

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»**

РАБОТА ПРОВЕРЕНА

Рецензент, заместитель директора
ООО «ПНК»

_____ О.А.Наумова
_____ 2019 г.

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой,
к.т.н., доцент

_____ А.Н. Соколов
_____ 2019 г.

**Организация защищенного канала подключения промышленно-
го предприятия к системе электронных паспортов транспортных
средств**

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.05.2019.412.ПЗ ВКР**

Консультанты

Безопасность жизнедеятельности,
к.т.н., доцент

_____ Н.В. Глотова
_____ 2019 г.

Экономическая часть,
ст. преп.

_____ С.А. Сабельников
_____ 2019 г.

Руководитель проекта,
доцент.

_____ В.Ю. Бердюгин
_____ 2019 г.

Автор проекта,
студент группы КЭ-572

_____ А. А. Сатин
_____ 2019 г.

Нормоконтролер,
к.т.н., доцент

_____ В.П. Мартынов
_____ 2019 г.

Челябинск 2019

АННОТАЦИЯ

Сатин А. А. Организация защищенного канала подключения промышленного предприятия к системе электронных паспортов транспортных средств на «Заводе тяжелого машиностроения» – Челябинск: ЮУрГУ, КЭ-572, 91 с., 4 ил., 11 табл., библиогр. список – 20 наим., 6 прил.

Выпускная квалификационная работа выполнена с целью создания защищенного канала связи для подключения к системе электронных паспортов завода тяжелого машиностроения

В выпускной квалификационной работе отражены все этапы создания защищенного канала связи, от сбора исходных данных до заключения о соответствии нормативным документам РФ.

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

					ЮУрГУ – 10.05.05.2019.412.ПЗ ВКР			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.		Сатин			<i>Организация защищенного канала подключения промышленного предприятия к системе электронных паспортов транспортных средств «ПНК»</i>	Лит.	Лист	Листов
Пров.		Бердюгин					6	91
Реценз.		Наумова				ЮУрГУ		
Н. Контр.		Мартынов				Кафедра ЗИ		
Утв.		Соколов						

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ	9
ВВЕДЕНИЕ	10
1 ПОНЯТИЕ ЭЛЕКТРОННЫЙ ПАСПОРТ ТРАНСПОРТНОГО СРЕДСТВА.....	12
1.1 Работа электронного паспорта транспортного средства.....	12
1.1.1 Описание и предназначение электронного паспорта транспортного средства.....	12
1.1.2 Сведения, содержащиеся в электронном паспорте транспортного средства.....	12
1.2 Правовое регулирование для подключения к системе электронных паспортов	13
1.3 Защищённая сеть передачи данных системы электронных паспортов	14
1.4 Порядок подключения заявителя к защищенному каналу передачи данных системы электронных паспортов	15
1.4.1 Определение Заявителем схемы подключения к защищенному каналу передачи данных системы электронных паспортов.....	15
1.4.2 Приобретение средств защиты информации	22
1.4.3 Обеспечение Заявителем установки и настройки средств защиты информации	22
1.4.4 Заключение Соглашения между Заявителем и Оператором о предоставлении доступа к защищенному каналу передачи данных системы электронных паспортов.....	22
1.5 Вывод	23
2 АНАЛИЗ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ЗАВОДЕ ТЯЖЕЛОВЕСНЫХ МАШИН	24
2.1 Разработка технического паспорта.....	24
2.2 Выявление защищаемой информации.....	25
2.3 Выявление объекта защиты	29
2.4 Построение частной модели угроз	30
2.4.1 Определение актуальности угроз	30
2.4.2 Расчет рисков важных объектов защиты	32
2.4.3 Определение актуальных угроз	33
2.5 Разработка технического задания.....	35
2.6 Вывод	35

