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.

ОГЛАВЛЕНИЕ

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.