ФЕДЕРЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный университет путей сообщения»
(ФГБОУ ВО УрГУПС)

Факультет Электротехнический

Кафедра Информационные технологии и защита информации

Направление подготовки Информационная безопасность

Допускается к защите:
Заведующий кафедрой к.т.н.,
доцент Зырянова Т.Ю.
«29» 06 2016 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Тема: Сравнительный анализ систем обнаружения вторжений с открытым исходным кодом для защиты локальных вычислительных сетей
(пояснительная записка)

10.03.01.05.ВКР.ИБ.ПЗ
(шифр документа)

Разработал: Кадочников Д.Е. ИБ-412 29.06.16
(студент-дипломник) (группа) (подпись) (дата)

Руководитель: ассистент кафедры «ИТиЗИ» Гузенкова Е.А. 29.06.16
(должность, звание) (подпись) (дата)

Консультанты: Доцент кафедры ТБ Шерстюченко О.А. 27.06.16
(должность, звание) (подпись) (дата)

старший преподаватель кафедры «Экономика транспорта» Селина О.В. 27.06.16
(должность, звание) (подпись) (дата)

Н. контролер: к.т.н., заведующий кафедрой «ИТиЗИ», доцент Зырянова Т.Ю. 29.06.16
(должность, звание) (подпись) (дата)

Екатеринбург

2016

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Уральский государственный университет путей сообщения»

(ФГБОУ ВО УрГУПС)

Факультет Электротехнический Кафедра ИТиЗИ

Специальность Информационная безопасность

УТВЕРЖДАЮ:
Зав. кафедрой
(Т.Ю. Загумнова)
«06» 06 2016 г.

Задание

на ВКР студенту

Кадочникову Денису Евгеньевичу

1. Тема проекта (работы) Сравнительный анализ систем обнаружения вторжений с открытым исходным кодом для защиты локальных вычислительных сетей
утверждена приказом по университету от «06» июня 2016 г. № 771-со

2. Срок сдачи студентом законченного проекта (работы) 29.06.16

3. Исходные данные к проекту (работе) Информация о свободном программном обеспечении, Руководство пользователя Snort, Руководство пользователя Suricata

4.Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов) разработка виртуального стенда, сравнительный анализ СОВ, разработка рекомендации по использованию СОВ

5. Перечень графического материала (с точным указанием обязательных чертежей) Цель работы, поставленные задачи, мировая статистика сетевых атак, классификация СОВ, архитектура СОВ Snort, Схема виртуального стенда, расчет стоимости внедрения СОВ, эффективность антибактериальных средств, результаты работы.

6. Консультанты по проекту (работе, с указанием относящихся к ним разделов)

Раздел	Консультанты	Подпись, дата	
		Задние выдал	Задание принял
Безопасность жизнедеятельности	Доцент кафедры ТБ Шерстюченко О.А.	06.06.16	27.06.16
Экономика	Старший преподаватель кафедры «Экономика транспорта» Селина О.В.	06.06.16	27.06.16

7. Дата выдачи задания 06.06.16

Руководитель Гузенкова Е.А. _____
(подпись)

Задание принял к исполнению студент-дипломник
Кадочников Д.Е. _____
(подпись)

КАЛЕНДАРНЫЙ ПЛАН

№ п/п	Наименование этапов дипломного проекта (работы)	Срок выполнения этапов проекта (работы)	Примечание
1	Сбор материала	23.05.2016-30.05.2016	
2	Написание теоретической части	30.05.2016-05.06.2016	
3	Написание практической части	06.06.2016-15.06.2016	
4	Написание раздела БЖД	15.06.2016-18.06.2016	
5	Написание раздела Экономики	18.06.2016-21.06.2016	
6	Оформление работы	21.06.2016-25.06.2016	
7	Корректировочные работы	25.06.2016-29.06.2016	

Студент-дипломник Кадочников Д.Е. _____
(подпись)

Руководитель Гузенкова Е.А. _____
(подпись)

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный университет путей сообщения»
(ФГБОУ ВО УрГУПС)

УТВЕРЖДАЮ:
Зав. кафедрой
_____ (Т.Ю. Зорина)
«06» 06 2016 г.

Задание
на специальный раздел ВКР

Студент Кадочников Денис Евгеньевич **Группа** ИБ-412
(Фамилия, Имя, Отчество)
Экономика
(наименование специального раздела)
1. Тема Сравнительный анализ систем обнаружения вторжений с открытым исходным кодом для защиты локальных вычислительных сетей
(название темы ВКР)
Утверждена приказом по университету от «06» июня 2016 г. № 771-со
Выпускающая кафедра Информационные технологии и защита информации
Руководитель проекта Гузенкова Е.А., ассистент кафедры «ИТиЗИ»
(Фамилия, инициалы, должность или ученое звание, ученая степень)
2. Консультант раздела Селина О.В., старший преподаватель
(Фамилия, инициалы, должность)
Кафедра, ведущая специальный раздел Экономика транспорта
3. Исходные данные Системы обнаружения вторжений с открытым исходным кодом
4. Срок сдачи студентом законченного раздела 29.06.16
5. Содержание специального раздела (перечень подлежащих разработке вопросов)
Расчет стоимости внедрения проекта
6. Название демонстрационно-графического(их) материала(ов)
Расчет стоимости внедрения СОВ
7. Дата выдачи задания 06.06.16 Консультант _____
(подпись)

