МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ

| *Факультет* | *Кафедра* |
|---|---|
| Вычислительной техники | Вычислительная техника |

Направление подготовки 09.03.01 «Информатика и вычислительная техника»

Профиль Вычислительные машины, комплексы, системы и сети

# ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА БАКАЛАВРА

на тему

## Блок сжатия криптографической хеш-функции на базе полносвязной нейронной сети

**Студент** _____ (подпись, дата) Петкилев Александр Алексеевич

**Руководитель** _____ (подпись, дата) Дубравин А.В.

**Нормоконтролёр** _____ (подпись, дата) Кучин А.В. 18.06.19

*Работа допущена к защите* (протокол зас. кафедры от 31.05.2019 г. № 38-09-14)

**Заведующий кафедрой** _____ (подпись) Митрохин М.А.

*Работа защищена с отметкой* отлично (протокол заседания ГЭК от 19.06.19 № 2)

**Секретарь ГЭК** _____ (подпись) Гурин Е.И.

Пенза, 2019

Федеральное государственное бюджетное образовательное учреждение
высшего образования
ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ

| *Факультет* | *Кафедра* |
|---|---|
| Вычислительной техники | Вычислительная техника |

«Утверждаю»
Заведующий кафедрой
_____ М.А. Митрохин
«23» апреля 2019 г.

**ЗАДАНИЕ**
**НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ**
**БАКАЛАВРА**

1. Студент Петкилев Александр Алексеевич гр. 15ВВ1 факультета вычислительной техники.

2.Тема работы: «Разработка криптографического блока сжатия хеш-функции».

Тема утверждена приказом ПГУ № 554/о от "29" апреля 2019 г.

3. Руководитель работы к.т.н., доцент каф. ВТ ПГУ Дубравин А.В..

4. Задание на работу (назначение разработки, исходные данные и т.п.).

Разработать блок сжатия криптографической хеш-функции и отображение в виде графиков результатов статистических проверок. Разработать и отладить взаимодействие модулей приложения. Система должна быть представлена в виде динамической библиотеки классов, с целью обеспечения возможности его применения в качестве компонента для решения конкретных практических задач.

5. Перечень подлежащих разработке вопросов.

Требуется произвести анализ предметных областей: изучить типы искусственных нейронных сетей, виды и свойства хеш-функций, рассмотреть функции хаотического отображения. Необходимо изучить методологии проектирования нейронных сетей и хеш-функций, а также изучить виды атак на хеш-функции.

# Результаты Всероссийского конкурса выпускных квалификационных работ, 2019 год

## Секция 2: Информатика и вычислительная техника

## Уровень подготовки: магистерская диссертация

### Направление: 09.04.01 Информатика и ВТ

| № | ВУЗ | Каф. | ФИО | Тема ВКР | Место |
|---|---|---|---|---|---|
| 1 | НГТУ | ВТ | Морозов Антон Евгеньевич | Разработка и исследование нейронной сети для восстановления структуры среды,содержащей каверновые зоны | 1 |
| 2 | ТПУ | ИШИТР, отд ИТ | Ягунов Тимофей Антонович | Программное обеспечение для конфигурирования и управления системой компьютерного зрения с аппаратно-реализованной на ПЛИС сверточной нейронной сетью | 2 |
| 3 | НГТУ | ВТ | Богомолов Дмитрий Александрович | Разработка и исследование информационной системы мониторинга состояния дорожного покрытия | 3 |

### Направление: 09.04.02 Информационные системы и технологии

| № | ВУЗ | Каф. | ФИО | Тема | Место |
|---|---|---|---|---|---|
| 1 | ТПУ | ИШИТР, отд.ИТ | Борухина Кристина Олеговна | Разработка информатизационной системы для автоматизации процесса найма персонала | 1 |
| 2 | ТПУ | ИШИТР, отд.ИТ | Ткачёв Семён Александрович | Разработка информатизационной системы дляоперативной связи с экстренными службами | 2 |
| 3 | ТПУ | ИШИТР, отд.ИТ | Клековкин Вадим Александрович | Статистический анализ результатов тестирования по информатике в НИ ТПУ выпускников 2018 года | 3 |

