|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | Джерело фінансування (код КПКВК, загальний спеціальний фонди, напрям фінансування) | Назва роботи  (реквізити охоронного документу) | Відповідність роботи пріоритетному напряму розвитку науки і техніки | Період виконання роботи | Фактичний обсяг фінансування за повний період (тис. грн.) | Одержаний науковий результат, його новизна, науковий рівень, значимість та практичне застосування | Інформація щодо укладення договору про апробацію, дослідне використання, передачу (трансфер) ліцензійної угоди, надана МОН |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | Загальний фонд № ДР 0116U000810. Шифр  1-41-16.  Прикладна. | Аналіз стану, обґрунтування вимог та напрямів розвитку, стандартизація, розробка та впровадження криптографічних систем для надання електронних довірчих послуг.  Керівник: д.т.н., проф. Горбенко І.Д. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17) | 01.01.2016 – 31.12.2017 | 2000,0 | Підвищення національної безпеки держави в інформаційній сфері за рахунок удосконалення та розробки нормативної бази, методів, механізмів, протоколів, алгоритмів та засобів криптографічного захисту інформації (КЗІ) для надання електронних довірчих послуг (ЕДП) а також їх впровадження на національному та міжнародному рівнях при використанні у оборонній сфері, банківському секторі, державному управлінні, виробництві, в тому числі для подвійного використання.  Отримано:  - моделі та методи оцінки ризиків та концептуальні положення в частині надання ЕДП в умовах ведення інформаційних та гібридних війн;  - основні положення проектів нормативно - правових актів в сфері надання ЕДП, в тому числі транскордонних;  - криптографічні методи та механізми направленого шифрування по критеріям криптографічна стійкість – складність (швидкодія), ТЗ та специфікації на створення засобів КЗІ;  - теоретичні основи побудови систем захисту від несанкціонованих дій в комп’ютерних системах критичного призначення на основі методів багатофакторної автентифікації та їх впровадження.  Одержані результати дозволяють забезпечити гарантовані показники стійкості криптоперетворень при цифровому підпису та шифруванні даних в державних та військових інформаційних системах. | Акт впровадження в ПАТ «Інститут інформаційних технологій»  Результати використано для розробки національних стандартів шифрування та функції гешування.  За результатами заключено договори на виконання НДР:  № 43-15; 44-15;53-16 із загальною сумою позабюджетного фінансування  1000,0 тис. грн. |
| 2 | Загальний фонд № ДР 0117U004832. Шифр  2-41-17.  Прикладна. | Розробка математичних моделей і методів синтезу, формування та обробки сигнально-кодових конструкцій для захищених телекомунікаційних систем подвійного призначення.  Керівник: д.т.н., доцент Рассомахін С.Г. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17) | 01.01.2017 – 31.12.2019 | 1500,0 | Підвищення національної безпеки держави в інформаційній сфері за рахунок удосконалення та розробки нових видів прихованих, завадостійких протоколів передачі даних та методів псевдовипадкового кодування в радіоканалах.  Отримано:   * математична модель псевдовипадкових кодів (ПВК) протоколу канального рівня, фізична модель ПВК протоколу фізичного рівня, моделі та методи побудови ПВК і лінеаризації цільової функції декодування; * оцінка підвищення показників завадостійкості та скритності каналів передачі даних у військових системах; * методи синтезу нелінійних криптографічних дискретних складних сигналів, який дозволяє створювати сигнали з необхідними ансамблевими, структурними та кореляційними властивостями, що дає можливість покращити показники завадозахищеності та інформаційної безпеки.   Одержані результати дозволяють суттєво покращити показники надійності, захищеності та скритності процесів передачі інформації та бойового управління. | Акт впровадження в ЦКБ «Протон», ДП КБ «Південне».  Результати використано при реалізації програми «Гром-2».  За результатами заключено договори на виконання НДР:  № 48-13; 53-13;11-17 із загальною сумою позабюджетного фінансування  3125,0 тис. грн. |
