3. Bessalov, A., Kovalchuk, L., Sokolov, V., Skladannyi, P., Radivilova, T. Analysis of 2-isogeny properties of generalized form edwards curves. CEUR Workshop Proceedings, 2020, 2746, стр. 1–13 4. Bessalov A., Grubiyani E., Sokolov |

V., Skladanniy P. 3- i 5- izogēnii supersingulyarnykh kryvykh Edvardsa // Kiberbezpeka: osvita, nauka, tekhnika (8). (2020) s. 6-21.

5. A. Bessalov, V. Sokolov, P. Skladanniy. Modeling of 3- and 5- Isogenies of Supersingular Edwards Curves // Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS'2020), June 2-3, 2020: abstracts. - No. I, vol. 2631. - Aachen : CEUR, 2020. - P. 30-39.

6. Бессалов А.В. Алгоритми і оцінки складності обчислень 3- і 5-ізогеній суперсингулярних кривих Едвардса // Радіотехніка, 200. (2020) с. 37-50.

7. Bessalov A., Sokolov V., Skladanniy P., Zhyltsov O. Computing of odd degree isogenies on supersingular twisted edwards curves. CEUR Workshop Proceedings , 2021, 2923, стр. 1-11.

Нааявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора):

1. Еліптичні криві у формі Едвардса та криптографія. Монографія. «Політехніка», Київ, 2017. - 272 с.

Наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня:

1. Циганкова О.В. Методи підвищення швидкодії асиметричних криптосистем з використанням еліптичних кривих у формі Едвардса: Дисертація на здобуття наукового ступеня канд.техн.наук: 05.13.21 / Київський національний

| | | | | | | | |
|-------|---------------------------|---|-------------------------------|--|----|---|--|
| | | | | | | <p>технічний університет України «КПІ» імені Ігоря Сікорського – Київ, 2021.</p> <p>Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах:</p> <p>1. Керівник науково-дослідної теми «Євсуг» за завданням ДССЗЗІ України з метою створення 3-х державних стандартів України у сфері криптографії (тема спеціальна) (2018-2020рр)., У 2020 р. затверджено стандарт ДСТУ 9041:2020 Інформаційні технології. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса. Підвищення кваліфікації:</p> <p>1. ТОВ «РДЛ», сертифікат про підвищення кваліфікації «Повний курс навчання по роботі зі шлюзом законного перехоплення для PS core компанії Huawei» від 2018 р. № 012/2018, 4 кредити ECTS (144 год.).</p> | |
| 11523 | Хоружа Людмила Леонідівна | Завідувач кафедри, Основне місце роботи | Факультет педагогічної освіти | Диплом доктора наук ДД 004216, виданий 09.03.2005, Атестат професора 12ІП 004760, виданий 19.04.2007 | 33 | Філософія і методологія наукової діяльності (Наукова етика) | Відповідність освіти: 1. Доктор педагогічних наук, 13.00.04 – теорія і методика професійної освіти. Тема дисертації: «Теоретичні засади формування етичної компетентності майбутніх учителів початкових класів» (ДД № 004216, 09.03.2005, Міністерство освіти і науки України). 2. Професор кафедри педагогіки (12ІП № |

007955, 26.09.2012, Міністерство освіти і науки України).
Наявність публікацій у наукових виданнях, які включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection:

1. Liudmyla Khoruzha, Mariia Bratko, Olha Kotenko, Olha Melnychenko, Volodymyr Proshkin. (2019) The Study of the Higher School Lecturer's Competence in Ukraine: Diagnostics and Analytics The New Education Review (55(1)). pp. 233-245. ISSN 1732-6729. (SCOPUS)
2. L.Khoruzha, V. Proshkin, O. Kotenko, E.Smyrnova-Trybulska Digital competence: abilities of a lecturer and expectations of students (Ukrainian-Polish context). E-learning and stem education, 2019. Vol. 11. PP. 421-441. (WOS).
3. Хоружа Л.Л., Прошкін В.В., Глушак О.М. Компетентнісний розвиток викладачів вищої школи засобами цифрових технологій. Інформаційні технології і засоби навчання, 2020. Том 78, № 4. 298-314. <https://journal.iitta.gov.ua/index.php/itlt/article/view/3042> (WOS).
4. Хоружа Л.Л. (2020) Сучасні стратегії трансформації змісту педагогічної освіти. Педагогічна освіта: теорія і практика. Психологія. Педагогіка. (33). с. 8-16.
5. Bratko, Mariia та Khoruzha, Liudmyla (2020) The research on educational environment of institution of higher education involving experts: results and analysis. SHS Web of Conferences 75, 02003 (2020) ICHTML 2020 (75). с. 1-6.
6. Хоружа, Людмила Леонідівна та Мельниченко, Ольга Володимирівна (2020) Academic staff`s social-personal dominant activity Society, integration, education. Proceedings of the

