РЕЦЕНЗІЯ

на Освітньо-наукову Програму третього рівня вищої освіти за спеціальністю № 125 «Кібербезпека» Харківського національного університету імені В. Н. Каразіна галузі знань №12 «Інформаційні технології» від стейкхолдера АТ «Інститут інформаційних технологій». Кваліфікація: доктор філософії з кібербезпеки.

Освітньо-наукова Програма (ОНП) розроблена згідно та у повній відповідності з нормативно – правовою базою України, в ній враховані вимоги законів України «Про вищу освіту», «Про наукову та науково – технічну діяльність», а також «Порядку підготовки здобувачів вищої освіти ступеня доктора філософії» і Національної рамки кваліфікацій.

ОНП розроблена за безпосередньої участі відомих в Україні спеціалістів з безпеки інформації професорів Горбенка Івана Дмитровича та Кузнєцова Олександра Олександровича, а також доцентів докторів технічних наук Рассомахіна Сергія Геннадійовича і Єсіна Віталія Івановича.

АТ «Інститут інформаційних технологій», м. Харків є провідною структурою України в галузі інформаційної безпеки, він є розробником Системи електронного підпису України, Криптографічно-захищених мереж України, Систем і комплексів захисту банківської інформації, Комплексних систем захисту інформації, виконує НДР та ДКР за державними та комерційними замовленнями, а також проєктує та виготовляє лінійку апаратно-програмних та програмно-апаратних засобів криптографічного захисту інформації – серверів та апаратно-програмних і програмних засобів, що мають відповідні експертні висновки (Web – сайт : http://iit.com.ua/).

Від нашої заінтересованої сторони (стейкхолдера) АТ «Інститут інформаційних технологій» на етапі розробки ОНП надійшли та враховані такі пропозиції щодо:

1) математичних методів в кібербезпеці та математичних методів синтезу та аналізу перспективних доказово стійких постквантових асиметричних криптоперетворень;

2) обгрунутування та побудування моделей безпеки при забезпеченні кібербезпеки в умовах застосування методів класичного та квантового криптоаналізу, а також атак сторонніми каналами та на основі помилок;

3) комплексних методик оцінки кіберзахищенності на основі застосування безумовних, умовних та прагматичних критеріїв безпеки тощо (дивись роботодавці);

4) математичні основи квантових обчислень та програмування для квантових комп'ютерів при вирішення завдань оцінки безпеки та ефективного здійснення квантового криптоаналізу тощо.

Вказані пропозиції враховані на етапі розробки ОНП та реалізовані введенням двох навчальних дисциплін (Математичні методи в кібербезпеці ОК 5 та Математичні методи синтезу та аналізу криптографічних примітивів ВБ 1.2).

Основними цілями введення таких дисциплін є вивчення оригінальних математичних методів – алгебраїчних решіток, мультиваріативних перетворень, математичних кодів та ізогеній еліптичних кривих, а також їх застосування як при синтезі та аналіз асиметричних постквантових криптоперетворень асиметричного шифрування, протоколи інкапсуляції ключів та електронні підписи, так і в навчальних процесах для освоєння та застосуванні для кібербезпеки тощо.

Їх врахування зумовлено суттєвою необхідністю побудови перспективних постквантових доказово стійких стандартів симетричних та асиметричних криптографічних перетворень. Вказана проблема вирішується на основі проведення NIST США конкурсу з розробки, прийняття та впровадження постквантових стандартів криптографічних перетворень в 2023 – 2026 роках. Необхідність вирішення проблеми пов'язана з появою та застосуванням для криптоаналізу та здійснення атак квантових комп'ютерів. Вказана проблема успішно вирішується засобом проведення на державному рівні НДР та ДКР, як наслідок прийняття та необхідність їх впровадження впроваджувати, в тому числі в навчальний процес(ДСТУ 7524:2014, ДСТУ 7624:2014, ДСТУ 8845:2019, ДСТУ 8961:2019 тощо).

Виконавчий директор
АТ «Інститут інформаційних технологій» В. Д. Кравченко

Перший заступник Головного конструктора,
Лауреат державної премії в галузі науки і техніки,
Доктор філософії Ю. І. Гобенко