### Направление: 09.04.03 Прикладная информатика

| № | ВУЗ | Каф. | ФИО | Тема | Место |
|---|---|---|---|---|---|
| 1 | КузГТУ | ПИТ | Диденко Андрей Александрович | Технология параллельных вычислений и программное обеспечение для анализа и оценки пользовательских предпочтений на основе аудит-логов использования системы Trackor One Vizion | 1 |
| 2 | КузГТУ | ПИТ | Иванов Артем Алексеевич | Исследование методов и алгоритмов оценки финансовых рисков и разработка проекта информационной системы поддержки | 2 |

### Направление: 09.04.04 Программная инженерия

| № | ВУЗ | Каф. | ФИО | Тема | Место |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| 1 | ТПУ | ИШИТР, отд. ИТ | Радишевский Владислав Леонидович | Комбинированный подход к извлечению структурированных данных для языков со свободным порядком слов | **1** |
| 2 | НГТУ | ВТ | Демянчук Алексей Иванович | Разработка системы распознавания семантики и прагматики предложений на естественном языке на основе нейронных | **2** |
| 3 | ТПУ | ИШИТР, отд. ИТ | Кайда Анастасия Юрьевна | Разработка протокола передачи данных для систем управления потоками данных | **3** |

**Направление: 10.04.01 Информационная безопасность**

| № | ВУЗ | Каф. | ФИО | Тема | Место |
|---|---|---|---|---|---|
| 1 | УГАТУ | ВТиЗИ | Слинин Андрей Владимирович | Интеллектуальная система оценки рисков информационной безопасности объектов критической информационной инфраструктуры | **1** |
| 2 | УГАТУ | ВТиЗИ | Тимерханова Сабина ровна | Модели и метод оценки уровня защищенности виртуальной инфраструктуры | **2** |
| 3 | УГАТУ | ВТиЗИ | Мухарлямов Айнур Айдарович | Система управления информационной безопасностью автматизированной системой управпения технологическим процессом | **3** |

**Направление: 27.04.04 Управление в технических системах**

| № | ВУЗ | Каф. | ФИО | Тема | Место |
|---|---|---|---|---|---|
| 1 | СамГТУ | АУТС | Капустина Алена Валерьевна | Оптимальное по быстродействию управление процессом индукционного нагрева в технологическом комплексе "нагрев-обработка давлением" | **1** |
| 2 | СамГТУ | АУТС | Ильина Наталья Андреевна | Оптимальное по быстродействию двухканальное граничное управление процессами нестационарной теплопроводимости | **2** |
| 3 | СамГТУ | АУТС | Коваленко Мария Сергеевна | Исследование протранственно-временного управляющего воздействия в процессе индукционного нагрева | **3** |

## Уровень подготовки: дипломная работа по специальности

**Направление: 10.05.02 Информационная безопасность телекоммуникационных**

| № | ВУЗ | Каф. | ФИО | Тема | Место |
|---|---|---|---|---|---|
| 1 | ПГУ | ИБСиТ | Круглов Алексей Сергеевич | Способы разграничения прав доступа при обеспечении информационной безопасности веб-приложений с динамически формируемым содержимым | **1** |

### Направление: 10.05.03 Информационная безопасность автоматизированных систем

| № | ВУЗ | Каф. | ФИО | Тема | Место |
|---|---|---|---|---|---|
| 1 | УГАТУ | ВТ и ЗИ | Бельский Станислав Михайлович | Система анализа риска информационной безопасности на основе нечетких когнитивных карт | **1** |
| 2 | УГАТУ | ВТ и ЗИ | Фатхутдинова Камила Дамировна | Интеллектуальная система распознавания эмоций в нейросетевом базисе | **2** |
| 3 | УГАТУ | ВТ и ЗИ | Старцева Арина Сергеевна | Модуль интеллектуального анализа в системе мониторинга банковских транзакций | **3** |