International Scientific Conference (1). с. 385-396.
7. Хоружа, Людмила Леонідівна (2021) Соціально-психологічні аспекти переходу педагогічного знання в інновацію. Освітологічний дискурс (4(35)). с.103-117.
8. Хоружа Л.Л. (2018) Intercultural education at the university: from theory to practice Acta Universitatis Nicolai Copernici (35). с. 139-154.
9. Хоружа Л.Л. Тадеуш О. М. (2020) Теорія і методологія неперервної професійної освіти Неперервна професійна освіта: теорія і практика (1(62)). с. 7-16.
10. Хоружа, Людмила Леонідівна (2021) Елективність як провідний принцип освіти дорослих. Педагогічна освіта: теорія і практика. Психологія. Педагогіка. (35(1)). с. 6-11. ISSN 2311-2409; 2412-2009.
11. Хоружа Л.Л. (2017) Педагогіка вищої школи: сучасні дидактичні стратегії Неперервна професійна освіта: теорія і практика. ISSN 1609-8595
12. Хоружа Л.Л. (2017) Конструктивний підхід у навчанні: з досвіду діяльності центрів компетентностей у європейських університетах Вища школа (8). с. 57-67. ISSN 1682 -2366
13. Хоружа Л.Л. (2017) Аксіологічні орієнтири професійної підготовки педагога (наукові ідеї доктора педагогічних наук, професора, академіка НАПН України О.Я. Савченко) Педагогічна освіта: теорія і практика. Психологія. Педагогіка (28). с. 12 - 15. ISSN 2311 -2409
14. Хоружа Л.Л. (2016) У пошуках нової педагогіки: критичний аналіз Неперервна професійна освіта: теорія і практика (3-4). с. 7-11. ISSN 1609-

8595
15. Хоружа Л.Л. (2016)
Професійна діяльність
учителя крізь призму
педагогічної
інноватики
Педагогічна освіта:
теорія і практика. с.
34-39. ISSN 2311-2409
16. Хоружа Л.Л. (2016)
"Науки про освіту": чи
є в них місце
педагогіці? Вища
школа (6). с. 30-39.
ISSN 1682-2366
Наявність свідоцтв
про реєстрацію
авторського права на
твір:
1. Хоружа Л.Л.
Соціологія виховання
особистості.
Навч. посібник. -К.:
Київський університет
імені Бориса
Грінченка. Авторське
свідоцтво № 72614 (2017 р.).
2. Хоружа Л.Л.
«Науки про освіту» -
чи є в них місце
педагогіці? Вища
школа. №6 (146). С.30-
40. Авторське
свідоцтво № 72623
(2017 р.)
3. Л. Хоружа, М.
Братко, О. Котенко, О.
Мельниченко, В.
Прошкін. Компетенції
викладачів вищої
школи в добу змін:
діагностика та
аналітика (за
результатами
дослідження в
Київському
університеті імені
Бориса Грінченка)
Колективна (три і
більше авторів).
Київський ун-т імені
Бориса Грінченка,
Київ, 2018. 92 с.
Авторське свідоцтво
№ 81084 (2018 р.)
4. L.Khoruzha, V.
Proshkin. Distance
learning: on the way to
developing a new
didactic model of
university education
Колективна (три і
більше авторів).
Innovative Educational
Technologies, Tools and
Methods for E-learning:
Monograph. Studio
NDA, Katowice–
Cieszyn. 171-182 с.
Авторське свідоцтво
№ 105791 (2021 р.).
5. Хоружа Л.Л.,
Прошкін В.В., Глушак
О.М. Компетентнісний
розвиток викладачів
вищої школи
засобами цифрових
технологій.
Інформаційні
технології і засоби

навчання, 2020. Том 78, №4. 298-314.
Авторське свідоцтво № 105787 (2021 р.).
Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії:
1. Хоружа Л.Л. Інваріантність та варіативність професійної діяльності викладача вищої школи в епоху змін. Теорія та методика професійно-педагогічної підготовки освітянських кадрів: акмеологічні аспекти : монографія / керівн. авт. кол. Н. В. Гузій ; Мін-во освіти і науки України, Нац. пед. ун-т імені М. П. Драгоманова. – Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. – 516 с.
2. Хоружа Л.Л. High School Teacher Competence in Change (according to the results of the project of the International Visegrad Fund “High School Teacher Competence in Change” No. 21720008) / [Doctor of Pedagogical Sciences, professor L. Khoruzha (ed.)]. – Kyiv: Borys Grinchenko Kyiv University, 2019. - 96 p.
3. Хоружа, Людмила Леонідівна та Прошкін, Володимир Вадимович (2020) Distance learning: on the way to developing a new didactic model of university education Колективна (три і більше авторів). Innovative Educational Technologies, Tools and Methods for E-learning: Monograph. Studio NDA, Katowice–Cieszyn.
4. Прошкін, Володимир Вадимович та Хоружа, Людмила Леонідівна та Семеніхіна, Олена (2021) Теорія і практика професійної підготовки майбутніх учителів математики та інформатики засобами цифрових технологій Колективна (три і більше авторів). Теоретичні та практичні аспекти використання математичних методів

та інформаційних технологій в освіті й науці: монографія. Київ. ун-т ім. Б. Грінченка, Київ. Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/робочих програм, інших друкованих навчально-методичних праць:

1. Хоружа Л. Л. (2017) Соціологія виховання особистості. Київський університет імені Бориса Грінченка, Київ, Україна. 148 с.
2. Мерзлякова О.Л., Хоружа Л.Л. (2020) Практикум з критичного мислення. Київський університет імені Бориса Грінченка, Київ, Україна. 160 с.

Наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня:

1. Братко М.В. Теоретичні і методичні засади управління професійною підготовкою фахівців в освітньому середовищі університетського коледжу : Дис... докт.пед.наук: 13.00.04/ 13.00.06 /Державний вищий навчальний заклад "Університет менеджменту освіти" НАПН України. – Київ, 2019.
2. Співакова І.Б. Інноваційний розвиток вчителя в системі методичної роботи закладу середньої освіти: Дис... канд.пед.наук: 13.00.04 /Київський університет імені Бориса Грінченка. – Київ, 2020.

Участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена разових

спеціалізованих
вчених рад:

1. Голова спеціалізованої Вченої ради Д 26.133.06 в Київському університеті імені Бориса Грінченка з правом прийняття до розгляду та проведення захисту дисертацій на здобуття наукового ступеня доктора (кандидата) педагогічних наук за спеціальністю 13.00.04 «Теорія і методика професійної освіти» (2019-2021 рр.).
2. Член спеціалізованої Вченої ради К 26.133.01 з правом прийняття до розгляду та проведення захисту дисертацій на здобуття наукового ступеня кандидата педагогічних наук за спеціальностями 13.00.01 та 13.00.05.
3. Голова разових спеціалізованих рад зі спеціальності 011 Освітні/Педагогічні науки у 2020-2021 рр.:
ДФ
26.133.001;26.133.002;26.133.003;26.133.012.

Офіційний опонент кандидатських дисертацій:

1. Шовш К.С.
Формування академічної культури майбутніх педагогічних працівників у закладах вищої освіти [Текст] : автореферат дис. ... канд. пед. наук : 13.00.04 "Теорія і методика професійної освіти" / Джура О. Д. ; Нац. пед. ун-т ім. М.П. Драгоманова . - Київ, 2019. - 20 с.

Офіційний опонент докторських дисертацій:

1. Журба К.О.
Теоретико-методичні засади виховання смисложиттєвих цінностей у школярів основної і старшої школи [Текст] : автореферат дис. ... докт. пед. наук : 13.00.07 "Теорія і методика виховання" / Бех І.Д. ; Нац. акад. пед. наук України, Ін-т проблем виховання.- Київ, 2019. - 40 с.
2. Цюняк О.П.
Система підготовки майбутніх магістрів початкової освіти до

інноваційної діяльності [Текст] : автореферат дис. ... докт. пед. наук : 13.00.04 "Теорія і методика професійної освіти" / Хомич Л.О.; Нац. акад. пед. наук України, Ін-т п педагогічної освіти і освіти дорослих імені Івана Зязюна.-Київ, 2020.-40 с.

Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України:

1. Керівник науково-дослідної теми кафедри теорії та історії педагогіки «Зміст і технології забезпечення якості неперервної педагогічної освіти в умовах євроінтеграції» (2015-2020 рр., Реєстраційний номер 0116U003295); з березня 2021 р. - керівник нової наукової теми кафедри теорії та історії педагогіки «Інноваційність розвитку вищої педагогічної освіти у міждисциплінарному вимірі» (реєстраційний №012U000123).
2. Член редколегії наукового фахового збірника «Педагогічна освіта: теорія і практика» (Психологія, Педагогіка) (категорія Б).

Робота у складі експертної ради з питань проведення експертизи дисертацій МОН або у складі галузевої експертної ради як експерта Національного агентства із забезпечення якості вищої освіти, або у складі Акредитаційної комісії, 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
або фахової
передвищої освіти
МОН,
наукових/науково-
методичних/експертн
их рад органів
державної влади та
органів місцевого
самоврядування, або у
складі комісій
Державної служби
якості освіти із
здійснення планових
(позапланових)
заходів державного
нагляду (контролю):
1. Експерт НАЗЯВО зі
спеціальності 011
Освітні /Педагогічні
науки;
2. Член предметної
(галузевої) експертної
комісії МОН України з
етики та предметів
морально-духовного
спрямування (наказ
МОН України № 95
від 22.01.2021 р.)
3. Член
координаційної ради
зі спеціальності
13.00.04 – теорія і
методика професійної
освіти Міжвідомчої
ради з координації
наукових досліджень у
галузі педагогіки і
психології НАПН
України.
Участь у міжнародних
наукових та/або
освітніх проектах:
1. «Компетенції
викладача вищої
школи в добу змін»
(01.01.2018 –
31.12.2018 р) – малий
грант Вишеградського
фонду № 21720008
(координатор
проекту).
2. «Навчай для
України» (2017-
2021р.) - Меморандум
про співпрацю між
Київським
університетом імені
Бориса Грінченка та
Громадською
організацією «Навчай
для України»
(розробник освітньої
програми,
координатор).
Наукове
консультування
підприємств, установ,
організацій, що
здійснювалося на
підставі договору із
закладом вищої освіти
(науковою
установою):
1. Член експертної

комісії з проведення дослідно-експериментальної роботи у закладах освіти м. Києва (2015-2020).

Наявність апробаційних та/або науково-популярних публікацій з наукової або професійної тематики:

1. Хоружа Л. Л., Мельниченко О. В. (2020) Academic staff's social-personal dominant activity Society, integration, education. Proceedings of the International Scientific Conference (1). с. 385-396.
2. Bratko M., Khoruzha L. (2020) The research on educational environment of institution of higher education involving experts: results and analysis. SHS Web of Conferences 75, 02003 (2020) ICHTML 2020 (75). с. 1-6.
3. Хоружа Л.Л. (2019) Як залучати молодь до педагогічної науки: досвід наукової школи. Збірник наукових праць «Педагогічні науки». с. 156-161.
4. Хоружа Л.Л. (2017) Аксіологічні орієнтири професійної підготовки педагога (наукові ідеї доктора педагогічних наук, професора, академіка НАПН України О.Я. Савченко) Педагогічна освіта: теорія і практика. Психологія. Педагогіка (28). с. 12-15.
5. Хоружа Л.Л. (2017) Конструктивний підхід у навчанні: з досвіду діяльності центрів компетентностей у європейських університетах . Вища школа (8). с. 57-67.

Участь у журі:

1. Голова журі Всеукраїнського турніру школярів з філософії та етики (2017, 2018, 2019 рр.)

Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях:

1. Член Української академії акмеології (з 2015 р. донині).