Согласовано: 06.06.16 _____
(дата и подпись руководителя ВКР)
Принято к исполнению 06.06.16 _____
(дата и подпись студента-дипломника)

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный университет путей сообщения»
(ФГБОУ ВО УрГУПС)

УТВЕРЖДАЮ:
Зав. кафедрой
_____ (Т.Ю. Зырянова)
«06» 06 2016 г.

Задание
на специальный раздел ВКР

Студент Кадочников Денис Евгеньевич **Группа** ИБ-412
(Фамилия, Имя, Отчество)
Безопасность жизнедеятельности
(наименование специального раздела)
1. Тема Сравнительный анализ систем обнаружения вторжений с открытым исходным кодом для защиты локальных вычислительных сетей
(название темы ВКР)
Утверждена приказом по университету от «06» июня 2016 г. № 771-со
Выпускающая кафедра Информационные технологии и защита информации
Руководитель проекта Гузенкова Е.А., ассистент кафедры «ИТиЗИ»
(Фамилия, инициалы, должность или ученое звание, ученая степень)
2. Консультант раздела Шерстюченко О.А., доцент кафедры ТБ
(Фамилия, инициалы, должность)
Кафедра, ведущая специальный раздел Техносферная безопасность
3. Исходные данные Болехан В.Н. Обеспечение микробиологической безопасности при эксплуатации персональных компьютеров на железнодорожном транспорте
4. Срок сдачи студентом законченного раздела 28.06.16
5. Содержание специального раздела (перечень подлежащих разработке вопросов)
Экспертиза условий труда, нормативные величины, Обеспечение микробиологической безопасности при эксплуатации персональных компьютеров
6. Название демонстрационно-графического(их) материала(ов)
Эффективность антибактериальных средств
7. Дата выдачи задания 06.06.16 Консультант _____
(подпись)

Согласовано: 06.06.16 _____
(дата и подпись руководителя ВКР)

Принято к исполнению 06.06.16 _____
(дата и подпись студента-дипломника)

СОДЕРЖАНИЕ

РЕФЕРАТ

Выпускная квалификационная работа содержит: с. 70, рис. 9, табл. 12, использованных источников 25 названий.

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ, СЕТЕВЫЕ АТАКИ, ЗАЩИТА ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ, ТЕСТИРОВАНИЕ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ, ВИРТУАЛЬНЫЙ СТЕНД

Цель работы – разработка виртуального стенда для тестирования и последующего сравнительного анализа эффективности систем обнаружения вторжений.

Для достижения цели работы произведен анализ систем обнаружения вторжения, а также связанных с ними понятий.

Результатом выпускной квалификационной работы является виртуальный стенд для тестирования систем обнаружения вторжений.

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Уральский Государственный Университет Путей Сообщения»
(ФГБОУ ВО УрГУПС)

ОТЗЫВ

о выпускной квалификационной работе студента факультета *Электротехнического*
(Наименование)

Направления подготовки (специальности) *10.03.01 «Информационная безопасность»*
(Код, наименование)

Кадочникова Дениса Евгеньевича
(Фамилия, имя, отчество)

Руководитель *ассистент кафедры ИТ и ЗИ Гузенкова Е.А.*
(Ученая степень, ученое звание, должность, Фамилия, имя, отчество)

Целью данной выпускной квалификационной работы является сравнительный анализ систем обнаружения вторжений с открытым исходным кодом.

Данная тема является актуальной, так как стремительно увеличивается число инцидентов в области информационной безопасности, а значит и возрастает необходимость в комплексных системах защиты информации. Системы обнаружения вторжений стали необходимым компонентом инфраструктуры безопасности организаций и служат механизмами мониторинга подозрительной активности.

В ходе работы были рассмотрены основные сведения и понятия, связанные с СОВ. Приведена мировая статистика реализованных сетевых атак за последние три года. Рассмотрены сравниваемые системы обнаружения вторжений с открытым исходным кодом. Проведен сравнительный анализ эффективности выбранных систем обнаружения вторжений с помощью разработанного виртуального стенда.

В результате работы был разработан виртуальный стенд для тестирования СОВ.

Структура работы логична, материал излагается последовательно. Тема выпускной работы раскрыта надлежащим образом. Задание на ВКР выполнено полностью, с учетом особенностей и специфики собранного материала. Выпускная квалификационная работа выполнена в соответствии с требованиями к оформлению.

Студент проявил высокую мотивацию в написании выпускной квалификационной работы. Считаю, что выпускная квалификационная работа Кадочникова Д.Е. рекомендуется к защите и заслуживает оценки «отлично».

Гузенкова Е.А.