ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

TÔ QUANG HIỆP

NGHIÊN CỨU VẤN ĐỀ BẢO MẬT THÔNG TIN VÀ ĐỀ XUẤT GIẢI PHÁP BẢO MẬT CHO HỆ THỐNG THÔNG TIN TRƯỜNG CAO ĐẲNG KINH TẾ - KỸ THUẬT VĨNH PHÚC

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - 2014

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

TÔ QUANG HIỆP

NGHIÊN CỨU VẤN ĐỀ BẢO MẬT THÔNG TIN VÀ ĐỀ XUẤT GIẢI PHÁP BẢO MẬT CHO HỆ THỐNG THÔNG TIN TRƯỜNG CAO ĐẲNG KINH TẾ - KỸ THUẬT VĨNH PHÚC

Chuyên ngành: **KHOA HỌC MÁY TÍNH**
Mã số: **60 48 01**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Người hướng dẫn khoa học: TS. PHÙNG VĂN ỔN

THÁI NGUYÊN - 2014

LỜI CÁM ƠN

Em xin chân thành cảm ơn sự chỉ bảo tận tình của TS Phùng Văn Ổn, người đã tận tình hướng dẫn, giúp đỡ em trong suốt thời gian thực hiện luận văn.

Em xin chân thành cảm ơn PGS. TSKH Nguyễn Xuân Huy – người đã tận tình giảng dạy hướng dẫn, hướng dẫn học phần "An toàn và bảo mật thông tin", "phương pháp nghiên cứu khoa học" là nguồn kiến thức chính cho luận văn này.

Em xin chân thành cảm ơn thầy, cô Viện Công nghệ thông tin cùng quý thầy, cô Trường Đại học Công nghệ thông tin và truyền thông – Đại học Thái Nguyên đã giảng dạy, giúp đỡ để chúng em có được những kiến thức quý báu trong những năm học qua.

Tôi xin chân thành cảm ơn các bạn đồng nghiệp Khoa Công nghệ thông tin – Trường Cao đẳng Kinh tế - Kỹ thuật Vĩnh Phúc đã cung cấp số liệu hiện trạng hệ thống thông tin nhà trường và cùng tôi tìm hiểu hiện trạng bảo mật hệ thống thông tin của nhà trường, đưa ra giải pháp khắc phục các nguy cơ bảo mật.

Con cảm ơn Cha, Mẹ và gia đình, những người đã dạy dỗ, khuyến khích, động viên con trong những lúc khó khăn, tạo mọi điều kiện cho chúng con nghiên cứu học tập.

Mặc dù đã cố gắng hết sức cùng với sự tận tâm của thầy giáo hướng dẫn song do trình độ còn hạn chế, nội dung đề tài rộng, mới nên Luận văn khó tránh khỏi những thiếu sót và hạn chế. Do vậy em rất mong nhận được sự thông cảm và góp ý kiến của thầy cô và các bạn.

Thái Nguyên, tháng 01/2014

HỌC VIÊN

Tô Quang Hiệp

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn "***Nghiên cứu vấn đề bảo mật thông tin và đề xuất giải pháp bảo mật cho hệ thống thông tin Trường Cao đẳng Kinh tế - Kỹ thuật Vĩnh Phúc***" này là kết quả nghiên cứu của riêng tôi. Các số liệu sử dụng trong luận văn là trung thực. Các kết quả nghiên cứu được trình bày trong luận văn chưa từng được công bố tại bất kỳ công trình nào khác.

Thái Nguyên, tháng 01/2014

HỌC VIÊN

Tô Quang Hiệp

MỤC LỤC

Trang

DANH MỤC CÁC KÝ HIỆU, CHỮ CÁI VIẾT TẮT

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
BCB	Cipher Block Chaining
BSD	Berkeley Software Distribution
CFB	Cipher Feedback Mode
CPU	Central Processing Unit
CTR	Counter mode
DES	Data Encryption Standard
DNS	Domain Name System
DOS	Disk Operating System
ECB	Electronic code book
FEAL	Fast Encryption Algorithm
FTP	File Transfer Protocol
GNFS	General Number Field Sieve ().
HAS	Human Auditory System
ICMP	Internetwork Control Message Protocol
IDEA	International Data Encryption Algorithm)
IP	Internet Protocol
ISA	Internet Security Accelerator
LAN	Local Area Network
MIPS	Million instructions per second
NIST	National Institute of Standards and Technology
NNTP	Network News Transfer Protocol
NSA	National Security Agency
NTFS	New Technology File System
OFB	Output Feedback Mode
PKCS	Public Key Cryptography Standards
RSA	Revised Statutes Annotated
SMTP	Simple Mail Transfer Protocol
TCP/UDP	Transmission control protocol/ User Datagram Protocol

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

MỞ ĐẦU

Với sự phát triển nhanh của công nghệ thông tin, hiện nay đa số dữ liệu được số hóa và lưu trữ trong máy tính đã tạo nên sự thuận tiện cho con người. Sự phát triển của mạng máy tính đã giúp con người khai thác thông tin một cách dễ dàng nhưng bên cạnh đó cũng này sinh vấn đề rất quan trọng về việc bảo về các thông tin riêng của cá nhân hay của tập thể. Thông tin riêng (cá nhân) có thể là mật khẩu đăng nhập vào hệ thống, chiến lược kinh doanh, các phát minh sáng chế chưa được công bố, kế hoạch quân sự … thông tin này rất quan trọng, nếu bị lộ có thể sẽ ảnh hưởng lớn đến cá nhân, tổ chức, hệ thống về mọi mặt như kinh tế, chính trị, thời gian, con người …

Khi có được thông tin đăng nhập hệ thống thông tin thì có thể sẽ có nhiều quyền với hệ thống đó. Khi đó các thông tin trên hệ thống có thể bị sửa đổi, chuyển cho người khác, thậm chí còn có thể bị phá cả hệ thống. Như vậy đi liền với phát triển hệ thống thông tin thì bảo vệ hệ thống thông tin cũng là vấn đề quan trọng. Để một hệ thống thông tin hoạt động chính xác, tin cậy, an toàn đáp ứng được nhu cầu của cá nhân, tập thể thì cần thiết phải áp dụng biện pháp, chính sách bảo mật. Bảo mật thông tin là các phương thức nhằm bảo vệ tính bí mật của thông tin. Phương pháp chủ yếu là biến đổi thông tin để người khác không thể đọc, không thể hiểu được. Chỉ người có thẩm quyền mới có thể biến đổi ngược lại để đọc được nội dung của thông tin đó.

Từ xưa con người đã có nhiều cách biến đổi thông tin nhằm đảm bảo tính bí mật khi gửi đi như thay thế bằng các biểu tượng, ký hiệu, viết ngược, viết vào gỗ sau đó phủ sáp lên, viết vào dây quấn quanh gậy, dùng hóa chất để viết khi hơ nóng sẽ hiện chữ ... Nếu một người có được thông tin biến đổi và biết được phương pháp biến đổi thông tin thì dễ dàng biết cách để đọc được thông tin. Vậy để giữ bí mật thông tin cần phải giữ bí mật cả phương pháp biến đổi thông tin.