Приблизний перелік індивідуальних завдань для проходження виробничої практики студентів 3- курсу

1. Розробка лабораторних робіт з комп'ютерного практикуму для курсу «Асиметричні криптосистеми».
2. Побудова та автоматичний розв'язок систем диференціальних переходів GUFNв залежності від кількості блоків та раундів
3. Статистичний аналіз топонімічних назв України. Розробка статистичних алгоритмів критеріїв перевірки деяких лінгвістичних та історичних гіпотез розподілу географічних назв.
4. Дослідження схем ключового розкладу сучасних блочних шифрів.
5. Дослідження алгоритмів розв'язання систем рівнянь зі спотворенням над скінченними полями та їх застосування в криптоаналізі.
6. Розрахунок додаткових варіантів для лабораторних робіт з курсу «Математичні методи захисту інформації».
7. Пошук та дослідження нових принципів та підходів для побудови статистичних тестів перевірки випадкових та псевдовипадкових послідовностей.
8. Розробка переборних алгоритмів криптоаналізу класичних шифрів із застосуванням бібліотеки паралельного програмування MPI для кластерної обчислювальної системи.
9. Використання атак компромісу на поточні шифри на прикладах LILI-129 Achterdahn
10. Розробка програмного засобу реалізації модульного контролю за дисципліною «Методи реалізації криптографічних механізмів захисту інформації».
11. Дослідження алгебраїчних атак на потокові криптосистеми.
12. Унікальні ідетифікатори та їх реалізація.
13. Застосування інфраструктури відкритих ключів.
14. Дослідженнянезбалансованихфейстелевських схем блоковихшифраторів.
15. Аналіз статистичних властивостей учасника конкурсу e – Stream алгоритму Creupt МТЗ StreamCipher.
17. Аналіз стійкості сучасних блокових шифрів до лінійно – різницевого криптоаналізу.
18. Дослідження стійкості алгоритмів гамування до методу ймовірного слова.
19. Аналіз методів факторизації багатослівних чисел та розробка бібліотеки програм факторизації для розподільних обчислювальних систем.
20. Аналіз методів дискретного логорифмування та розробка бібліотеки програм обчислення дискретного логарифмування для розподільних обчислювальних систем.
21. Дослідження алгоритмів побудови оцінок диференціальної та лінійної ймовірності SP мереж.
22. Розробка механізмів шифрування та геджування для оперативних систем мобільних теміналів на прикладі OCWindousMobile та Simbian.
23. Атаки компромісу на потоковий генератор A 5\1.
24. Огляд сучасних квантових протоколів розподілу ключа та типових атак на них.

Матеріали, що отримав студент під час виконання індивідуального завдання, можуть в подальшому бути використані для виконання кваліфікаційної роботи, для підготовки доповіді, статті або для інших цілей за погодженням з кафедрою і базою практики.