MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef departament:
FIODOROV Ion dr., conf.univ.

„___" _____ 2024

MODELE DE SECURITATE APLICATE PENTRU INTERPRINDERI MICI SI MIJLOCII

Proiect de master

Student: _____ **Bucari Eduard, TIA-221M**

Coordonator: _____ **Turcanu Dinu, conf. univ., dr.**

Consultant: _____ **Cojocaru Svetlana, asist.univ.**

Chişinău, 2024

REZUMAT

Proiectul de diplomă are 44 de pagini și reprezintă un studiu amplu care vizează îmbunătățirea securității cibernetice pentru întreprinderile mici și mijlocii și organizarea proceselor de afaceri continue pe exemplul întreprinderii "Rezonanta S.A.". Obiectivul principal al lucrării este de a studia în detaliu abordările teoretice și metodologice ale organizării securității informaționale și de a elabora recomandări specifice pentru optimizarea proceselor-cheie, ceea ce contribuie la îmbunătățirea sistemului de management la întreprinderea selectată.

Lucrarea acoperă o gamă largă de modele de securitate informatică și cibernetică, de la fundamente teoretice la exemple practice de aplicare a acestora.

Primul capitol al lucrării prezintă principalele aspecte teoretice și metodologice ale organizării IMM-urilor și trece în revistă standardul de securitate a informațiilor ISO/IEC 27001.

Al doilea capitol include o defalcare a principalelor modele, precum și studiul principiilor și abordărilor moderne de securitate cibernetică.

Al treilea capitol conține partea analitică a lucrării, în care sunt studiate și descrise principiile de apărare, amenințările web și tehnologiile de protecție a informațiilor.

Cel de-al patrulea capitol examinează amenințările moderne la adresa securității informațiilor și metodele de apărare împotriva acestor amenințări.

Al cincilea capitol include o prezentare generală a sistemului de operare Linux și a aplicării acestui sistem pentru testarea penetrării.

Capitolul șase analizează aplicarea inteligenței artificiale în domeniul securității cibernetice. Concluzia acestui proiect oferă sugestii pentru îmbunătățirea securității cibernetice și a eficienței pentru întreprinderile mici și mijlocii.

Lista surselor utilizate totalizează 13 titluri, ceea ce indică o abordare profundă și cuprinzătoare a subiectului studiat.

ABSTRACT

The diploma project is written on 44 pages and is a comprehensive study aimed at improving cybersecurity for small and medium-sized businesses and the organization of continuous business processes on the example of the enterprise "Rezonanta S.A.". The main purpose of the work is to study in detail the theoretical and methodological approaches to the organization of information security and to develop specific recommendations to optimize key processes, which contributes to the improvement of the management system at the selected enterprise.

The work covers a wide range of information and cyber security models, ranging from theoretical foundations to practical examples of their application.

The first chapter of the paper presents the main theoretical and methodological aspects of the SME organization and reviews the information security standard ISO/IEC 27001.

The second chapter includes the analysis of the main models, as well as the study of modern cybersecurity principles and approaches.

The third chapter contains the analytical part of the work, in which there is a study and description of the principles of protection, web threats and information protection technologies.

The fourth chapter reviews modern threats to information security and methods of defense against these threats.

The fifth chapter includes a review of the Linux operating system and the use of this system for penetration testing.

Chapter six discusses the application of artificial intelligence in cybersecurity.

The conclusion of this project provides suggestions for improving cybersecurity and efficiency for small and medium-sized businesses.

The list of sources used includes 13 titles, which indicates an in-depth and comprehensive approach to the topic under study.

АННОТАЦИЯ

Дипломный проект написан на 44 страницах и представляет собой комплексное исследование, направленное на усовершенствование кибербезопасности для предприятий малого и среднего бизнеса и организации непрерывных бизнес-процессов на примере предприятия "Rezonanta S.A.". Основная цель работы заключается в детальном изучении теоретических и методических подходов к организации информационной безопасности и разработке конкретных рекомендаций для оптимизации ключевых процессов, что способствует улучшению системы управления на выбранном предприятии.

Работа охватывает широкий спектр моделей информационной и кибер безопасности, начиная от теоретических основ и заканчивая практическими примерами их применения.

В первом главе документа представлены основные теоретические и методические аспекты организации малого и среднего бизнеса, а также рассмотрен стандарт информационной безопасности ISO/IEC 27001.

Вторая глава включает разбор основных моделей, а также изучение современных принципов и подходов кибербезопасности.

Третья глава содержит аналитическую часть работы, в которой происходит изучение и описание принципов защиты, веб угроз и технологий защиты информации.

В четвертой главе рассмотрены современные угрозы информационной безопасности и методы защиты от данных угроз.

Пятая глава включает обзор операционной системы Linux и применение данной системы для тестирования на проникновение.

В шестой главе рассматривается применение искусственного интелекта в кибербезопасности.

В заключении данного проекта представлены предложения для повышения кибербезопасности и эффективности для предприятий малого и среднего бизнеса.

Список использованных источников насчитывает 13 наименований, что свидетельствует о глубоком и всестороннем подходе к изучаемой теме.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном мире корпоративные данные, являются одним из основных активов любой компании. Обеспечение информационной безопасности стало приоритетным и необходимым условием для нормального функционирования компаний разного уровня. Защита корпоративных данных уже сегодня, становится основным условием для надежной и стабильной работы бизнеса. В этой работе я рассмотрю основные инструменты и средства для обеспечения безопасности корпоративных информационных систем.

Принимая во внимание основные цели данной работы, важно отметить, что защита корпоративных данных особенно актуалена для предприятий как с простой, так и со сложной разветвленной структурой, важно отметить что к подобным организациям малого, среднего и крупного бизнеса относятся не только предприятия сетевой торговли, производственные комплексы и банки. Важно отметить, что масштабы организации не имеют значения. Под угрозой оказываются компании любого уровня.

Сейчас большая часть бизнес-процессов происходят с помощью глобальной сети. Для каждой организации важно наличие продуманной грамотной стратегии обеспечения безопасности, способной предотвратить утечку конфиденциальных сведений и финансовой информации.

Безусловно, сегодня корпоративные данные – это один из самых ценных активов любой компании. Они включают в себя финансовые отчеты, конфиденциальную информацию, персональные данные сотрудников и клиентов, коммерческие тайны и многое другое. Несанкционированный доступ к этим данным может привести к серьезным последствиям, включая утечки информации, финансовые потери, утрату доверия клиентов и нарушение законодательства. Поэтому защита корпоративных данных – это один из основных приоритетов любой компании.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

[1] Стандарт управления информационной безопасностью ISO/IEC 27001.
[Электронный вариант] доступно на: https://www.iso.org/ru/standard/27001

[2] “The Practice of Network Security Monitoring: Understanding Incident Detection and Response”
By Richard Bejtlich (Author), No Starch Press, Inc. 2013.
38 Ringold Street, San Francisco, CA 94103

[3] “Defensive Security Handbook: Best Practices for Securing Infrastructure”.
By Lee Brotherston (Author), Amanda Berlin (Author).
Released April 2017, Publisher(s): O'Reilly Media, Inc.

[4] “Industrial Cybersecurity: Efficiently secure critical infrastructure systems “
by Pascal Ackerman (Author).
Publishe: Packt Publishing, Publication Date: October 18, 2017

[5] “Zero Trust Networks: Building Secure Systems in Untrusted Networks”
by Evan Gilman (Author), Doug Barth (Author).
Publisher: O'Reilly Media, Edition 1, Publication Date: July 25, 2017

[6] “The Social Engineer's Playbook: A Practical Guide to Pretexting”.
By Jeremiah Talamantes (Author). Publisher: Hexcode Publishing; 1 edition (23 Nov. 2014)

[7] “Penetration Testing: A Hands-On Introduction to Hacking”.
by Georgia Weidman (Author).
Publisher: No Starch Press, Edition 1, Publication Date: June 14, 2014

[8] “Mastering Kali Linux for Advanced Penetration Testing”
by Robert W. Beggs (Author), Publisher: Packt Pub Ltd, Publication Date: June 24, 2014

[9] “Basic Security Testing With Kali Linux, Third Edition”
by Daniel W Dieterle (Author), Publisher: Packt Pub Ltd, Publication Date: August 22, 2018

[10] “Computer security model A Complete Guide”
by Gerardus Blokdyk (Author) Publication Date: February 24, 2022

[11] “A Guide to Understanding Security Modeling in Trusted Systems”
National Computer Security Center (U.S.), Publisher: DIANE Publishing, 1993

[12] “Small and Medium Enterprisess: Concepts, Methodoligies, Tools, and Applications”
Information Resources Management Association USA
Managing Director: Lindsay Johnston
Published by Busisness Science Reference 2013.

[13] “ИИ-2041. Десять образов нашего будущего”
Автор: Ли Кай-Фу, Чэнь Цюфань. Китай. Перевод:Москва, Манн, Иванов и Фербер, 2019.