

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.

**Организация процесса категорирования объектов критической
информационной инфраструктуры
АО «Миасский машиностроительный завод»**

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.03.01.2019.187.ПЗ ВКР

Руководитель проекта,
Индивидуальный предприниматель
_____ С.А. Сабельников
_____ 2019 г.

Автор проекта,
студент группы КЭ-454
_____ М.О. Авшенюк
_____ 2019 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2019 г.

Челябинск 2019

АННОТАЦИЯ

Авшенюк М.О. Организация процесса категорирования объектов критической информационной инфраструктуры АО «Миасский Машиностроительный Завод» – Челябинск: ЮУрГУ, КЭ-454, 129 с., 1 ил., 12 табл., библиогр. список – 14 наим., 14 прил.

Выпускная квалификационная работа выполнена с целью проработки вопросов и реализации требований по обеспечению безопасности информации на объекте критической информационной инфраструктуры государственного предприятия.

В выпускной квалификационной работе отражены все этапы категорирования объектов критической информационной инфраструктуры Российской Федерации (КИИ) от описания общей структуры субъекта КИИ до передачи сведений в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации о значимых объектах КИИ.

В процессе выполнения квалификационной работы было проведено исследование и описание субъекта КИИ, выделены критические процессы и информационные системы, обеспечивающие эти процессы. Проведен анализ угроз безопасности информации с учетом банка данных угроз ФСТЭК, подготовлена модель угроз для объекта КИИ. Проведено категорирование ИС, объекту присвоена категория значимости. Разработаны требования к обеспечению безопасности КИИ.

					ЮУрГУ – 10.03.01.2019.187.ПЗ ВКР			
Изм.	Лист	№ докум.	Подпись	Дата	<i>Организация процесса категорирования объектов критической информационной инфраструктуры АО «ММЗ»</i>	Лит.	Лист	Листов
Разраб.		Авшенюк						
Пров.		Сабельников					5	129
Реценз.						ЮУрГУ Кафедра ЗИ		
Н. Контр.		Мартынов						
Утв.		Соколов						

ОГЛАВЛЕНИЕ

ОГЛАВЛЕНИЕ	5
ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ	7
ВВЕДЕНИЕ.....	9
1 ОПИСАНИЕ СУБЪЕКТА КИИ. ОПРЕДЕЛЕНИЕ ПРОЦЕССОВ СУБЪЕКТА КИИ И ВЫЯВЛЕНИЕ СРЕДИ НИХ КРИТИЧЕСКИХ. ОПРЕДЕЛЕНИЕ ОБЪЕКТОВ КИИ, НЕОБХОДИМЫХ ДЛЯ КРИТИЧЕСКИХ ПРОЦЕССОВ	10
1.1 Правовые основы защиты информации в АО «ММЗ».....	10
1.2 Описание субъекта информационной инфраструктуры	10
1.3 Определение и описание процессов предприятия.....	11
1.4 Выделение критических процессов	13
1.5 Описание информационных систем, обеспечивающих критические процессы.....	14
1.6 Автоматизированная система «Проекты».....	14
1.7 Автоматизированная система «Расчеты»	17
1.8 Информационная система персональных данных «Управление персоналом».....	20
1.9 Выводы.....	23
2 КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ КИИ. АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ, ВОЗМОЖНЫХ ДЕЙСТВИЙ НАРУШИТЕЛЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРОЕКТНОГО ЗАВОДА	25
2.1 Модель нарушителей.....	25
2.2 Модель безопасности данных при их обработке в АС ИАС «Проекты». 29	
2.2.1 Возможные способы реализации угроз безопасности информации ...	29
2.2.2 Анализ угроз безопасности данных при их обработке в АС ИАС «Проекты»	30
2.2.3 Актуальные угрозы АС ИАС «Проекты»	38
2.3 Категорирование объекта КИИ	39
2.4 Выводы.....	44
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	45

3.1 Необходимые меры по обеспечению безопасности ЗОКИИ.....	45
3.2 Организационно-распорядительная документация и нормативно-методические документы по защите информации	50
3.3 Реализованные меры по обеспечению безопасности АС ИАС «Проекты».....	51
3.4 Дополнение адаптированного набора мер по обеспечению безопасности АС ИАС «Проекты».....	57
3.5 Подготовка сведений о результатах категорирования.....	57
3.6 Выводы.....	58
ЗАКЛЮЧЕНИЕ	59
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	60
ПРИЛОЖЕНИЕ А	61
ПРИЛОЖЕНИЕ Б.....	62
ПРИЛОЖЕНИЕ Г.....	84
ПРИЛОЖЕНИЕ Д	88
ПРИЛОЖЕНИЕ Е.....	95
ПРИЛОЖЕНИЕ Ж	102
ПРИЛОЖЕНИЕ З.....	109
ПРИЛОЖЕНИЕ И	110
ПРИЛОЖЕНИЕ К	112
ПРИЛОЖЕНИЕ Л	123
ПРИЛОЖЕНИЕ М	124
ПРИЛОЖЕНИЕ Н	127
ПРИЛОЖЕНИЕ О	128
ПРИЛОЖЕНИЕ П	129

ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

Автоматизированная система управления – комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления таким оборудованием и процессами;

Безопасность критической информационной инфраструктуры – состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;

Значимый объект критической информационной инфраструктуры – объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки;

Критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

Объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

Субъекты критической информационной инфраструктуры – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

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;
 ЗОКИИ – значимый объект критической информационной инфраструктуры;
 ИАС – информационно-аналитическая система;
 ИБ – информационная безопасность;
 ИБП – источник бесперебойного питания;
 ИС – информационная система;
 ИСПДн – информационная система персональных данных;
 КИИ – критическая информационная инфраструктура;
 НЖМД – накопитель на жестких магнитных дисках;
 НИОКР – научно-исследовательская опытно-конструкторская работа;
 НИР – научно-исследовательская работа;
 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;
 СМНИ – съемный машинный носитель информации;
 СрЗИ – средство защиты информации;
 ТС – техническое средство;
 ФСТЭК – Федеральная служба по техническому и экспортному контролю.

ВВЕДЕНИЕ

Актуальность выпускной квалификационной работы обусловлена необходимостью обеспечения безопасности информации на объекте критической информационной инфраструктуры предприятия, в условиях современного законодательства.

Объектом выпускной квалификационной работы является предприятие, работающее с государственными и оборонными заказами.

Предметом выпускной квалификационной работы является критическая информационная инфраструктура государственного предприятия.

Целью дипломной работы является обеспечение безопасности информации на объекте критической информационной инфраструктуры государственного предприятия.

В соответствии с поставленной целью необходимо решить следующие задачи:

1) Описать общую структуру субъекта КИИ с его процессами и объектами, обеспечивающими 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 проектного предприятия.

4) Разработать организационные и технические меры 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.