Відомості про підвищення

| | | | | | | |
|--|--|--|--|--|--|--|
| | | | | | | <p>кваліфікації викладача:</p> <p>1. Львівський політехнічний національний університет (м. Львів), участь в осінній школі «Transfer of Technologies and Innovations: European and Ukrainian Experiences» в рамках модульної програми фонду Жан Моне «Європейський досвід трансферу технологій для українських університетів», 10.11.2021 р., 1 кредит ECTS (30 год.).</p> <p>2. Київський університет імені Бориса Грінченка, сертифікат про проходження Дидактичного модуля від 26.02.2021 №1485/21, 1 кредит ECTS (30 год.).</p> <p>3. НАПН України (відділення загальної педагогіки та філософії освіти), довідка про підвищення кваліфікації (фаховий модуль) від 02.03.2021 № 2-7/18 р., 6 кредитів ECTS (180 год.).</p> <p>У 2016 році запрошувалась як гостьовий професор для викладання питань педагогічної етики у Сілезькому університеті в м. Катовіце.</p> |
|--|--|--|--|--|--|--|

Таблиця 3. Матриця відповідності програмних результатів навчання, освітніх компонентів, методів навчання та оцінювання

| Програмні результати навчання ОП | ПРН відповідає результату навчання, визначено му стандартом вищої освіти (або охоплює його) | Обов'язкові освітні компоненти, що забезпечують ПРН | Методи навчання | Форми та методи оцінювання |
|--|---|--|---|---|
| ПРН 5 Розробляти та аналізувати проекти ІКС базуючись на стандартизованих технологіях та протоколах передачі даних. Аналізувати та визначати можливість застосування технологій, | <input type="checkbox"/> | Прикладні аспекти протидії кібератакам в соціотехнічних системах | Аналіз, синтез, порівняння, індукція, дедукція, лекція, навчальні дискусії, мозковий штурм, моделювання, самоаналіз взаємоаналіз, термінологічний аналіз, рефлексивний аналіз, мікрОВикладання. | Самооцінювання, взаємооцінювання, усне опитування, перевірка та аналіз виконаних завдань, індивідуальні бесіди про результати виконання завдань, залік. |

методів та засобів КТЗІ в ІКС.
Проектувати та реалізовувати комплексні системи КТЗІ в ІКС відповідно до вимог чинних нормативно-правових документів систем захисту інформації.
Вирішувати задачі впровадження, супроводу та управління комплексними системами захисту інформації в ІКС, проведення їх експертизи та випробувань.
Забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту.
ПРН 6 Розробляти та впроваджувати дослідницькі проекти в сфері захисту інформації, інформаційної та кібербезпеки.
Розробляти алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки.
Здійснювати захист ресурсів і процесів в ІКС на основі моделей безпеки та встановлених режимів їх безпечного функціонування.
Забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ.
Забезпечувати

| | | | | |
|---|--------------------------|--|--|--|
| <p>функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф. <i>ПРН 7</i> Вирішувати задачі централізованого і децентралізованого адміністрування доступом до IP і процес ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них. Володіти науково-організаційними основами проведення аудиту безпеки ІКС, а також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в ІТ системах та мережах.</p> | | | | |
| <p><i>ПРН 5</i> Розробляти та аналізувати проекти ІКС базуючись на стандартизованих технологіях та протоколах передачі даних. Аналізувати та визначати можливість застосування технологій, методів та засобів КТЗІ в ІКС. Проектувати та реалізовувати комплексні системи КТЗІ в ІКС відповідно до вимог чинних нормативно-правових документів систем захисту інформації. Вирішувати задачі впровадження, супроводу та управління комплексними системами захисту інформації в ІКС, проведення їх експертизи та випробувань. Забезпечувати процеси захисту інформаційно-комунікаційних</p> | <input type="checkbox"/> | <p>Технології безпеки складних соціотехнічних систем</p> | <p>Аналіз, синтез, порівняння, індукція, дедукція, лекція, навчальні дискусії, мозковий штурм, моделювання, самоаналіз взаємоаналіз, термінологічний аналіз, рефлексивний аналіз, мікрорікладання.</p> | <p>Самооцінювання, взаємооцінювання, усне опитування, перевірка та аналіз виконаних завдань, індивідуальні бесіди про результати виконання завдань, залік.</p> |

систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту.
ПРН 6 Розробляти та впроваджувати дослідницькі проекти в сфері захисту інформації, інформаційної та кібербезпеки.
Розробляти алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки.
Здійснювати захист ресурсів і процесів в ІКС на основі моделей безпеки та встановлених режимів їх безпечного функціонування.
Забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ.
Забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф.
ПРН 7 Вирішувати задачі централізованого і децентралізованого адміністрування доступом до ІР і процес ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них.
Володіти науково-

| | | | | |
|--|--------------------------|--|--|--|
| <p>організаційними основами проведення аудиту безпеки ІКС, а також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в ІТ системах та мережах.</p> | | | | |
| <p>ПРН 4 Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності. Проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД. Обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах. Використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів. ПРН 7 Вирішувати задачі централізованого і децентралізованого адміністрування</p> | <input type="checkbox"/> | <p>Прикладні аспекти управління інформаційною та кібербезпекою об'єктів критичної інфраструктури</p> | <p>Аналіз, синтез, порівняння, індукція, дедукція, лекція, навчальні дискусії, мозковий штурм, моделювання, самоаналіз взаємоаналіз, термінологічний аналіз, рефлексивний аналіз, мікровикладання.</p> | <p>Самооцінювання, взаємооцінювання, усне опитування, перевірка та аналіз виконаних завдань, індивідуальні бесіди про результати виконання завдань, екзамен.</p> |

