

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

\_\_\_\_\_ 2020 г.

**Модернизация модуля информационной системы для контроля  
трафика и предотвращения угроз информационной безопасности  
на предприятии АО «НПО Электромашина»**

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА  
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ  
ЮУрГУ – 10.03.01.2020.157.ПЗ ВКР**

Руководитель проекта,

д.п.н., проф.

\_\_\_\_\_ Л.В. Астахова

\_\_\_\_\_ 2020 г.

Автор проекта,

студент группы КЭ-407

\_\_\_\_\_ А. В. Некрасов

\_\_\_\_\_ 2020 г.

Нормоконтролер,

к.т.н., доцент

\_\_\_\_\_ В. П. Мартынов

\_\_\_\_\_ 2020 г.

## АННОТАЦИЯ

Некрасов А. В. Модернизация модуля информационной системы для контроля трафика и предотвращения угроз информационной безопасности на предприятии АО «НПО Электромашина» – Челябинск: ЮУрГУ, КЭ-407, 121 с., 8 ил., 16 табл., библиогр. список – 16 наим., 10 прил.

Выпускная квалификационная работа выполнена с целью совершенствования системы защиты конфиденциальной информации в акционерном обществе АО «НПО Электромашина».

В выпускной квалификационной работе отражены все этапы создания системы защиты персональных данных и коммерческой тайны, от сбора исходных данных до заключения о соответствии нормативным документам РФ по защите персональных данных и коммерческой тайны.

В процессе выполнения квалификационной работы было проведено предпроектное обследование предприятия, созданы все необходимые документы, регламентирующие порядок защиты информации, а также описывающих информационную систему персональных данных предприятия. Было проведено проектирование системы защиты, включающее в себя выбор средств защиты, предотвращающих актуальные угрозы предприятия, обоснования их эффективности и экономической целесообразности.

					ЮУрГУ – 10.03.01.2020.157.ПЗ ВКР			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.		Некрасов			<i>Модернизация модуля информационной системы для контроля трафика и предотвращения угроз информационной безопасности на предприятии АО «НПО Электромашина»</i>	Лит.	Лист	Листов
Пров.		Астахова					5	121
Реценз.						ЮУрГУ		
Н. Контр.		Мартынов				Кафедра ЗИ		
Утв.		Соколов						

## ОГЛАВЛЕНИЕ

Сокращения и определения.....	8
Введение.....	9
1. Анализ состояния информационной системы .....	11
1.1. Разработка технического паспорта .....	11
1.2. Разработка модели деятельности .....	11
1.3. Выявление защищаемой информации .....	11
1.4. Описание информационной системы .....	12
1.5. Выявление объектов защиты .....	15
1.6. Анализ введенного режима коммерческой тайны.....	15
1.7. Разработка модели угроз и уязвимостей для важных объектов защиты..	16
1.7.1. Общие положения.....	16
1.7.2. Определение уровня исходной защищённости .....	16
1.7.3. Определение актуальных угроз безопасности информации.....	17
1.7.4. Составление перечня приоритетных к устранению угроз .....	25
1.8. Разработка технического задания на модернизацию системы защиты информации на предприятии .....	26
1.9. Вывод.....	26
2. Теоретическое обоснование выбора средств защиты .....	28
2.1. Обзор возможных методов устранения уязвимостей.....	28
2.2. Угрозы утечки информации.....	28
2.2.1. Классификация видов утечки .....	28
2.2.2. Основные каналы утечки информации .....	30
2.2.3. Нормативная основа.....	31
2.3. Системы защиты от утечек конфиденциальной информации (DLP) .....	33
2.4. Обзор DLP решений.....	35
2.5. Вывод.....	55
3. Разработка технического задания по модернизации модуля информационной системы для контроля трафика и предотвращения угроз информационной безопасности на предприятии АО «НПО Электромашина» .....	56
3.1. Описание объекта.....	56
3.2. Резюме технического задания.....	56
3.3. Цели и задачи технического задания .....	56
3.4. Объекты поставки технического задания.....	57

