

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»**

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой,

к.т.н., доцент

_____ А.Н. Соколов

_____ 2020 г.

**Экспериментальный лабораторный стенд «Аудит
информационной безопасности»**

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.03.01.2020.158.ПЗ ВКР

Руководитель проекта,
нач. отд. АНО «Центр экспертиз
и научно-технических
исследований»

_____ В.С. Лужнов

_____ 2020 г.

Автор проекта,
студент группы КЭ-407

_____ В.С. Попов

_____ 2020 г.

Нормоконтролер,
к.т.н., доцент

_____ В.П. Мартынов

_____ 2020 г.

АННОТАЦИЯ

Попов В.С. Разработка экспериментального стенда для проведения лабораторных работ по дисциплине «Аудит информационной безопасности» – Челябинск: ЮУрГУ, КЭ-407, 154 с., 53 ил., 4 табл., библиогр. список – 44 наим., 7 прил.

Выпускная квалификационная работа выполнена с целью разработки стенда «Аудит информационной безопасности».

В выпускной квалификационной работе отражены все этапы создания стенда «Аудит информационной безопасности».

Выпускная квалификационная работа состоит из трех глав. В процессе выполнения ВКР был проведен анализ существующих решений изучения аудита информационной безопасности, были предложены варианты реализации лабораторного стенда и выбран самый оптимальный. В проектной части работы были разработаны лабораторные работы, состоящие из практических и принципиальных частей, реализованных в приложениях.

					ЮУрГУ – 10.03.01.2020.158.ПЗ ВКР			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.		Попов			Экспериментальный лабораторный стенд «Аудит информационной безопасности»	Лит.	Лист	Листов
Пров.		Лужнов					5	154
Реценз.						ЮУрГУ Кафедра ЗИ		
Н. Контр.		Мартынов						
Утв.		Соколов						

ОГЛАВЛЕНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ	7
ВВЕДЕНИЕ.....	9
1 ПОНЯТИЕ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	10
1.1 Определение аудита информационной безопасности.....	11
1.2 Цели и задачи аудита.....	12
1.3 Этапы проведения аудита.....	13
1.4 Концептуальные основы аудита.....	14
1.5 Классификация мероприятий аудита.....	23
1.6 Тестирование как один из основных типов аудита	29
2 АНАЛИЗ СРЕДСТВ И МЕТОДОВ АУДИТА ИБ.....	39
2.1 Классификация средств проведения аудита ИБ	39
2.3 Методология аудита ИБ в национальных и отраслевых стандартах.....	45
2.4 Поиск информации по уязвимостям компьютерных систем	48
3 РАЗРАБОТКА УЧЕБНО-МЕТОДИЧЕСКОГО СТРЕНДА «АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»	53
3.1 Лабораторная работа 1. Построить модель компьютерной сети.	55
3.2 Лабораторная работа №2. Обнаружение сетевых узлов.....	57
3.3. Лабораторная работа №3. Сканирование портов и идентификация ОС..	61
3.4. Лабораторная работа №4. Использование DNS для обнаружения и выяснения назначения сетевых узлов.....	61
3.5 Лабораторная работа 5. Создание карт сети	63
3.6 Лабораторная работа 6. Использование сканера безопасности Nessus.....	64
3.7 Лабораторная работа 7. Анализ защищенности web-серверов	68
3.8 Лабораторная работа 8. Этап внутреннего аудита	75
3.9 Лабораторная работа 9. Поиск уязвимостей web-приложений.....	82
ЗАКЛЮЧЕНИЕ	115
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	116
ПРИЛОЖЕНИЕ А	121
ПРИЛОЖЕНИЕ Б.....	122
ПРИЛОЖЕНИЕ В	127
ПРИЛОЖЕНИЕ Г.....	133
ПРИЛОЖЕНИЕ Д.....	136
ПРИЛОЖЕНИЕ Е	137
ПРИЛОЖЕНИЕ Ж	147