| | | | | |
|--|--------------------------|---|--|--|
| <p>доступом до IP і процес ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них. Володіти науково-організаційними основами проведення аудиту безпеки ІКС, а також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в IT системах та мережах.</p> | | | | |
| <p>ПРН 4 Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності. Проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД. Обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в IT системах та мережах. Використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а</p> | <input type="checkbox"/> | <p>Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів</p> | <p>Аналіз, синтез, порівняння, індукція, дедукція, лекція, навчальні дискусії, мозковий штурм, моделювання, самоаналіз взаємоаналіз, термінологічний аналіз, рефлексивний аналіз, мікрОВикладання.</p> | <p>Самооцінювання, взаємооцінювання, усне опитування, перевірка та аналіз виконаних завдань, індивідуальні бесіди про результати виконання завдань, екзамен.</p> |

| | | | | |
|---|--------------------------|---|--|--|
| <p>також наукових досліджень вищих рівнів. ПРН 7 Вирішувати задачі централізованого і децентралізованого адміністрування доступом до ІР і процес ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них. Володіти науково-організаційними основами проведення аудиту безпеки ІКС, а також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в ІТ системах та мережах.</p> | | | | |
| <p>ПРН 4 Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності. Проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД. Обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах. Використовувати сучасні техніки для проведення досліджень за напрямом захисту</p> | <input type="checkbox"/> | <p>Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем</p> | <p>Аналіз, синтез, порівняння, індукція, дедукція, лекція, навчальні дискусії, мозковий штурм, моделювання, самоаналіз взаємоаналіз, термінологічний аналіз, рефлексивний аналіз, мікровикладання.</p> | <p>Самооцінювання, взаємооцінювання, усне опитування, перевірка та аналіз виконаних завдань, індивідуальні бесіди про результати виконання завдань, залік.</p> |

| | | | | |
|--|---------------------------------|--|--|--|
| <p>інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів. ПРН 7 Вирішувати задачі централізованого і децентралізованого адміністрування доступом до IP і процес ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них. Володіти науково-організаційними основами проведення аудиту безпеки ІКС, а також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в IT системах та мережах.</p> | | | | |
| <p>ПРН 4 Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності. Проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД. Обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що</p> | <p><input type="checkbox"/></p> | <p>Організація захисту розподілених інформаційних ресурсів</p> | <p>Аналіз, синтез, порівняння, індукція, дедукція, лекція, навчальні дискусії, мозковий штурм, моделювання, самоаналіз взаємоаналіз, термінологічний аналіз, рефлексивний аналіз, мікровикладання.</p> | <p>Самооцінювання, взаємооцінювання, усне опитування, перевірка та аналіз виконаних завдань, індивідуальні бесіди про результати виконання завдань, залік.</p> |

| | | | | |
|--|--------------------------|---|--|--|
| <p>циркулює в ІТ системах та мережах. Використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів. ПРН 7 Вирішувати задачі централізованого і децентралізованого адміністрування доступом до ІР і процес ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них. Володіти науково-організаційними основами проведення аудиту безпеки ІКС, а також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в ІТ системах та мережах.</p> | | | | |
| <p>ПРН 4 Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності. Проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення</p> | <input type="checkbox"/> | <p>Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем</p> | <p>Аналіз, синтез, порівняння, індукція, дедукція, лекція, навчальні дискусії, мозковий штурм, моделювання, самоаналіз взаємоаналіз, термінологічний аналіз, рефлексивний аналіз, мікровикладання.</p> | <p>Самооцінювання, взаємооцінювання, усне опитування, перевірка та аналіз виконаних завдань, індивідуальні бесіди про результати виконання завдань, залік.</p> |

інформаційної та/або кібербезпеки ОІД. Обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах. Використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.

ПРН 5 Розробляти та аналізувати проекти ІКС базуючись на стандартизованих технологіях та протоколах передачі даних. Аналізувати та визначати можливість застосування технологій, методів та засобів КТЗІ в ІКС. Проектувати та реалізовувати комплексні системи КТЗІ в ІКС відповідно до вимог чинних нормативно-правових документів систем захисту інформації. Вирішувати задачі впровадження, супроводу та управління комплексними системами захисту інформації в ІКС, проведення їх експертизи та випробувань. Забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту.

ПРН 6 Розробляти та впроваджувати дослідницькі проекти в сфері захисту

| | | | | |
|---|--------------------------|--|---|---|
| <p>інформації, інформаційної та кібербезпеки. Розробляти алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки. Здійснювати захист ресурсів і процесів в ІКС на основі моделей безпеки та встановлених режимів їх безпечного функціонування. Забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ. Забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф.</p> | | | | |
| <p>ПРН 4 Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності. Проводити або</p> | <input type="checkbox"/> | Проектування і впровадження захищених інформаційно-комунікаційних систем | Аналіз, синтез, порівняння, індукція, дедукція, лекція, навчальні дискусії, мозковий штурм, моделювання, самоаналіз взаємоаналіз, термінологічний аналіз, рефлексивний аналіз, мікровикладання. | Самооцінювання, взаємооцінювання, усне опитування, перевірка та аналіз виконаних завдань, індивідуальні бесіди про результати виконання завдань, залік. |

керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД. Обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах. Використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.

ПРН 5 Розробляти та аналізувати проекти ІКС базуючись на стандартизованих технологіях та протоколах передачі даних. Аналізувати та визначати можливість застосування технологій, методів та засобів КТЗІ в ІКС.

Проектувати та реалізовувати комплексні системи КТЗІ в ІКС відповідно до вимог чинних нормативно-правових документів систем захисту інформації.

Вирішувати задачі впровадження, супроводу та управління комплексними системами захисту інформації в ІКС, проведення їх експертизи та випробувань.

Забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та

| | | | | |
|---|--------------------------|------------------------------|--|--|
| <p>програмно-апаратних комплексів засобів захисту. ПРН 6 Розробляти та впроваджувати дослідницькі проекти в сфері захисту інформації, інформаційної та кібербезпеки. Розробляти алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки. Здійснювати захист ресурсів і процесів в ІКС на основі моделей безпеки та встановлених режимів їх безпечного функціонування. Забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ. Забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф.</p> | | | | |
| <p>ПРН 1 Застосовувати знання держаної та іноземних мов для забезпечення ефективності професійної комунікації. ПРН 2 Здійснювати інформаційний пошук. Аналізувати потреби, пов'язані з науковими дослідженнями, з розвитком загальних</p> | <input type="checkbox"/> | <p>Дослідницька практика</p> | <p>Словесні, наочні, практичні, логічні (аналіз і синтез, індукція і дедукція, моделювання, системний аналіз, спостереження і експеримент), інтерактивні методи.</p> | <p>Усне опитування, презентація, виступ на конференції, методи практичного контролю, звіт з практики, залік.</p> |

компетентностей фахівців і професіоналів із захисту інформації, інформаційної та/або кібербезпеки. Реалізовувати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, застосовуючи їх як в побуті, так і в професійній діяльності.

ПРН 3 Виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією.

ПРН 4 Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності.

Проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД. Обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ

| | | | | |
|---|---------------------------------|-------------------------------------|--|---|
| <p>системах та мережах. Використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.</p> | | | | |
| <p>ПРН 1 Застосовувати знання держаної та іноземних мов для забезпечення ефективності професійної комунікації. ПРН 2 Здійснювати інформаційний пошук. Аналізувати потреби, пов'язані з науковими дослідженнями, з розвитком загальних компетентностей фахівців і професіоналів із захисту інформації, інформаційної та/або кібербезпеки. Реалізовувати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, застосовуючи їх як в побуті, так і в професійній діяльності. ПРН 3 Виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією. ПРН 4 Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або</p> | <p><input type="checkbox"/></p> | <p>Науково-викладацька практика</p> | <p>Словесні, наочні, практичні, логічні (аналіз і синтез, індукція і дедукція, моделювання, системний аналіз, спостереження і експеримент), інтерактивні методи.</p> | <p>Усне опитування, презентація, виступ на конференції, методи практичного контролю, звіт з практики, залік. залік.</p> |

| | | | | |
|--|--------------------------|--|--|--|
| <p>кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності. Проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД. Обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах. Використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.</p> | | | | |
| <p>ПРН 6 Розробляти та впроваджувати дослідницькі проекти в сфері захисту інформації, інформаційної та кібербезпеки. Розробляти алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки. Здійснювати захист ресурсів і процесів в ІКС на основі моделей безпеки та встановлених режимів їх безпечного функціонування.</p> | <input type="checkbox"/> | <p>Прикладні аспекти теорій ризиків, конфліктів і катастроф в системах безпеки</p> | <p>Аналіз, синтез, порівняння, індукція, дедукція, лекція, навчальні дискусії, мозковий штурм, моделювання, самоаналіз взаємоаналіз, термінологічний аналіз, рефлексивний аналіз, мікровикладання.</p> | <p>Самооцінювання, взаємооцінювання, усне опитування, перевірка та аналіз виконаних завдань, індивідуальні бесіди про результати виконання завдань, залік.</p> |

| | | | | |
|--|---------------------------------|--|--|--|
| <p><i>Забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ.</i></p> <p><i>Забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф.</i></p> | | | | |
| <p><i>ПРН 4</i></p> <p><i>Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів.</i></p> <p><i>Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності.</i></p> <p><i>Проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД.</i></p> <p><i>Обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах.</i></p> <p><i>Використовувати</i></p> | <p><input type="checkbox"/></p> | <p>Прикладні аспекти створення та застосування систем криптографічного захисту</p> | <p>Аналіз, синтез, порівняння, індукція, дедукція, лекція, навчальні дискусії, мозковий штурм, моделювання, самоаналіз взаємоаналіз, термінологічний аналіз, рефлексивний аналіз, мікрОВикладання.</p> | <p>Самооцінювання, взаємооцінювання, усне опитування, перевірка та аналіз виконаних завдань, індивідуальні бесіди про результати виконання завдань, залік.</p> |

сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.

ПРН 5 Розробляти та аналізувати проекти ІКС базуючись на стандартизованих технологіях та протоколах передачі даних. Аналізувати та визначати можливість застосування технологій, методів та засобів КТЗІ в ІКС. Проектувати та реалізовувати комплексні системи КТЗІ в ІКС відповідно до вимог чинних нормативно-правових документів систем захисту інформації. Вирішувати задачі впровадження, супроводу та управління комплексними системами захисту інформації в ІКС, проведення їх експертизи та випробувань. Забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту.

ПРН 6 Розробляти та впроваджувати дослідницькі проекти в сфері захисту інформації, інформаційної та кібербезпеки. Розробляти алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки.

| | | | | |
|---|--------------------------|--|--|--|
| <p>Здійснювати захист ресурсів і процесів в ІКС на основі моделей безпеки та встановлених режимів їх безпечного функціонування. Забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ. Забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф.</p> | | | | |
| <p>ПРН 4 Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності. Проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД.</p> | <input type="checkbox"/> | <p>Прикладні аспекти створення та застосування систем технічного захисту</p> | <p>Аналіз, синтез, порівняння, індукція, дедукція, лекція, навчальні дискусії, мозковий штурм, моделювання, самоаналіз взаємоаналіз, термінологічний аналіз, рефлексивний аналіз, мікровикладання.</p> | <p>Самооцінювання, взаємооцінювання, усне опитування, перевірка та аналіз виконаних завдань, індивідуальні бесіди про результати виконання завдань, залік.</p> |

Обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах.

Використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.

ПРН 5 Розробляти та аналізувати проекти ІКС базуючись на стандартизованих технологіях та протоколах передачі даних. Аналізувати та визначати можливість застосування технологій, методів та засобів КТЗІ в ІКС.

Проектувати та реалізовувати комплексні системи КТЗІ в ІКС відповідно до вимог чинних нормативно-правових документів систем захисту інформації.

Вирішувати задачі впровадження, супроводу та управління комплексними системами захисту інформації в ІКС, проведення їх експертизи та випробувань.

Забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту.

ПРН 6 Розробляти та впроваджувати дослідницькі проекти в сфері захисту інформації, інформаційної та кібербезпеки.

| | | | | |
|--|--------------------------|---|--|---|
| <p>Розробляти алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки. Здійснювати захист ресурсів і процесів в ІКС на основі моделей безпеки та встановлених режимів їх безпечного функціонування. Забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ. Забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф.</p> | | | | |
| <p><i>ПРН 1</i> Презентувати та обговорювати результати наукових досліджень державною та іноземною мовами. <i>ПРН 3</i> Виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією.</p> | <input type="checkbox"/> | <p>Наукова комунікація іноземною мовою (за ОНП 2019, зі змінами 2020)</p> | <p>Словесні, наочні, практичні, проблемно-пошукові, самостійна робота, інтерактивні методи, заняття з елементами дистанційного навчання.</p> | <p>Усний контроль (індивідуальне опитування, фронтальне опитування, співбесіда); письмовий контроль (письмова перевірка, наукове есе); самоконтроль (уміння самостійно оцінювати свої знання, самоаналіз), екзамен.</p> |
| <p><i>ПРН 2</i> Здійснювати інформаційний пошук;</p> | <input type="checkbox"/> | <p>Стратегії наукових досліджень (Сучасні технології)</p> | <p>Аналіз, синтез, порівняння, індукція, дедукція, лекція, навчальні дискусії,</p> | <p>Самооцінювання, взаємооцінювання, усне опитування, перевірка та</p> |

аналізувати потреби, пов'язані з науковими дослідженнями, з розвитком загальних компетентностей фахівців і професіоналів із захисту інформації, інформаційної та/або кібербезпеки; реалізувати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, застосовуючи їх як в побуті, так і в професійній діяльності.

ПРН з Виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією.

ПРН 4

Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів; здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності; проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД;

інформаційної і кібербезпеки та захисту інформації)

мозковий штурм, моделювання, самоаналіз взаємоаналіз, термінологічний аналіз, рефлексивний аналіз, мікровикладання.

аналіз виконаних завдань, індивідуальні бесіди про результати виконання завдань, залік.

| | | | | |
|---|---------------------------------|--|--|--|
| <p>обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів, зокрема дотичних міждисциплінарних напрямів.</p> | | | | |
| <p><i>РН 4</i> Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів; здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності; проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД; обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й</p> | <p><input type="checkbox"/></p> | <p>Системний аналіз та прийняття рішень в інформаційній і кібербезпеці</p> | <p>Аналіз, синтез, порівняння, індукція, дедукція, лекція, навчальні дискусії, мозковий штурм, моделювання, самоаналіз взаємоаналіз, термінологічний аналіз, рефлексивний аналіз, мікровикладання.</p> | <p>Самооцінювання, взаємооцінювання, усне опитування, перевірка та аналіз виконаних завдань, індивідуальні бесіди про результати виконання завдань, залік.</p> |

| | | | | |
|--|--------------------------|---|--|---|
| <p>забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів, зокрема дотичних міждисциплінарних напрямів.</p> | | | | |
| <p><i>РН 1</i> Презентувати та обговорювати результати наукових досліджень державною та іноземною мовами. <i>РН 3</i> Виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією.</p> | <input type="checkbox"/> | <p>Наукова комунікація іноземною мовою (за ОНП 2022)</p> | <p>Словесні, наочні, практичні, проблемно-пошукові, самостійна робота, інтерактивні методи, заняття з елементами дистанційного навчання.</p> | <p>Усний контроль (індивідуальне опитування, фронтальне опитування, співбесіда); письмовий контроль (письмова перевірка, наукове есе); самоконтроль (уміння самостійно оцінювати свої знання, самоаналіз), екзамен.</p> |
| <p><i>РН 1</i> Презентувати та обговорювати результати наукових досліджень державною та іноземною мовами. <i>РН 2</i> Здійснювати інформаційний пошук; аналізувати потреби, пов'язані з науковими дослідженнями, з розвитком загальних компетентностей фахівців і професіоналів із захисту інформації, інформаційної та/або кібербезпеки. <i>РН 3</i> Виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією.</p> | <input type="checkbox"/> | <p>Стратегії наукових досліджень (Інтернаціоналізація науки: Змістовий модуль 2. Інформаційна грамотність; Змістовий модуль 3. Наукові публікації в цифровому середовищі)</p> | <p>Словесні, наочні, практичні, проблемно-пошукові, самостійна робота, інтерактивні методи, заняття з елементами дистанційного навчання.</p> | <p>Усний контроль (індивідуальне опитування, фронтальне опитування, співбесіда); письмовий контроль (письмова перевірка, наукове есе); самоконтроль (уміння самостійно оцінювати свої знання, самоаналіз), залік.</p> |

