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 отдела защиты информационных систем ООО «ПНК»
_____О.А. Наумова
_____ 2019 г.

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

Организация процесса категорирования объектов критической информационной инфраструктуры машиностроительного предприятия

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2019.390.ПЗ ВКР

Консультанты

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

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

Автор проекта,
студент группы КЭ-570
_____ А.В. Хмель
_____ 2019 г.

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

Челябинск 2019

АННОТАЦИЯ

Хмель А.В. Обеспечение информационной безопасности на объектах критической информационной инфраструктуры машиностроительного предприятия – Челябинск: ЮУрГУ, КЭ-570, 127 с., 2 ил., 12 табл., библиогр. список – 19 наим., 5 прил.

Целью выполнения выпускной квалификационной работы является организация процесса категорирования объектов КИИ машиностроительного предприятия, подготовка сведений о результатах присвоения объектам КИИ категорий значимости либо об отсутствии таких категорий для отправки во ФСТЭК и анализ мер по обеспечению безопасности для значимых объектов КИИ.

В первой главе описана структура предприятия, определена принадлежность предприятия к субъектам критической информационной инфраструктуры, составлен приказ о создании комиссии, определены и описаны процессы предприятия, выделены критические процессы, составлен перечень объектов критической информационной инфраструктуры и произведено описание каждого из объектов критической информационной инфраструктуры.

Во второй главе проведен анализ угроз безопасности информации объектов КИИ и категорий нарушителей, были установлены возможные негативные последствия, которые могут возникнуть в случае возникновения сбоев в работе объектов КИИ. На основании установленных возможных негативных последствий объектам КИИ были присвоены категории значимости.

В третьей главе подготовлены сведения о результатах присвоения объектам КИИ категорий значимости для отправки во ФСТЭК и установлено какие меры по обеспечению безопасности значимых объектов КИИ уже реализованы на предприятии, а какие требуется реализовать, были выбраны способы реализации данных мер.

Так как информация о предприятии, приведенная в данной выпускной квалификационной работе является информацией ограниченного доступа, некоторые данные искажены и название предприятия не раскрывается.

ОГЛАВЛЕНИЕ

ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

АРМ - автоматизированное рабочее место
АСУ- автоматизированная система управления
ГИС - государственная информационная система
ИБП - источник бесперебойного питания
ИС - информационная система
ИТС - информационно-телекоммуникационные сети
КЗ - контролируемая зона
КСИИ - ключевые системы информационной инфраструктуры
КИИ - критические информационные инфраструктуры
МФУ - многофункциональное устройство
МЭ – межсетевое экранирование
НДВ - недекларированные возможности
НСД - несанкционированный доступ
ПО - программное обеспечение
СКЗИ - средства криптографической защиты информации
СЗИ - средства защиты информации
ТКУИ - технические каналы утечки информации
ТП – технический процесс
УБИ - угрозы безопасности информации
УП - управляющая программа
ФСТЭК - Федеральная служба по техническому и экспортному контролю
ЧПУ - числовое программное управление
ЭП - электронная подпись

ВВЕДЕНИЕ

В настоящее время в Российской Федерации в области безопасности критической информационной инфраструктуры действуют следующие нормативные документы:

- Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 [1], который регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

- Постановление Правительства РФ от 8 февраля 2018 г. № 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» [2], которое содержит правила, устанавливающие порядок и сроки категорирования объектов критической информационной инфраструктуры Российской Федерации.

- Приказ ФСТЭК от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ» [3], содержащий требования, направленные на обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры Российской Федерации при проведении в отношении них компьютерных атак.

Были внесены и вступили в силу изменения Уголовного кодекса РФ [6], согласно которым Уголовный кодекс Российской Федерации дополнен статьёй 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» [4]. Были внесены изменения в прочие отдельные законодательные акты РФ [15].

Исходя из требований законодательства в области обеспечения безопасности КИИ для всех государственных органов, государственных учреждений, российских юридических лиц и индивидуальных предпринимателей, которым на праве собственности, аренды или на ином законном основании принадлежат ИС, ИТС, АСУ, требуется определить принадлежность данного субъекта к КИИ. При принадлежности к КИИ субъект обязан провести категорирование имеющихся у него ИС, ИТС и АСУ и определить состав мер защиты информации.

Актуальность выпускной квалификационной работы обусловлена требованиями действующего законодательства.

Объектом выпускной квалификационной работы является машиностроительное предприятие.

Предметом выпускной квалификационной работы является безопасность критической информационной инфраструктуры Машиностроительного предприятия в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Целью выпускной квалификационной работы является организация процесса категорирования объектов критической информационной инфраструктуры машиностроительного предприятия и анализ мер по обеспечению безопасности значимых объектов КИИ в соответствии с присвоенными категориями значимости.

Задачами выпускной квалификационной работы в связи с указанной целью являются:

1. Описание машиностроительного предприятия и сбор исходных данных для категорирования.
2. Анализ угроз безопасности и возможных действий нарушителя.
3. Категорирование объектов КИИ машиностроительного предприятия.
4. Подготовка сведений о результатах категорирования для отправки во ФСТЭК.
5. Анализ мер по обеспечению безопасности значимых объектов КИИ.