

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,

начальник цеха ФГУП «ПСЗ»

\_\_\_\_\_ Н.П. Олейник

\_\_\_\_\_ 2020 г.

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой,

к.т.н., доцент

\_\_\_\_\_ А.Н. Соколов

\_\_\_\_\_ 2020 г.

**Обеспечение безопасности автоматизированной системы  
радиационного контроля ФГУП «Приборостроительный завод»**

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА  
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ  
ЮУрГУ – 10.05.03.2020.409.ПЗ ВКР

Руководитель проекта,  
доцент

\_\_\_\_\_ В.Ю. Бердюгин

\_\_\_\_\_ 2020 г.

Автор проекта,  
студент группы КЭ-555

\_\_\_\_\_ А.А. Ковалева

\_\_\_\_\_ 2020 г.

Нормоконтролер,  
к.т.н., доцент

\_\_\_\_\_ В.П. Мартынов

\_\_\_\_\_ 2020 г.

Челябинск 2020

## АННОТАЦИЯ

Ковалева А.А. Обеспечение безопасности автоматизированной системы радиационного контроля на ФГУП «Приборостроительный завод» – Челябинск: ЮУрГУ, КЭ-555, 131 с., 3 ил., 31 табл., библиогр. список – 9 наим., 13 прил.

Выпускная квалификационная работа выполнена с целью присвоения объекту критической информационной инфраструктуры на Федеральном Государственном Унитарном предприятии «Приборостроительный завод» одной из категорий значимости и модернизацией защиты этого объекта в соответствии с присвоенной категорией.

В выпускной квалификационной работе отражены все этапы: от категорирования до установки актуальных средств защиты и внесения изменений в организационную документацию.

В процессе выполнения квалификационной работы было проведено предпроектное обследование предприятия, созданы все необходимые документы, регламентирующие порядок защиты информации, а также описывающих рассматриваемую автоматизированную систему. Было проведено категорирование объекта с присвоением ему категории значимости а так же модернизация его защиты, включающая в себя выбор средств защиты, предотвращающих актуальные угрозы безопасности.

					ЮУрГУ – 10.05.03.2020.409.ПЗ ВКР			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.		Ковалева			<i>Обеспечение безопасности автоматизированной системы радиационного контроля на ФГУП «Приборостроительный завод»</i>	Лит.	Лист	Листов
Пров.		Бердюгин					6	131
Реценз.		Олейник				ЮУрГУ		
Н. Контр.		Мартынов				Кафедра ЗИ		
Утв.		Соколов						

## ОГЛАВЛЕНИЕ

ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ .....	9
ВВЕДЕНИЕ.....	10
1 ОПИСАНИЕ СУБЪЕКТА КИИ. ОПРЕДЕЛЕНИЕ ПРОЦЕССОВ СУБЪЕКТА КИИ И ВЫЯВЛЕНИЕ СРЕДИ НИХ КРИТИЧЕСКИХ. ОПРЕДЕЛЕНИЕ ОБЪЕКТОВ КИИ, НЕОБХОДИМЫХ ДЛЯ КРИТИЧЕСКИХ ПРОЦЕССОВ ..	12
1.1 Описание субъекта информационной инфраструктуры .....	12
1.2 Определение и описание процессов предприятия .....	13
1.3 Выделение критических процессов.....	14
1.4 Описание информационных систем, обеспечивающих критические процессы.....	15
1.4.1 Автоматизированная система радиационного контроля.....	16
1.5 Выводы по главе .....	17
2 КАТЕГОРИРОВАНИЕ ОБЪЕКТА КИИ. АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ, ВОЗМОЖНЫХ ДЕЙСТВИЙ НАРУШИТЕЛЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ФГУП .....	19
2.1 Модель нарушителей .....	19
2.2 Модель угроз безопасности информации при ее обработке в АСРК .....	25
2.2.1 Возможные способы реализации угроз безопасности.....	25
2.2.2. Актуальные угрозы из банка данных угроз.....	27
2.2.3 Реализация угроз в АСРК .....	32
2.2.4 Актуальные угрозы АСРК.....	35
2.3 Категорирование объекта КИИ.....	36
2.4 Выводы по главе .....	42
3 РАЗРАБОТКА ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. ПОДГОТОВКА СВЕДЕНИЙ О РЕЗУЛЬТАТАХ ПРИСВОЕНИЯ ОБЪЕКТУ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОДНОЙ ИЗ КАТЕГОРИЙ ЗНАЧИМОСТИ .....	44
3.1 Необходимые меры по обеспечению безопасности ЗОКИИ .....	44
3.2 Организационно-распорядительная документация и нормативно-методические документы по защите информации .....	51
3.3 Дополнение адаптированного набора мер по обеспечению безопасности АСРК.....	61
3.4 Подготовка сведений о результатах категорирования.....	61
3.5 Выводы по главе .....	62

