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.

Челябинск 2020

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.

ОГЛАВЛЕНИЕ

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» предназначено 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 неправомочного 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)