| | | | | |
|--|--------------------------|---|--|---|
| <p><i>РН 4</i> Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів; здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності; проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД; обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів, зокрема дотичних міждисциплінарних напрямів.</p> | | | | |
| <p><i>РН 1</i> Презентувати та обговорювати результати наукових досліджень державною та іноземною мовами. <i>РН 2</i> Здійснювати інформаційний пошук; аналізувати потреби, пов'язані з науковими дослідженнями, з розвитком</p> | <input type="checkbox"/> | <p>Стратегії наукових досліджень (Інтернаціоналізація науки: Змістовий модуль 1. Основи інтернаціоналізації вищої освіти і науки)</p> | <p>Словесні, наочні, практичні, проблемно-пошукові, самостійна робота, інтерактивні методи, заняття з елементами дистанційного навчання.</p> | <p>Усний контроль (індивідуальне опитування, фронтальне опитування, співбесіда); письмовий контроль (письмова перевірка, наукове есе); самоконтроль (уміння самостійно оцінювати свої знання, самоаналіз), залік.</p> |

загальних компетентностей фахівців і професіоналів із захисту інформації, інформаційної та/або кібербезпеки.
РН 3 Виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією.
РН 4 Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів; здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності; проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД; обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої

| | | | | |
|--|---------------------------------|---|--|---|
| <p>інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів, зокрема дотичних міждисциплінарних напрямів.</p> | | | | |
| <p><i>РН 1 Презентувати та обговорювати результати наукових досліджень державною та іноземною мовами.</i> <i>РН 2 Здійснювати інформаційний пошук; аналізувати потреби, пов'язані з науковими дослідженнями, з розвитком загальних компетентностей фахівців і професіоналів із захисту інформації, інформаційної та/або кібербезпеки.</i> <i>РН 3 Виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією.</i> <i>РН 4 Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів; здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності; проводити або керувати проведенням</i></p> | <p><input type="checkbox"/></p> | <p>Стратегії наукових досліджень (Нормативно-правова база наукових досліджень та наукової діяльності)</p> | <p>Словесні, наочні, практичні, проблемно-пошукові, самостійна робота, інтерактивні методи, заняття з елементами дистанційного навчання.</p> | <p>Усний контроль (індивідуальне опитування, фронтальне опитування, співбесіда); письмовий контроль (письмова перевірка, наукове есе); самоконтроль (уміння самостійно оцінювати свої знання, самоаналіз), залік.</p> |

| | | | | |
|--|--------------------------|--|--|---|
| <p>наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД; обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів, зокрема дотичних міждисциплінарних напрямів.</p> | | | | |
| <p><i>РН 1</i> Презентувати та обговорювати результати наукових досліджень державною та іноземною мовами. <i>РН 2</i> Здійснювати інформаційний пошук; аналізувати потреби, пов'язані з науковими дослідженнями, з розвитком загальних компетентностей фахівців і професіоналів із захисту інформації, інформаційної та/або кібербезпеки. <i>РН 3</i> Виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією.</p> | <input type="checkbox"/> | <p>Філософія і методологія наукової діяльності (Наукова етика)</p> | <p>Словесні, наочні, практичні, проблемно-пошукові, самостійна робота, інтерактивні методи, заняття з елементами дистанційного навчання.</p> | <p>Усний контроль (індивідуальне опитування, фронтальне опитування, співбесіда); письмовий контроль (письмова перевірка, наукове есе); самоконтроль (уміння самостійно оцінювати свої знання, самоаналіз), екзамен.</p> |

| | | | | |
|---|--------------------------|---|--|---|
| <p><i>РН 4</i> Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів; здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності; проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД; обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів, зокрема дотичних міждисциплінарних напрямів</p> | | | | |
| <p><i>РН 1</i> Презентувати та обговорювати результати наукових досліджень державною та іноземною мовами. <i>РН 2</i> Здійснювати інформаційний пошук; аналізувати потреби, пов'язані з науковими дослідженнями, з розвитком</p> | <input type="checkbox"/> | <p>Філософія і методологія наукової діяльності (Філософія науки; Загальнонаукова методологія)</p> | <p>Словесні, наочні, практичні, проблемно-пошукові, самостійна робота, інтерактивні методи, заняття з елементами дистанційного навчання.</p> | <p>Усний контроль (індивідуальне опитування, фронтальне опитування, співбесіда); письмовий контроль (письмова перевірка, наукове есе); самоконтроль (уміння самостійно оцінювати свої знання, самоаналіз), екзамен.</p> |

загальних компетентностей фахівців і професіоналів із захисту інформації, інформаційної та/або кібербезпеки.
РН 3 Виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією.
РН 4 Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів; здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності; проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД; обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої

| | | | | |
|--|---------------------------------|--|--|--|
| <p>інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів, зокрема дотичних міждисциплінарних напрямів.</p> | | | | |
| <p><i>ПРН 3</i> Виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та кібербезпеки, представляти їх в усній та/або письмових формах перед фаховою і нефаховою аудиторією.</p> <p><i>ПРН 4</i> Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності. Проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД. Обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах. Використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення</p> | <p><input type="checkbox"/></p> | <p>Інформаційно-аналітичні процеси в системах безпеки державних інформаційних ресурсів</p> | <p>Аналіз, синтез, порівняння, індукція, дедукція, лекція, навчальні дискусії, мозковий штурм, моделювання, самоаналіз взаємоаналіз, термінологічний аналіз, рефлексивний аналіз, мікровикладання.</p> | <p>Самооцінювання, взаємооцінювання, усне опитування, перевірка та аналіз виконаних завдань, індивідуальні бесіди про результати виконання завдань, залік.</p> |

| | | | | |
|--|--|--|--|--|
| <i>безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.</i> | | | | |
|--|--|--|--|--|