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.

„___” _____ 2023

Analiza comparativă a modelelor de securitate informațională pe categorii de bineficiari

Proiect de master

Studenta: **Matrohina Ecaterina, TIA-211M**

Conducător: **Peca Ludmila, lector universitar**

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

Chişinău, 2023

ABSTRACT

Securitatea informațiilor este crucială pentru organizațiile de toate tipurile, în special pentru întreprinderile mici și mijlocii. Importanța securității informațiilor poate fi explicată prin triada securității informațiilor, care cuprinde confidențialitate, integritate și disponibilitate. Confidențialitatea se referă la protecția informațiilor împotriva dezvăluirii neautorizate, integritatea la protecția informațiilor împotriva modificărilor neautorizate și disponibilitatea pentru asigurarea că informațiile sunt disponibile atunci când este necesar.

Pentru a implementa măsuri de securitate a informațiilor, două cadre utilizate în mod obișnuit sunt NIST 800-53 și CIS Controls. NIST 800-53 este un cadru cuprinzător care acoperă întregul spectru al securității cibernetice și este extrem de personalizabil. Acesta oferă îndrumări detaliate și este adesea folosit ca bază de conformitate pentru organizațiile care manipulează informații sensibile. Pe de altă parte, CIS Controls este un set de 20 de controale concepute pentru a proteja împotriva amenințărilor cibernetice comune. Se concentrează pe cele mai importante domenii de securitate și simplifică implementarea pentru organizațiile cu cunoștințe limitate în domeniul securității cibernetice. Deși nu oferă îndrumări detaliate pentru monitorizarea continuă, poate ajuta organizațiile să îndeplinească cerințele de conformitate.

Ambele cadre necesită monitorizare constantă și evaluare a riscurilor pentru a fi la curent cu cele mai recente amenințări cibernetice. IMM-urile din Moldova pot beneficia de utilizarea acestor cadre pentru a dezvolta un cadru de securitate personalizat care prioritizează cele mai importante controale în funcție de nivelul de risc pe care îl atenuează și de fezabilitatea lor pentru implementare. Acest lucru poate ajuta IMM-urile să reducă riscul atacurilor cibernetice și să își protejeze informațiile sensibile. În plus, implementarea acestor cadre poate ajuta IMM-urile să îndeplinească cerințele de reglementare și de conformitate, ceea ce le poate ajuta să evite sancțiunile și daunele reputației.

КРАТКОЕ СОДЕРЖАНИЕ

Информационная безопасность имеет решающее значение для организаций всех типов, особенно для малых и средних предприятий (МСП). Важность информационной безопасности можно объяснить триадой информационной безопасности, которая включает конфиденциальность, целостность и доступность. Конфиденциальность относится к защите информации от несанкционированного раскрытия, целостность — к защите информации от несанкционированного изменения, а доступность — к гарантии того, что информация будет доступна, когда это необходимо.

Для реализации мер информационной безопасности обычно используются две структуры: NIST 800-53 и CIS Controls. NIST 800-53 — это всеобъемлющая структура, охватывающая весь спектр кибербезопасности и обладающая широкими возможностями настройки. Он содержит подробное руководство и часто используется в качестве основы соответствия для организаций, работающих с конфиденциальной информацией. С другой стороны, CIS Controls представляет собой набор из 20 элементов управления, предназначенных для защиты от распространенных киберугроз. Он фокусируется на наиболее важных областях безопасности и упрощает внедрение для организаций с ограниченными знаниями в области кибербезопасности. Хотя он не содержит подробных рекомендаций по непрерывному мониторингу, он может помочь организациям выполнить требования соответствия.

Обе платформы требуют постоянного мониторинга и оценки рисков, чтобы быть в курсе последних киберугроз. МСП в Молдове могут извлечь выгоду из использования этих рамок для разработки индивидуальной системы безопасности, в которой приоритет отдается наиболее важным средствам контроля на основе уровня риска, который они снижают, и возможности их реализации. Это может помочь МСП снизить риск кибератак и защитить свою конфиденциальную информацию. Кроме того, внедрение этих рамок может помочь МСП соблюдать нормативные требования, что может помочь им избежать штрафов и репутационного ущерба.

ABSTRACT

Information security is crucial for organizations of all types, especially small and medium-sized enterprises (SMEs). The importance of information security can be explained by the information security triad, which comprises confidentiality, integrity, and availability. Confidentiality refers to the protection of information from unauthorized disclosure, integrity to the protection of information from unauthorized modification, and availability to the assurance that information is available when needed.

To implement information security measures, two commonly used frameworks are NIST 800-53 and CIS Controls. NIST 800-53 is a comprehensive framework that covers the full spectrum of cybersecurity and is highly customizable. It provides detailed guidance and is often used as a compliance basis for organizations handling sensitive information. On the other hand, CIS Controls is a set of 20 controls designed to protect against common cyber threats. It focuses on the most important security areas and simplifies implementation for organizations with limited cybersecurity knowledge. While it does not provide detailed guidance for continuous monitoring, it can help organizations meet compliance requirements.