ЗАКЛЮЧЕНИЕ .....	64
БИБЛИОГРАФИЧЕСКИЙ СПИСОК .....	66
ПРИЛОЖЕНИЕ А .....	67
ПРИЛОЖЕНИЕ Б.....	75
ПРИЛОЖЕНИЕ В .....	85
ПРИЛОЖЕНИЕ Г .....	91
ПРИЛОЖЕНИЕ Д .....	100
ПРИЛОЖЕНИЕ Е .....	109
ПРИЛОЖЕНИЕ Ж .....	112
ПРИЛОЖЕНИЕ З.....	113
ПРИЛОЖЕНИЕ И.....	115
ПРИЛОЖЕНИЕ К .....	126
ПРИЛОЖЕНИЕ Л .....	127
ПРИЛОЖЕНИЕ М .....	130
ПРИЛОЖЕНИЕ Н.....	131

## ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

- АИБ – администратор информационной безопасности;
- АПКШ – аппаратно-программный комплекс шифрования;
- АРМ – автоматизированное рабочее место;
- АС – автоматизированная система;
- ВДТ – видеодисплейный терминал;
- ВКР – выпускная квалификационная работа;
- ГК – государственная корпорация;
- ЗАТО – закрытое административно-территориальное образование;
- ЗОКИИ – значимый объект критической информационной инфраструктуры;
- ИБ – информационная безопасность;
- ИБП – источник бесперебойного питания;
- ИС – информационная система;
- КИИ – критическая информационная инфраструктура;
- НСД – несанкционированный доступ;
- ОКИИ – объект критической информационной инфраструктуры;
- ОС – операционная система;
- ПО – программное обеспечение;
- ПРД – правила разграничения доступа;
- ПЭВМ – персональная электронная вычислительная машина;
- САВЗ – средство антивирусной защиты;
- СВТ – средство вычислительной техники;
- СЗИ – система защиты информации;
- СКЗИ – система криптографической защиты информации;
- ТС – техническое средство;
- ФСТЭК – федеральная служба по техническому и экспортному контролю.

## ВВЕДЕНИЕ

В последние годы законодательство Российской Федерации в области обеспечения безопасности претерпевает значительные изменения.

Вступил в силу новый федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017, который регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры (КИИ) РФ. В документе сформулированы определения субъекта и объекта КИИ, безопасности КИИ и компьютерного инцидента.

Издано Постановление Правительства РФ № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» от 08.02.2018. В документе определены правила категорирования объектов КИИ.

Принят Приказ ФСТЭК № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ» от 25.12.2017.

В текущий период времени законодательство активно изменяется, обновляется и совершенствуется, обязывая предприятия создавать, пересматривать и корректировать меры по обеспечению безопасности информационной инфраструктуры предприятия.

Актуальность ВКР обусловлена необходимостью обеспечения безопасности объекта критической информационной инфраструктуры предприятия, в условиях современного законодательства.

В качестве субъекта критической информационной инфраструктуры я выбрала одно из ведущих предприятий Росатома – Федеральное государственное унитарное предприятие «Приборостроительный завод» (ФГУП «ПСЗ»).

Целью дипломной работы является обеспечение безопасности объекта критической информационной инфраструктуры государственного предприя-

тия.

Для реализации поставленной цели необходимо решить следующие задачи:

1) Описать общую структуру субъекта КИИ, определить его процессы и объекты, которые обеспечивают критические процессы.

2) Провести категорирование выбранного объекта критической информационной инфраструктуры в соответствии с критериями значимости и показателями их значений.

3) Провести анализ угроз безопасности, с учетом банка данных угроз ФСТЭК, и возможных действий нарушителя критической информационной инфраструктуры ПСЗ.

4) Разработать меры (организационные и технические) для обеспечения безопасности значимых объектов критической информационной инфраструктуры, провести выбор дополнительных СрЗИ, описать применяемые средства и меры защиты информации для объекта.

5) Подготовить в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости.