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.С.Наумова
_____ 2019 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2019 г.

Обеспечение безопасности критическое информационной инфраструктуры АО «Завод «Пластмасс»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2019.388.ПЗ ВКР

Консультанты
Безопасность жизнедеятельности,
к.т.н., доцент
_____ Н.В. Глотова
_____ 2019 г.

Руководитель проекта,
н.с. НОЦ «Информационная безопасность»
_____ А.Е. Баринов
_____ 2019 г.

Автор проекта,
студент группы КЭ-570
_____ Н.Ю.Трегубов
_____ 2019 г.

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

Челябинск 2019

АННОТАЦИЯ

Трегубов Н.Ю. Обеспечение безопасности критическое информационной инфраструктуры АО «Завод «Пластмасс» – Челябинск: ЮУрГУ, КТУР-570, 87 с., 1 ил., 9 табл., библиогр. список – 8 наим., 5 прил.

Целью выпускной квалификационной работы является изучение вопросов и реализация требований по обеспечению безопасности информации на объекте критической информационной инфраструктуры (КИИ).

В выпускной квалификационной работе отражены поочередно все этапы обеспечения безопасности критической информационной инфраструктуры РФ, от описания, до отправки сведений о значимых объектах КИИ в федеральный орган исполнительной власти.

В процессе выполнения работы было проведено исследование субъекта критической информационной инфраструктуры с последующим его описанием, были выделены критические процессы для предприятия и информационные системы обеспечивающие их. Проведен анализ угроз безопасности информации с учетом банка данных угроз ФСТЭК. Подготовлена модель угроз. Проведено категорирование и присвоена категория значимости. Разработаны требования к обеспечению безопасности КИИ.

ОГЛАВЛЕНИЕ

ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

АИБ – администратор информационной безопасности
АПКШ – аппаратно-программный комплекс шифрования
АРМ – автоматизированное рабочее место
АС – автоматизированная система
АСП – авиационные средства поражения
АТС – автоматическая телефонная станция
ВКР – выпускная квалификационная работа
ГК – государственная корпорация
ЗО КИИ – значимый объект критической информационной инфраструктуры
ИАС – информационно-аналитическая система
ИБ – информационная безопасность
ИБП – источник бесперебойного питания
ИТС – информационной телекоммуникационная сеть
ИС – информационная система
КИИ – критическая информационная инфраструктура
КП – критические процессы
НСД – несанкционированный доступ
О КИИ - 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

В последние годы законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры стремительно развивается.

Вступает в силу новый федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017, регулирующий отношения в области обеспечения безопасности критической информационной инфраструктуры РФ. В документе сформулированы ключевые определения такие как: автоматизированная система управления, компьютерный инцидент и компьютерная атака, субъект и объект КИИ.

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 и Приказ ФСТЭК России №60 от 26.03.2019 «О внесении изменений в Требования по обеспечению безопасности значимых объектов КИИ РФ, утвержденные приказом ФСТЭК №239 от 25.12.2017»

В текущий период времени законодательство корректируется, обновляется и совершенствуется, обязывая предприятия адаптировать меры по обеспечению безопасности информационной инфраструктуры предприятия.

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

Объектом выпускной квалификационной работы является оборонное предприятие.

Предметом выпускной квалификационной работы является безопасность критической информационной инфраструктуры оборонного предприятия.

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

В соответствии с поставленной целью необходимо решить следующие задачи:

- Описать общую структуру субъекта КИИ с его процессами и объектами, выделить критические процессы.
- Провести категорирование выбранного объекта критической информационной инфраструктуры в соответствии с критериями значимости и показателями их значений.
- Провести анализ угроз безопасности, с учетом банка данных угроз ФСТЭК, и возможных действий нарушителя критической информационной инфраструктуры.

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

- 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.