Both frameworks require constant monitoring and risk assessment to stay up to date with the latest cyber threats. SMEs in Moldova can benefit from using these frameworks to develop a customized security framework that prioritizes the most important controls based on the level of risk they mitigate and their feasibility for implementation. This can help SMEs reduce the risk of cyber attacks and protect their sensitive information. Furthermore, the implementation of these frameworks can help SMEs meet regulatory and compliance requirements, which can help them avoid penalties and reputational damage.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ.....9

ВВЕДЕНИЕ.....10

1 ОБЩЕПРИНЯТАЯ КЛАССИФИКАЦИЯ ПРЕДПРИЯТИЙ В ЗАВИСИМОСТИ ОТ РАЗМЕРА.....11

1.1 Определение предприятия.....11

1.2 Классификация предприятий в зависимости от размера.....11

2 КАТЕГОРИИ ПРЕДПРИЯТИЙ ПО МЕТОДОЛОГИИ NIS и NIS2.....13

2.1 Определение Директивы NIS 13

2.2 Определение операторов основных услуг (OES).....13

2.3 Цели и принципы директивы NIS.....14

2.4 Определение Директивы NIS2 16

2.5 Сравнение NIS и NIS2.....18

3 МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В NIST 800-53 И NIST 800-53B.....21

3.1 Определение стандарта соответствия требованиям безопасности NIST 800-53.....21

3.2 Цель стандарта соответствия требованиям безопасности NIST 800-53…….....21

3.3 Преимущества стандарта соответствия требованиям безопасности NIST 800-53.....22

3.4 Какие данные защищает NIST SP 800-53 и Семейства контроля безопасности NIST 800-53.....22

4 МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В CIS CONTROLS.....25

4.1 Определение методологии CIS Controls.....25

4.2 Группы реализации (IG) CIS Controls.....26

4.3 Базовые контроли 1-6.....30

4.4 Основные контроли 7-16…….....33

4.5 Организационные контроли 17-20…….....37

5 АНАЛИЗ ТЕКУЩЕГО ПОЛОЖЕНИЯ РАЗНЫХ КАТЕГОРИЙ БЕНЕФИЦИАРОВ В РЕСПУБЛИКИ МОЛДОВА.....40

5.1 Законодательство Республики Молдова об информационной безопасности.....40

5.2 Типы предприятий в Республики Молдова.....41

5.3 Статистика компаний по размеру в Республики Молдова.....42

6 ВНЕДРЕНИЕ РАЗЛИЧНЫХ МОДЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ МСП В РЕСПУБЛИКИ МОЛОДВА.....43

6.1 Описание категорий компаний в Молдове по директиве NIS2.....43

6.2 Внедрение NIST 800-53 для МСП в Молдове.....44

6.3 Внедрение CIS Controls для МСП в Молдове.....45

6.4 Сравнительный анализ NIST 800-53 и CIS Controls для малого и среднего бизнеса.....47

7 РАЗРАБОТКА НОВОЙ МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ МСП В РЕСПУБЛИКИ МОЛОДВА.....50

7.1 Текущая ситуация с информационной безопасностью МСП в Молдове.....51

7.2 Определение соответствующих стандартов безопасности для МСП в Молдове.....52

7.3 Разработка индивидуальной системы безопасности для МСП в Молдове.....54

7.4 Приоритизация контроля безопасности.....55

7.5 Внедрение структуры безопасности.....57

7.6 Мониторинг и проверка системы безопасности.....58

ВЫВОДЫ.....60

БИБЛИОГРАФИЯ.....61

СОКРАЩЕНИЯ

1. NIS – The Network and Information Security
2. OES – Operators of Essential Services
3. DSP – Digital Service Providers
4. CIS – Centre for Internet Security
5. NIST – National Institute of Standards and Technology
6. IG – Implementation Group
7. МСП – Малый-средний бизнес
8. CAF – Cyber Assessment Framework
9. NCSC – National Cyber Security Centre
10. EE – Essentials Entities
11. IE – Important Entities
12. FIPS – Federal Information Processing Standards
13. AES – Advanced Encryption Standard
14. FISMA – Federal Information Security Modernization Act
15. SP – Special Publication
16. HIPAA – The Health Insurance Portability and Accountability Act
17. DFARS – Defence Federal Acquisition Regulation Supplement
18. PCI DSS – Payment Card Industry Data Security Standard
19. GDPR – General Data Protection Regulation
20. FIPS – Federal Information Processing Standards
21. CIS RAM – Center for Internet Security Risk Assessment Method
22. SaaS – Software as a Service
23. IDS – Intrusion Detection System
24. BYOD - Bring Your Own Device

ВВЕДЕНИЕ

Информационная безопасность является важнейшим аспектом современных бизнес-операций, независимо от отрасли или размера компании. В сегодняшнюю цифровую эпоху компании всех размеров и типов уязвимы для киберугроз, включая утечку данных, атаки программ-вымогателей и другие формы злонамеренной деятельности. В результате для предприятий важно уделять приоритетное внимание информационной безопасности, чтобы защитить свои активы, клиентов и репутацию.

