

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное автономное образовательное учреждение  
высшего образования

«Южно-Уральский государственный университет  
(национальный исследовательский университет)»

**Высшая школа электроники и компьютерных наук  
Кафедра «Защита информации»**

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой,

к.т.н., доцент

\_\_\_\_\_ А.Н. Соколов

\_\_\_\_\_ 2019 г.

**Проектирование подсистемы криптографической защиты  
информации государственной информационной системы  
управления общественными финансами**

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА  
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ  
ЮУрГУ – 10.03.01.2019.197.ПЗ ВКР

Руководитель проекта,  
начальник отдела  
Министерства финансов  
Челябинской области

\_\_\_\_\_ А.А. Повышев

\_\_\_\_\_ 2019 г.

Автор проекта,  
студент группы КЭ-454

\_\_\_\_\_ В.Д. Сапегина

\_\_\_\_\_ 2019 г.

Нормоконтролер,  
к.т.н., доцент

\_\_\_\_\_ В.П. Мартынов

\_\_\_\_\_ 2019 г.

Челябинск 2019

## АННОТАЦИЯ

Сапегина В.Д. Проектирование подсистемы криптографической защиты информации государственной информационной системы управления общественными финансам – Челябинск: ЮУрГУ, КЭ-454, 182 с., 18 ил., 27 табл., библиогр. список – 21 наим., 13 прил.

Выпускная квалификационная работа выполнена с целью проектирования подсистемы криптографической защиты информации государственной информационной системы управления общественными финансами.

В выпускной квалификационной работе отражены этапы создания государственной информационной системы и подсистемы криптографической защиты до этапа ввода в эксплуатацию.

В процессе выполнения выпускной квалификационной работы было проведено предпроектное обследование Министерства финансов Челябинской области, изучены нормативные правовые акты, регулирующие создание государственных информационных систем и применение криптографических средств защиты информации. Был разработан проект подсистемы криптографической защиты информации государственной информационной системы управления общественными финансами, подготовлены организационно-распорядительные документы, необходимые для функционирования подсистемы, в соответствии с требованиями законодательства Российской Федерации.

					ЮУрГУ – 10.03.01.2019.197.ПЗ ВКР			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.		Сапегина			<i>Проектирование подсистемы криптографической защиты информации государственной информационной системы управления общественными финансам</i>	Лит.	Лист	Листов
Пров.		Повышев					5	182
Реценз.						ЮУрГУ		
Н. Контр.		Мартынов				Кафедра ЗИ		
Утв.		Соколов						

## ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ .....	9
1. АНАЛИТИЧЕСКАЯ ЧАСТЬ .....	10
1.1. Общая характеристика Министерства финансов .....	10
1.2. Основные виды деятельности .....	10
1.3. Выявление защищаемой информации .....	11
1.4. Описание ГИС управления общественными финансами .....	11
1.5. Выявление объектов защиты .....	18
1.6. Вывод .....	18
2. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ .....	20
2.1. Статус информационных систем государственных органов .....	20
2.2. Законодательство в сфере криптографии .....	21
2.3. Стандарты Российской Федерации в сфере шифрования .....	25
2.3.1. Блочный шифр .....	25
2.3.2. Функция хэширования .....	26
2.3.3. Электронная подпись .....	27
2.4. Обеспечение безопасности персональных данных с использованием средств криптографической защиты информации .....	28
2.5. Удостоверяющий центр и электронная подпись .....	29
2.6. Требования к использованию криптографических средств .....	32
2.7. Требования к государственным информационным системам .....	33
2.8. Вывод .....	36
3. ПРАКТИЧЕСКАЯ ЧАСТЬ .....	38
3.1. Организационные и технические меры .....	38
3.2. Система криптографической защиты ViPNet .....	40
3.3. Средства электронной подписи .....	43
3.4. Схема обеспечения информационной безопасности государственной информационной системы управления общественными финансами .....	45
3.5. Проект подсистемы криптографической защиты информации государственной информационной системы управления общественными финансами .....	50
3.6. Разработка организационно-распорядительной документации .....	52
3.7. Вывод .....	54
ЗАКЛЮЧЕНИЕ .....	56
БИБЛИОГРАФИЧЕСКИЙ СПИСОК .....	58
ПРИЛОЖЕНИЕ А .....	60
ПРИЛОЖЕНИЕ Б .....	76
ПРИЛОЖЕНИЕ В .....	78
ПРИЛОЖЕНИЕ Г .....	79
ПРИЛОЖЕНИЕ Д .....	81
ПРИЛОЖЕНИЕ Е .....	104
ПРИЛОЖЕНИЕ Ж .....	105
ПРИЛОЖЕНИЕ З .....	118
ПРИЛОЖЕНИЕ И .....	119