| 3 | Загальний фонд № ДР 0118U002024. Шифр  1-41-18.  Прикладна. | Аналіз, дослідження, розробка та стандартизація криптографічних систем для захисту інформації в пост-квантовому середовищі, в умовах інформаційних і гібридних війн.  Керівник: д.т.н., проф. Кузнецов О.О. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17) | 01.01.2018 – 31.12.2020 | 6000,0 | Підвищення національної безпеки держави в інформаційній сфері, забезпечення конфіденційності, цілісності та доступності державних інформаційних ресурсів, інформації з обмеженим доступом, зокрема тієї, що циркулює на об’єктах критичної інформаційної інфраструктури, забезпечення кібербезпеки в пост-квантовому середовищі та в умовах ведення інформаційних і гібридних війн.  Отримано:   * аналіз сучасних проблем КЗІ у пост-квантовий період та дослідження можливих шляхів їх вирішення із застосуванням різних сімейств квантово-стійких криптоперетворень; * розробка, удосконалення та гармонізація квантово-стійких криптосистем, механізмів та протоколів КЗІ, розробка положень теорії аналізу та оцінки кібербезпеки;   Практичне впровадження квантово-стійких криптопримітивів в системи, комплекси та засоби КЗІ, в тому числі військового призначення, дозволяє зберегти та підвищити стійкість крипто та імітозахисту навіть після появи квантових обчислювачів. | Реалізація в ПАТ «Інститут інформаційних технологій».  Результати використано в програмах модернізації механізмів та засобів криптографічного захисту інформації.  Заключено договори на виконання НДР:  № 38-17; 44-15;53-18. Загальна сума позабюджетного фінансування  1100,0 тис. грн. |
| 4 | Загальний фонд № ДР 0119U002546. Шифр  3-41-19.  Прикладна. | Тема 3-41-19 № ДР 0119U002546. Формулювання та розробка принципів, методів і засобів швидкої та достовірної обробки цілочисельних даних, що представлені у непозиційній системи числення залишкових класів в комп’ютерних системах та мережах подвійного призначення.  Керівник: д.т.н., проф. Краснобаєв В.А. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17) | 01.01.2019 – 31.12.2021 | 1890,0 | Підвищення швидкодії (продуктивності) та достовірності обробки цілочисельних даних комп'ютерних систем та компонент (КСК) подвійного призначення на основі застосування систем числення у залишкових класах (СЗК). Розвиток теоретичних і практичних положень застосування нових інформаційних технологій контролю, діагностики та корекції помилок у СЗК, з точки зору підвищення швидкодії проведення процедур операцій.  Використання результатів надає можливість забезпечити потрібний рівень швидкості та надійності функціонування комп’ютерних елементів управляння і контроля сучасних зразків зброї. | Акт впровадження ЦКБ «Протон», ПАТ «Інститут інформаційних технологій».  Результати роботи планується використати в ХНУ імені В.Н. Каразіна при створенні дослідного зразку спец. обчислювача у системі залишкових класів. |
| 5 | Державне підприємство «Конструкторське бюро «Південне» імені М.К. Янгеля.  Шифр 48-13. | Аналіз загроз та розробка моделей порушників для системи управління спеціального призначення.  Керівник: д.т.н., доцент Рассомахін С.Г. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17) | 25.11.2013 - 25.03.2014 | 235,0 | Обґрунтування переліку загроз та розробка алгоритмів та технічних засобів щодо захисту від несанкціонованих дій та доступу до даних.  Використання результатів дозволяє обґрунтувати вимоги та розробити специфікацію на програмно-технічну реалізацію автоматизованої системи контролю та санкціонування доступу суб’єктів до елементів системи управління військами та зброєю. | Акт впровадження у ДП КБ «Південне». Програма «Гром-2». |
| 6 | Державне підприємство «Конструкторське бюро «Південне»  імені М.К. Янгеля.  Шифр 53-13. | Розробка програмно-апаратної підсистеми захисту від несанкціонованих дій та доступу до даних «Trusted Launch».  Керівник: д.т.н., доцент Рассомахін С.Г. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17) | 01.12.2013 - 15.03.2016 | 2430,0 | Розроблені вимоги, функціональні та принципові схеми підсистеми спеціального контролю та санкціонування. Виготовлено конструкторську документацію підсистеми запобігання несанкціонованому доступу та діям.  Використання результатів дозволило досягнути потрібний рівень безпечного управління та санкціонування застосування ракетної зброї. | Акт впровадження у ДП КБ «Південне». Програма «Гром-2». |