3.4.1. Организационно-распорядительная документация .....	57
3.4.2. Организационные меры .....	57
3.4.3. Программно-аппаратные и инженерно-технические меры.....	58
3.4.4. Обучение персонала .....	58
3.5. Риски технического задания .....	58
3.6. Вывод.....	60
Заключение .....	62
Библиографический список .....	64
Приложение А .....	66
Приложение Б.....	76
Приложение В.....	82
Приложение Г .....	91
Приложение Д .....	95
Приложение Е.....	99
Приложение Ж.....	108
Приложение З .....	109
Приложение И .....	111
Приложение К.....	112

## СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

- ИБ – информационная безопасность;
- ЗИ – защита информации;
- ИС – информационная система;
- АРМ – автоматизированные рабочие места;
- ПД – персональные данные;
- КТ – коммерческая тайна;
- КЗ – контролируемая зона;
- ФСБ – Федеральная служба безопасности;
- ИТ – информационные технологии;
- ТЗ – техническое задание;
- ФЗ – Федеральный закон;
- ОС – операционная система;
- СЗИ – система защиты информации;
- ПАК – программно-аппаратный комплекс;
- АО – акционерное общество;
- ПЭВМ – персональная электронная вычислительная машина;
- ПК – персональный компьютер;
- ПО – программное обеспечение;
- НСД – несанкционированный доступ;
- РФ – Российская Федерация;
- БД – Базы данных;
- ФСТЭК – Федеральная служба по техническому и экспортному контролю;
- Утечки информации — неправомерная передача конфиденциальных сведений (материалов, важных для различных компаний или государства, персональных данных граждан), которая может быть умышленной или случайной.
- Фишинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

## ВВЕДЕНИЕ

Современные организации используют всё большее количество информационных систем (ИС) для хранения, обработки и распространения ценных информационных активов. С ростом ИС растёт и число инцидентов информационной безопасности. Какие именно информационные активы считаются ценными зависит от организации, но примерами являются стратегическая информация и интеллектуальная собственность, которые дают организации конкурентное преимущество.

Большое количество инцидентов ИБ связано именно с утечкой конфиденциальных данных, увеличивающееся с каждым годом. Это обусловлено тем, что традиционные средства защиты, такие как антивирусы, межсетевые экраны и системы аутентификации, не способны обеспечить эффективную защиту от внутренних нарушителей [15].

В 2013 г. были утверждены приказ ФСТЭК России № 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" и приказ ФСТЭК России № 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах". В 2014 г. был утвержден методический документ "Меры защиты информации в государственных информационных системах", раскрывающий и детализирующий меры защиты, определенные в приказах. Также в 2014 г. издан проект нормативного правового акта ФСТЭК России "Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды". Данные документы имеют схожий набор мер по защите информации.

Применение систем предотвращения утечек информации позволяет эффективно обеспечить защиту информации с выполнением мер перечисленных в нормативных документах. Внутренний нарушитель является наиболее опасным (инсайдерские угрозы), системы DLP-системы ориентированы на борьбу именно с внутренними нарушителями, и потому являются приоритетным инструментом обеспечения информационной безопасности для организации, желающей успешно реализовать требования и пройти аудит соответствия стандартам ИБ.

Таким образом, актуальность работы выражена в необходимости модернизации модуля информационной системы для контроля трафика и предотвращения угроз информационной безопасности на предприятии АО «НПО Электромашина».

Объектом выпускной квалификационной работы является АО «НПО Электромашина».

Предметом выпускной квалификационной работы является информационная система обработки конфиденциальной информации в ИС предприятия АО «НПО Электромашина».

Целью выпускной квалификационной работы является разработка мер по организации защиты ПД и КТ в ИС предприятия АО «НПО Электромашина».

Для достижения поставленной цели необходимо:

- 1) провести анализ информационной системы предприятия АО «НПО Электромашина»;
- 2) провести теоретическое обоснование выбора средств и методов защиты информации ограниченного доступа;
- 3) разработать техническое задание по модернизации модуля информационной системы для контроля трафика и предотвращения угроз информационной безопасности на предприятии АО «НПО Электромашина».