ПРИЛОЖЕНИЕ К .....	131
ПРИЛОЖЕНИЕ Л .....	137
ПРИЛОЖЕНИЕ М .....	139
ПРИЛОЖЕНИЕ Н .....	144

## СПИСОК СОКРАЩЕНИЙ

АРМ – автоматизированное рабочее место  
ГИС – государственная информационная система  
ГРБС – главные распорядители бюджетных средств  
КЗ – контролируемая зона  
ЛВС – локальная вычислительная сеть  
Минфин – Министерство финансов Челябинской области  
НСД – несанкционированный доступ  
ПАК – программно-аппаратный комплекс  
ПБС – получатели бюджетных средств  
ПДн – персональные данные  
ПО – программное обеспечение  
СЗИ – средство защиты информации  
СКЗИ – средства криптографической защиты информации  
УЗ – уровень защищенности  
ФАПСИ – Федеральное агентство правительственной связи и информации при Президенте Российской Федерации  
ФСБ – Федеральная служба безопасности Российской Федерации  
ФСТЭК – Федеральная служба по техническому и экспортному контролю  
ЭП – электронная подпись (электронно-цифровая подпись)

## ВВЕДЕНИЕ

В настоящее время все большую важность приобретает проблема обеспечения защиты информации. Для стабильного функционирования информационной среды предприятия, а также для минимизации рисков и потерь необходимо тщательно рассмотреть каждый аспект защиты информации. Помимо организационных, правовых и программно-аппаратных аспектов, немаловажным аспектом является защита информации криптографическими методами.

Существенное увеличение объема обрабатываемой информации приводит к необходимости улучшения методов сбора, обработки, хранения информации в организациях любого масштаба. На государственном уровне создаются государственные информационные системы в целях реализации полномочий государственных органов и обеспечения обмена информацией между ними, а также в иных предусмотренных законодательством целях. В последний год наблюдается рост количества создаваемых ГИС в связи с высказанной позицией Управления ФСТЭК России по Уральскому федеральному округу, по вопросу ГИС: «Если система не признана государственной информационной системой, но имеет признаки ее признаки (создана в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами), ФСТЭК будет считать её государственной информационной системой.»

Таким образом, актуальность работы обусловлена необходимостью создания государственной информационной системы управления общественными финансами в связи с необходимостью исполнения требований законодательства Российской Федерации.

Объектом данной работы является Министерство финансов Челябинской области, а предметом является информация ограниченного доступа, обрабатываемая в Министерстве финансов Челябинской области.

Целью выпускной квалификационной работы является разработка проекта подсистемы криптографической защиты информации государственной информационной системы управления общественными финансами. Для реализации поставленной цели необходимо решить следующие задачи:

- 1) провести анализ учреждения;
- 2) изучить нормативные правовые акты, регулирующие создание ГИС и применение криптографических средств;
- 3) изучить криптографические средства, выбранные для построения подсистемы криптографической защиты информации, произвести их настройку;
- 4) разработать проект подсистемы криптографической защиты информации;
- 5) подготовить организационно-распорядительные документы, необходимые для функционирования подсистемы криптографической защиты информации.