3 ПОДГОТОВКА АРМ К ПОДКЛЮЧЕНИЮ ЗАЩИЩЕННОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ СИСТЕМЫ ЭЛЕКТРОННЫХ ПАСПОРТОВ.....	36
3.1 Анализ и выбор средств защиты от несанкционированного доступа	36
3.2 Анализ и выбор средств криптографической защиты.....	44
3.3 Анализ и выбор средств антивирусной защиты	47
3.4 Разработка руководств для пользования.....	48
3.5 Экономическая эффективность	49
3.6 Вывод	51
4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ.....	53
4.1 Введение	53
4.2 Требования к освещению помещения и рабочих мест	53
4.3 Требования к уровню шума	53
4.4 Микроклимат	54
4.5 Электробезопасность.....	54
4.6 Пожарная безопасность.....	55
4.7 Организация рабочего места.....	56
4.8 Сравнение требуемых и фактических параметров	58
4.9 Вывод	60
ЗАКЛЮЧЕНИЕ	61
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	62
ПРИЛОЖЕНИЕ А	64
ПРИЛОЖЕНИЕ Б.....	67
ПРИЛОЖЕНИЕ В	73
ПРИЛОЖЕНИЕ Г.....	78
ПРИЛОЖЕНИЕ Д	82
ПРИЛОЖЕНИЕ Е.....	87

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

СЭП – система электронных паспортов;
ЭПТС – электронный паспорт транспортного средства;
ЗСПД- защищенный канал передачи данных;
ПТС – паспорт транспортного средства;
ЗИ – защита информации;
ИБ – информационная безопасность;
ТЗ – техническое задание;
АРМ - автоматизированные рабочие места
НСД – несанкционированный доступ;
ОС – операционная система;
СЗИ – система защиты информации;
ПЭВМ – персональная электронная вычислительная машина;
ПК – персональный компьютер;
ПО – программное обеспечение;
ИТ – информационные технологии;
РФ – Российская Федерация; Ф
З – Федеральный закон;
ФСБ – Федеральная служба безопасности;
ФСТЭК - Федеральная служба по техническому и экспортному контролю;
ПО – программное обеспечение;
ОТСС – основные технические средства и системы;
ВТСС – вспомогательные технические средства и системы;
ИБП – источник бесперебойного питания;

ВВЕДЕНИЕ

На территории государств-членов Евразийского экономического союза (ЕАЭС) вступило в силу Соглашение о введении единых форм электронных паспортов транспортных средств (ЭПТС), самоходных машин и других видов техники и организации Систем электронных паспортов (СЭП). На данный момент на территории России идет тестирование данной системы. Но уже к концу 2019 года водители должны перейти с бумажных документов на онлайн. Данная система необходима при работе с органами ГИБДД, банками, ломбардами, налоговыми службами и т.д. Благодаря чему структуры при необходимости могут сами запросить информацию об ЭПТС из СЭП. Так же преимуществом для организаций будет:

- исключение необходимости использования бумажных бланков строгой отчетности (их получения хранения учета);
- исключение Госавтоинспекции по выдаче бумажных бланков организациям изготовителям (снижение административной нагрузки на бизнес со стороны держателя бланков, уменьшение коррупционных рисков);
- упрощение процедуры оформления паспорта транспортного средства, связанной с учетом утилизационного сбора.

ЭПТС отражает полную информацию об автомобиле. Приобретая автомобиль, и другие виды самоходной техники они уже будет с оформленным электронным паспортом. Все данные из ЭПТС будут храниться в единой системе электронных паспортов к которой должен подключиться каждый участник СЭП:

- организации-изготовители;
- уполномоченные органы (организации);
- регистрирующие органы;
- таможенные органы;
- правоохранительные органы;
- налоговые органы;
- иные органы государственной власти;
- собственники;
- кредитные организации;
- страховые компании;
- лизинговые компании;
- национальные операторы в государствах-членах ЕАЭС;
- администратор СЭП – АО «Электронный паспорт»

Была поставлена цель: Организовать подключение к защищенной сети передачи данных СЭП России.

Данная тема выпускной дипломной работы является актуальной так как Российская федерация активно развивается и стремится автоматизировать все свои направленные деятельности. Переход от бумажного паспорта к электронной обработке данных требует принятия не только законодательных актов о создании таких систем, но и построение защиты таких систем

Были сформулированы следующие задачи:

- организовать автоматизированное рабочее место (АРМ), которое будет подключено к СЭП;
- составить технический паспорт;
- составить частную модель угроз;
- изучит регламент СЭП, выбрать схему подключения;
- анализ и выбор средств антивирусной защиты и средств защиты от не-санкционированного доступа;
- анализ и выбор средств криптографической защиты;
- составить техническое задание;
- организовать защищенный канал связи в рамках защищенной сети передачи данных СЭП.