| 7 | ПАТ «Інститут інформаційних технологій».  Шифр 49-13. | Дослідження режимів застосування блокових симетричних шифрів.  Керівник: д.т.н., проф. Горбенко І.Д. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17) | 01.11.2013 - 01.09.2014 | 120,0 | Отримано та статистичне досліджено нові режими застосування блокового симетричного шифру «Калина».  Результати досліджень дозволили створити та ввести в дію перший національний стандарт криптографічного шифрування «Калина». | Акт впровадження в ПАТ «Інститут інформаційних технологій».  Впроваджено в перший національний стандарт блокового шифрування. |
| 8 | ПАТ «Інститут інформаційних технологій».  Шифр 51-14. | Дослідження потокових симетричних шифрів та потокових режимів блокових симетричних шифрів.  Керівник: д.т.н., проф. Горбенко І.Д. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17) | 01.10.2014 - 31.12.2015 | 180,0 | Отримано та статистичне досліджено режими застосування нового потокового шифру.  Отримані нові статистичні дані результатів використання блокового шифру у режимі потокового шифрування.  Використання результатів дозволило створити основні компоненти національного стандарту потокового шифрування «Струмок» та підготувати стандарт до затвердження. | Акт впровадження в ПАТ «Інститут інформаційних технологій».  Впроваджено в перший національний стандарт потокового шифрування. |
| 9 | ПАТ «Інститут інформаційних технологій».  Шифр 02-14. | Розробка методів та механізмів направленого шифрування.  Керівник: д.т.н., проф. Горбенко І.Д. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17) | 01.02.2014 - 31.12.2014 | 100,0 | Отримано та статистично досліджено алгоритми NTRU спрямованого шифрування для перспективного застосування в національних асиметричних криптосистемах.  Використання результатів дозволяє забезпечити потрібні рівні конфіденційності, цілісності та неспростовності національних електронних довірчих послуг при використанні ефективних NTRU криптоперетворень та підвищує рівень інформаційної безпеки держави.. | Акт впровадження в ПАТ «Інститут інформаційних технологій».  Впроваджені нові застосування експериментально-обчислювальних алгоритмів перевірки стійкості направленого шифрування. |
| 10 | ПАТ «Інститут інформаційних технологій».  Шифр 01-15 | Порівняльний аналіз стандартизованих методів та протоколів криптографічного захисту інформації та генерування ключових даних методами квантової фізики.  Керівник: д.т.н., проф. Горбенко І.Д. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17 | 01.02.2015 - 31.12.2015 | 360,0 | Розроблено математичне забезпечення та апаратний макет квантового генератора випадкових чисел для генерування ключових даних криптографічних систем.  Результати досліджень дозволяють впровадити ефективні датчики числових даних, які побудовані на нових фізичних принципах, для генерації ключів національних, у тому числі військових, криптосистем. Це суттєво поліпшує показники стійкості криптоперетворень та усуває можливість виникнення колізій. | Акт впровадження в ПАТ «Інститут інформаційних технологій».  Використано при розробці пропозицій щодо створення системи забезпечення експлуатації систем захисту інформації в державних та військових структурах. |
| 11 | ПАТ «Інститут інформаційних технологій».  Шифр 43-15 | Методи та засоби криптографічного захисту інформації у пост квантовий період.  Керівник: д.т.н., проф. Горбенко І.Д. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17 | 01.01.2016 - 31.12.2016 | 360,0 | Розроблено криптографічні алгоритми і протоколи для можливого застосування в постквантовий період.  Використання результатів забезпечує стійкість систем захисту інформації в державних та військових установах в умовах здійснення атак потенційних зловмисників та криптоаналізу з використанням квантових комп’ютерів. | Акт впровадження в ПАТ «Інститут інформаційних технологій».  Використано у перспективних алгоритмах криптоперетворень. |
