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, ведущий специалист по
обеспечению инф. безопасности,
ПАО «ЧТПЗ»
_____ М.Н. Семёнов
_____ 2020 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2020 г.

# Автоматизированная система управления событиями информационной безопасности в корпоративной сети ПАО «ЧТПЗ»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2020.408.ПЗ ВКР

Руководитель проекта,
специалист по ЗИ
_____А.Е. Баринов
_____ 2020 г.

Автор проекта,
студент группы КЭ-555
_____Э.Р. Исрафилов
_____ 2020 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2020 г.

Челябинск 2020

# АННОТАЦИЯ

Исрафилов Э.Р. Автоматизированная система управления событиями информационной безопасности в корпоративной сети ПАО «ЧТПЗ» – Челябинск: ЮУрГУ, КЭ-555, 73 с., 29 ил., 8 табл., библиогр. список – 35 наим., 2 прил.

Выпускная квалификационная работа выполнена с целью анализа процесса мониторинга автоматизированной системы, корпоративной сети ПАО «ЧТПЗ, для повышения эффективности управления инцидентами в результате внедрения и сопровождения MaxPatrol SIEM от компании Positive Technologies.

В выпускной квалификационной работе отражены этапы внедрения, конфигурации и сопровождения автоматизированной системы по управлению событиями информационной безопасности в корпоративной сети, от анализа рынка доступных решений на рынке SIEM – систем, до сопровождения, финальной конфигурации продукта.

В процессе выполнения квалификационной работы было проведено предпроектное обследование предприятия, проведены все необходимые исследования, обоснован выбор необходимого продукта, а также проведены работы по внедрению и сопровождению.

СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

Управление инцидентами информационной безопасности (ИБ) на сегодняшний день является одной из наиболее обсуждаемых и актуальных тем для многих компаний и организаций. Это связано с тем, что управление инцидентами ИБ является важнейшим процессом развития и совершенствования всей системы управления информационной безопасности (СУИБ). Обозначенный процесс позволяет определить конкретные уязвимости ИБ компании, обнаружить следы атак и вторжений в информационную среду компании, что, в свою очередь, дает информацию о слабостях в системе защиты информации. Таким образом, управление инцидентами ИБ позволяет оценить эффективность СУИБ, определить ключевые роли персонала в результате возникновения нештатных ситуаций, и главное, за минимальный промежуток времени принять необходимые меры для восстановления полноценной работы компании.

Тема: Автоматизированная система управления событиями информационной безопасности в корпоративной сети ПАО «ЧТПЗ».

Объектом исследования является мониторинг информационных инцидентов во внутренних сетях промышленного предприятия.

Предмет исследования: автоматизация работы систем службы информационной безопасности во внутренних сетях промышленного предприятия.

Цель исследования: повышение эффективности мониторинга инцидентов во внутренних сетях промышленного предприятия в результате внедрения и сопровождения системы MaxPatrol SIEM.

Задачи:

Провести анализ процесса мониторинга информационных инцидентов во внутренних сетях промышленного предприятия

Описать постановку задачи на внедрение и сопровождение системы мониторинга информационных инцидентов во внутренних сетях промышленного предприятия (SIEM-системы).

1. Обосновать выбор MaxPatrol SIEM Positive Technologies.
2. Провести обзор архитектуры MaxPatrol SIEM Positive Technologies.
3. Разработать проектные решения по сопровождению системы мониторинга информационных инцидентов MaxPatrol SIEM Positive Technologies.
4. Разобрать принцип работы с продуктом.

В процессе исследования использованы следующие методы исследования и инструменты: теоретические методы: анализ, классификация, многокритериальный анализ; эмпирические методы: наблюдение, сравнение, измерение; инструменты моделирования бизнес-процессов.