- Розробка та впровадження архітектури Zero Trust для корпоративних інформаційних систем
- Моделювання політик безпеки підприємства на основі ризик-орієнтованого підходу
- Розробка моделі адаптивної системи кіберзахисту організації
- Побудова системи управління інформаційною безпекою (ISMS) відповідно до ISO/IEC 27001
- Розробка архітектури безпеки для хмарних середовищ
- Дослідження ефективності постквантових криптографічних алгоритмів
- Розробка системи захисту даних із використанням гомоморфного шифрування
- Аналіз вразливостей сучасних криптографічних протоколів
- Розробка системи управління криптографічними ключами (KMS)
- Використання блокчейн-технологій для забезпечення цілісності даних
- Розробка системи виявлення вторгнень (IDS/IPS) на основі машинного навчання
- Аналіз і захист від DDoS-атак у корпоративних мережах
- Побудова системи безпечної маршрутизації в SDN-мережах
- Виявлення аномалій мережевого трафіку за допомогою AI
- Розробка системи моніторингу мережевої безпеки в реальному часі
- Розробка системи автоматизованого тестування безпеки веб-додатків
- Аналіз вразливостей OWASP Top 10 у сучасних веб-системах
- Розробка методів захисту мікросервісної архітектури
- Побудова системи DevSecOps для безпечної розробки ПЗ
- Дослідження атак типу injection та методів їх запобігання
- Використання глибокого навчання для виявлення кіберзагроз
- Розробка системи виявлення фішингових атак із використанням ML
- Аналіз поведінки користувачів (UEBA) на основі AI
- Розробка системи прогнозування кіберінцидентів
- Виявлення шкідливого програмного забезпечення за допомогою нейронних мереж
- Розробка системи кіберзахисту SCADA/ICS
- Моделювання кіберзагроз для об’єктів критичної інфраструктури
- Оцінювання стійкості кіберфізичних систем до атак
- Захист енергетичних систем від кіберінцидентів
- Розробка системи моніторингу безпеки транспортної інфраструктури
- Розробка методики оцінювання кіберризиків організації
- Побудова системи управління інцидентами інформаційної безпеки
- Аудит інформаційної безпеки підприємства відповідно до міжнародних стандартів
- Розробка системи забезпечення безперервності бізнесу (BCP/DRP)
- Аналіз ефективності заходів захисту інформації
- Розробка системи захисту IoT-пристроїв від ботнет-атак
- Аналіз вразливостей вбудованих систем і методи їх усунення
- Побудова безпечної архітектури IoT-мереж
- Розробка системи автентифікації для IoT-пристроїв
- Захист бездротових сенсорних мереж від кіберзагроз