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, сотрудник отдела защиты информации
ООО «АГАМА»
_____ А.В.Майер
_____ 2019 г.

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

# Модернизация технологии процесса выявления инцидентов информационной безопасности в организации на основе SIEM-системы

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.05.2019.355.ПЗ ВКР

Консультанты

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

Экономическая часть,
ст. преп.
_____ С.А. Сабельников
_____ 2019 г.

Руководитель проекта,
к.ю.н., доцент
_____ В.Л. Жернова
_____ 2019 г.

Автор проекта,
студент группы КЭ-572
_____ В.Д. Каменев
_____ 2019 г.

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

Челябинск 2019

# АННОТАЦИЯ

Каменев В.Д. Модернизация технологии процесса выявления инцидентов информационной безопасности в организации на основе SIEM - систем - Челябинск: ЮУрГУ, КЭ-572, 99 с., 23 ил., 18 табл., библиогр. список - 11 наим., 4 прил.

Выпускная квалификационная работа состоит из введения, теоретической части, практической части, разделов оценки рисков информационной безопасности, части обоснования экономической эффективности, части безопасности жизнедеятельности, заключения и списка использованных источников.

В выпускной квалификационной работе описан объект защиты, приведен обзор нормативно-правовых документов, проанализирован рынок SIEM-систем, проведено их сравнение по функциональным характеристикам, осуществлен выбор оптимальной системы.

В разделах оценки рисков информационной безопасности приведены результаты расчетов рисков информационной безопасности спроектированной системы защиты.

В разделе обоснования экономической эффективности приведены расчёты экономической эффективности создания и внедрения SIEM-системы в информационную инфраструктуру предприятия.

ОГЛАВЛЕНИЕ

# СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АО - Акционерное общество;

ГРЦ - Государственный ракетный центр;

АС - автоматизированная система;

ИБ - информационная безопасность;

ИТ - информационные технологии;

ЗИ - защита информации;

АРМ - автоматизированное рабочее место;

ПДн - персональные данные;

ДСП - для служебного пользования;

СЗИ - средство защиты информации;

НСД - несанкционированный доступ;

ИС - информационная система;

ИСПДн - информационная система персональных данных;

ОС - операционная система;

ПО - программное обеспечение;

РФ - Российская Федерация;

ФСБ - Федеральная служба безопасности;

ФСТЭК - Федеральная служба по техническому и экспортному контролю;

ФЗ - Федеральный Закон.

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Информационная система персональных данных - это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Несанкционированный доступ - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Для служебного пользования - это служебная информация ограниченного распространения, относящуюся к несекретной информации, касающуюся деятельности организации, ограничение на распространение которой диктуется служебной необходимостью.

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

SIEM (Security Information and Event Management) - это технология, осуществляющая контроль мониторинга информационных систем, которая анализирует события информационной безопасности в реальном времени, исходящие от сетевых устройств, средств защиты информации, ИТ-сервисов, инфраструктуры систем и приложений, а также помогают обнаруживать инциденты информационной безопасности.

# ВВЕДЕНИЕ

С развитием информационных технологий, с ростом технических возможностей по копированию и распространению информации, она подвергается воздействию различных процессов (неисправностям и сбоям оборудования, ошибкам операторов и т.д.), которые могут привести к ее разрушению, изменению, а также создать предпосылки к доступу к ней третьих лиц.

С появлением сложных автоматизированных систем, связанных с вводом, хранением, обработкой и выводом информации, проблемы ее защиты приобретают еще большее значение для организаций. Этому способствует: увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью автоматизированной информационной системы; сосредоточение в единых базах данных информации различного назначения и принадлежности; расширение круга пользователей, имеющих доступ к ресурсам информационной системы, и находящимся в ней данных.

Постоянно совершенствующееся законодательство в области защиты информации обуславливает необходимость организациям обновлять меры по защите сведений.

Актуальность данной работы обусловлена трудностью выбора и установки SIEM-системы на предприятие «ГРЦ Макеева» города Миасс.

Объектом выпускной квалификационной работы является информационная инфраструктура предприятия «ГРЦ Макеева» города Миасс.

Целью дипломной работы является обоснование ряда мер по модорнизации и повышение уровня защищенности конфиденциальной информации при ее циркуляции во внутренней сетевой инфраструктуре предприятия.

В соответствии с поставленной целью необходимо решить следующие задачи:

1) обследование объекта защиты;

2) теоретическое обоснование выбора средств защиты;

3) выбор оптимальной SIEM-системы;

4) установка и первоначальная настройка SIEM-системы;

5) осуществить расчет рисков информационной безопасности;

6) расчет затрат и обоснование экономической эффективности.