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ACK – Acknowledgement field significant
AD – Active Directory
AH – Authentication Header
ARP – Address Resolution Protocol
CDP – Cisco Discovery Protocol
CIFS – Common Internet File System
CVE – Common Vulnerabilities and Exposures
CVSS – Common Vulnerability Scoping System
ESP – Encapsulating Security Payload
FTP – File Transfer Protocol
GRE – Generic Routing Encapsulation
HTTP – Hypertext Transfer Protocol
ICMP – Internet Control Message Protocol
IIS – Internet Information Services
IKE – Internet Key Exchange
IP – Internet Protocol
ISO – International Standard Organization
L2F – Layer-2 Forwarding
L2TP – Layer-2 Tunneling Protocol
LDAP – Lightweight Directory Access Protocol
MAC – Medium Access Control
MSCHAP – Microsoft Challenge Handshake Authentication Protocol
MSTS – Microsoft Terminal Services
NAT – Network Address Translation
NSS – Name Service Switch
NTP – Nessus Transport Protocol
PAM – Pluggable Authentication Modules
POP3 – Post Office Protocol
PPP – Point-to-Point Protocol

PPTP – Point-to-Point Tunneling Protocol
RDP – Remote Desktop Protocol
RFC – Request For Comments
RST – Reset the connection
S/MIME – Secure Multipurpose Internet Mail Extension
SHTTP – Secure HTTP
SKIP – Simple Key management for Internet Protocol
SMB – Server Message Blocks
SMTP – Simple Mail Transfer Protocol
SOA – Start of Authority
SSL – Secure Socket Layer
SYN – Synchronize sequence numbers
TCP – Transmission Control Protocol
TLS – Transport Layer Security
UDP – User Datagram Protocol
VPN – Virtual Private Network
АИС – Автоматизированная информационная система
ИБ – Информационная безопасность
ИП – Инструментальные проверки
МЭ – Межсетевой экран
ОС – Операционная система
ПИБ – Подсистема информационной безопасности
ПК – Персональный компьютер
ПО – Программное обеспечение
СЗИ – Средство защиты информации
СОА – Система обнаружения атак
СОИБ – Система обеспечения информационной безопасности
ЦС – Центр сертификации
ЭЦП – Электронно-цифровая подпись

ВВЕДЕНИЕ

Целью работы является разработка экспериментального стенда для проведения лабораторных работ по дисциплине «Аудит информационной безопасности», так как в ходе выполнения лабораторных работ будут получены навыки и знания, которые на сегодняшний день актуальны в сфере информационной безопасности.

Лабораторный стенд по курсу «Аудит информационной безопасности» предназначен для студентов укрупненной группы направлений и специальностей «Информационная безопасность» уровней бакалавриат и специалитет. В лабораторных работах рассмотрены способы оценки текущего состояния системы информационной безопасности, устанавливающей уровень ее соответствия определенным критериям, и предоставление результатов в виде рекомендаций. Аудит ИБ позволяет получить наиболее полную и объективную оценку защищенности информационной системы (ИС), локализовать имеющиеся проблемы и разработать эффективную программу построения системы обеспечения ИБ организации. В рамках аудита ИБ или отдельным проектом может быть проведено тестирование на проникновение, позволяющее проверить способность информационной системы противостоять попыткам проникновения в сеть и неправомерного воздействия на информацию. Определены закономерности создания защищённых информационных систем, раскрыты принципы обеспечения информационной безопасности государства, уделено внимание информационным войнам и информационному противоборству. Дан краткий анализ моделей и политики безопасности (разграничения доступа), а также международных стандартов в области информационной безопасности. Стенд может использоваться студентами других специальностей при изучении курсов, связанных с защитой информации.

Актуальность обосновывается высокой потребностью в свежих лабораторных работах из-за выхода новых стандартов защиты информации (таких как ГОСТ Р ИСО/МЭК 15408-2-2013, ГОСТ Р ИСО/МЭК 15408-3-2013, ГОСТ Р ИСО/МЭК 15408 и прочих стандартов касающиеся аудита информационной безопасности)