

Список тем  
выпускных квалификационных работ студентов  
образовательной программы 10.05.01. Компьютерная безопасность  
в 2019-2020 учебном году

| №п/п | Тема выпускной квалификационной работы  |
|------|---|
| 1    | Создание доверенной системы исследования остаточных данных на запоминающих устройствах на базе hexedit  |
| 2    | Исследование уязвимостей и мер обеспечения защиты систем, построенных с использованием протокола LDAP   |
| 3    | Обеспечение безопасности базы данных системы "Монитор КПЭ" для определения и хранения ключевых показателей эффективности НИУ ВШЭ  |
| 4    | Исследование перемешивающих свойств подстановок двоичных регистров сдвига с тремя обратными связями   |
| 5    | Исследование влияния фрагментации файлов на возможность их восстановления   |
| 6    | Разработка методов построения MDS матриц специального вида над полем GF(256)  |
| 7    | Исследование возможности встраивания отечественного криптографического протокола в стек TCP/IP ядра Linux   |
| 8    | Исследование методов реализации VPN-туннелей  |
| 9    | Разработка методов построения циклических MDS матриц размера $n \times n$ , $8 < n \leq 16$ с большим числом единиц и малым числом различных элементов над конечным полем GF(q) |
| 10   | Разработка модели обнаружения факта мошенничества с банковскими картами   |
| 11   | Экспериментальные модули построения понимающих пар для булевых функций без запрета  |
| 12   | Исследование возможности создания доверенной системы анализа реестра ОС семейства Windows на базе RegRipper   |
| 13   | Создание доверенной системы сборки TCP соединений из записанного сетевого трафика в условиях больших потерь информации  |
| 14   | Реализация и анализ маскированных алгоритмов блочного шифрования "Магма" и "Кузнечик"   |
| 15   | Исследование эффективности методов вычисления кратных точек на эллиптических кривых   |
| 16   | Анализ и реализация атак по скрытым логическим каналам  |
| 17   | Построение методов определения авторства на основе текстовой информации   |
| 18   | Создание доверенной системы извлечения информации из файлов формата .lnk и списков быстрого доступа   |
| 19   | Исследование механизмов распараллеливания хэширования на основе древовидной модели  |
| 20   | Анализ безопасности протокола WPA3  |
| 21   | Экспериментальные исследования периодов двоичных многочленов специального вида  |
| 22   | Исследование TLS сокетов ядра Linux   |