## Уровень подготовки: выпускная квалификационная работа бакалавра

### Направление: 09.03.01 Информатика и ВТ

| № | ВУЗ | Каф. | ФИО | Тема | Место |
|---|---|---|---|---|---|
| 1 | ТПУ | ИШИТР отд. ИТ | Пантюхин Евгений Игоревич | Исследование возможностей нейронных сетей для управления беспилотными аппаратами | **1** |
| 2 | ПГУ | ВТ | Петкилев Александр Алексеевич | Блок сжатия криптографической хэш-функции на базе полносвязной нейронной сети | **2** |
| 3 | НГТУ | ВТ | Пешков Александр Викторович | Разработка программного обеспечения PTT-гарнитуры для применения в шахте | **3** |

### Направление: 09.03.02 Информационные системы и технологии

| № | ВУЗ | Каф. | ФИО | Тема | Место |
|---|---|---|---|---|---|
| 1 | ТПУ | ИШИТР отд. ИТ | Маслов Константин Андреевич | Разработка системы автоматизированного мониторинга изменений земной поверхности с использованием данных дистанционного зондирования земли | **1** |
| 2 | ТПУ | ИШИТР отд. ИТ | Зобнина Анастасия Александровна | Разработка комплекса мобильных приложений для структурных подразделений АО "Воркутауголь" | **2** |
| 3 | ТПУ | ИШИТР отд. ИТ | Чурсина Елена Андреевна | Разработка модуля поддержки принятия решенийв процессе диагностики функционального состояния системы гемостаза | **3** |

### Направление: 09.03.03 Прикладная информатика

| № | ВУЗ | Каф. | ФИО | Тема | Место |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| 1 | КузГТУ | ПИТ | Фидченко Михаил Викторович, Хаданова Каролина Викторовна | Программное обеспечение организации сложных экспертиз на основе решающих матриц и методики ПАТТЕРН | **1** |
| 2 | ЮТИ ТПУ | Отд. цифр. технологий | Соколовский Дмитрий Евгеньевич | Информационная система учета и анализа деятельности кабинета ультразвуковой диагностики "БИОМЕД" | **2** |
| 3 | ЮТИ ТПУ | Отд. цифр. технологий | Антонов Константин Федорович | Информационная система оценки профессиональных рисков на рабочих местах методом анкетирования | **3** |

**Направление: 09.03.04 Программная инженерия**

| № | ВУЗ | Каф. | ФИО | Тема | Место |
|---|---|---|---|---|---|
| 1 | ТПУ | ИШИТР, отд. ИТ | Федоров Константин Борисович | Процедурная генерация ландшафтов | **1** |
| 2 | ТПУ | ИШИТР, отд. ИТ | Клюшов Павел Дмитриевич | Программное обеспечение для определения, построения и визуализации двухмерной и трехмерной графики | **2** |
| 3 | НГТУ | ВТ | Дудаков Глеб Денисович | Разработка вев-сервиса орфографического анализа русскоязычного текста | **3** |

**Направление: 10.03.01 Информационная безопасность**

| № | ВУЗ | Каф. | ФИО | Тема | М |
|---|---|---|---|---|---|
| 1 | УГАТУ | ВТиЗИ | Гайнуллин Камиль Альбертович | Алгоритмы интеллектуального анализа данных | **1** |
| 2 | УГАТУ | ВТиЗИ | Герасимов Владислав Владимирович | Усиление аунтефикации пользователей web-ресурсов путем привязки к устройствам компьютера | **2** |

**Направление: 27.03.04 Управление в технических системах**

| № | ВУЗ | Каф. | ФИО | Тема | Место |
|---|---|---|---|---|---|
| 1 | СамГТУ | АУТС | Шишов Николай Сергеевич | Систума управления движением мобильного колесного робота | **1** |
| 2 | ПГУ | АиТ | Растов Максим Алексеевич | Цифровая модель ШИМ для трехфазного двигателя | **2** |
| 3 | СамГТУ | АУТС | Воронцов Дмитрий Сергеевич | Эффективность искусственных нейронных сетей различных типов в задаче классификации | **3** |