| 12 | ПАТ «Інститут інформаційних технологій» (м. Харків).  Шифр 44-15 | Аналіз, розробка та дослідження пост квантових криптографічних примітивів та обґрунтування умов їхнього застосування в Україні.  Керівник: д.т.н., проф. Горбенко І.Д. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17 | 01.01.2016 - 31.12.2016 | 140,0 | Розроблено криптографічні примітиви для можливого застосування в постквантовий період.  Використання результатів забезпечує стійкість систем захисту інформації в державних та військових установах в умовах здійснення криптоаналізу з використанням квантових комп’ютерів. | Акт впровадження в ПАТ «Інститут інформаційних технологій».  Використано у перспективних алгоритмах криптоперетворень. |
| 13 | ПАТ «Інститут інформаційних технологій».  Шифр 53-16 | Моделі, механізми, методи та засоби криптографічного захисту інформації та стандартизації у перехідний та пост квантовий період.  Керівник: д.т.н., проф. Горбенко І.Д. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17 | 01.01.2017 - 31.12.2017 | 500,0 | Моделі, механізми, методи та засоби криптографічного захисту для забезпечення стійкості захисту інформації до атак за допомогою квантових комп’ютерів.  Використання результатів дозволило підготувати пропозиції побудови криптоалгоритмів пост квантового періоду та висунути їх до участі у міжнародному конкурсі NIST. | Акт впровадження в ПАТ «Інститут інформаційних технологій».  Використано у перспективних алгоритмах криптоперетворень. |
| 14 | Державне підприємство «Конструкторське бюро «Південне» імені М.К. Янгеля.  Шифр 11-17. | Розробка дослідного зразка спеціальної системи захисту від несанкціонованого доступу та дій.  Керівник: д.т.н., доцент Рассомахін С.Г. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17 | 01.01.2017 - 16.02.2018 | 460,0 | Розроблено програмно-апаратний макет спеціального пристрою захисту від несанкціонованого доступу до інформації бойового управління та несанкціонованих дій.  Використання результатів дозволило створити дослідний зразок програмно-апаратної підсистеми захисту та забезпечити ходові випробування комплексу «Гром-2». | Акт впровадження у ДП КБ «Південне», програма «Гром-2».  Використано у процесі ходових випробувань дослідного зразка ракетного комплексу «Гром-2» |
| 15 | ПАТ «Інститут інформаційних технологій».  Шифр 38-17. | Механізми, методи та засоби криптографічного захисту інформації та стандартизації у перехідний та пост квантовий період.  Керівник: д.т.н., проф. Горбенко І.Д. | Інформаційні та комунікаційні технології (згідно з Законом України від 12.10.2010 № 2519-17 | 01.01.2018 - 31.12.2018 | 500,0 | Моделі, механізми, методи та засоби криптографічного захисту для забезпечення стійкості захисту інформації до атак за допомогою квантових комп’ютерів.  Використання результатів суттєво розширить номенклатуру засобів, що є гарантовано стійкими в умовах інформаційної протидії в постквантовий період. | Робота у даний час виконується.  Передбачено реалізацію в ПАТ «Інститут інформаційних технологій». |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 16 | “Samsung Electronics Ukraine Company»  Прикладна НДР | Scalable System of Images Processing  Кузнецов О.О. | Технології та засоби захисту інформації | 2017 | 480,0 | Scalable System of Images Processing.  Створені математичні методи перетворення фото обличчя людини у парольну послідовність | Реалізація в “Samsung Electronics Ukraine Company» для мобільних гаджетів. |
| 17 | “Samsung Electronics Ukraine Company»  Прикладна НДР | Fuzzy Verification System.  Рассомахін С. Г. | Технології та засоби захисту інформаці | 2018 | 400,0 | Development & implementation of fuzzy extraction biometrical system for digital signature mechanism.  Розроблені математичні і програмні засоби автоматичного формування та верифікації цифрового підпису за обличчям людини. | Реалізація в “Samsung Electronics Ukraine Company» для мобільних гаджетів |
| 18 | “Samsung Electronics Ukraine Company»  Прикладна НДР | Authentication System for Multi-Device Experience,  Рассомахін С. Г. | Технології та засоби захисту інформаці | 2018 | 700,0 | Development & implementation mathematical methods for fingerprint authentication systems.  Розроблена система автоматичної верифікації персоналій за відбитками пальців з двократно покращеними показниками достовірності у порівнянні з існуючими системами | Реалізація в “Samsung Electronics Ukraine Company» для мобільних гаджетів |