В этом контексте важность информационной безопасности варьируется в зависимости от типа компании. Для крупных многонациональных корпораций информационная безопасность является главным приоритетом из-за значительного объема конфиденциальных данных, которые они обрабатывают, и потенциального влияния нарушения безопасности на их деятельность и репутацию. С другой стороны, малые и средние предприятия (МСП) могут считать, что они менее подвержены киберугрозам из-за своего размера и ограниченных ресурсов. Однако малые и средние предприятия часто становятся мишенью киберпреступников именно потому, что им не хватает изощренных мер безопасности и ресурсов более крупных организаций.

Независимо от размера или типа компании потенциальные последствия нарушения безопасности могут быть серьезными. Нарушение данных может привести к финансовым потерям, юридическим последствиям и ущербу для репутации компании. Более того, затраты на восстановление после нарушения безопасности могут быть значительными как с точки зрения финансовых ресурсов, так и времени.

Поэтому для всех компаний крайне важно осознать важность информационной безопасности и принять меры для создания комплексной системы безопасности. Уделяя приоритетное внимание информационной безопасности, компании могут снизить потенциальные риски, защитить свои активы и операции и обеспечить долговечность своего бизнеса во все более цифровом мире.

Библиография

1. PECA, Ludmila, ȚURCANU, Dinu. *Computer networks: Practical examples solved to be introduced in computer networks.* Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Software Engineering Department and Automatics. Chișinău: Tehnica-UTM, 2022. ISBN 978-9975-45-812-2. http://www.repository.utm.md/handle/5014/20549

2. DUMBRAVEANU, Roza, PECA, Ludmila. *E-learning Strategy in the Elaboration of Courses, International Conference on Virtual Learning*. ISSN 2971-9291, ISSN-L 1844-8933, vol. 17, pp. 15-26, 2022. https://doi.org/10.58503/icvl-v17y202201

3. SIEVERS, Thomas. *Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations.* International Cybersecurity Law Review, 2021, 2, pages 223–231. https://doi.org/10.1365/s43439-021-00033-8

4. SCHMIEMANN, Manfred. *Enterprises by size class – overview of SMEs in the EU.* Eurostat. Statistics in Focus, 31/2008. KS-SF-08-031. https://ec.europa.eu/eurostat/web/products-statistics-in-focus/-/ks-sf-08-031

5. NEGREIRO ACHIAGA, Maria Del Mar. *The NIS2 Directive: A high common level of cybersecurity in the EU.* European Union, Briefing 08-02-2023. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

6. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Approved on: 2018-04-16.

7. NATIONAL INSTITUTE OF STANDARTS AND TECHNOLOGY. Security and Privacy Controls for Information Systems and Organizations, SP 800-53 Rev. 5, 2020. NSPUE2. https://doi.org/10.6028/NIST.SP.800-53r5

8. NATIONAL INSTITUTE OF STANDARTS AND TECHNOLOGY. Control Baselines for Information Systems and Organizations, SP 800-53B, 2020. NSPUE2. https://doi.org/10.6028/NIST.SP.800-53B

9. NICCS: NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES, ©2018 [cited on 14.09.2021]. Available on: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#T.

10. CENTER FOR INTERNET SECURITY. CIS Critical Security Control. 2019.

11. CENTER FOR INTERNET SECURITY. CIS Critical Security Controls SME Companion Guide for v7.1. 2019.

12. CENTER FOR INTERNET SECURITY. CIS RAM (Risk Assessment Method). 2022.

13. DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS (NIS Directive). EU 2016/1148. Available: https://www.itgovernance.eu/da-dk/nis-directive-dk

14. Glossary: Enterprise. Eurostat Statistics Explained. [viewed 01.02.2023] Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Enterprise.

15. Archive: Business economy - size class analysis. Eurostat Statistics Explained. [viewed 01.02.2023] Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:Business_economy_-_size_class_analysis#Methodology_.2F_Metadata.

16. An Overview of the NIS Directive. SSH Academy. [viewed 03.02.2023] Available: https://www.ssh.com/academy/compliance/nis-directive

17. A Guide to the NIS2 Directive. SSH Academy. [viewed 03.02.2023] Available: https://www.ssh.com/academy/compliance/nis2-directive

18. NIS2: expansion to additional business sectors and strengthened security requirements. Houthoff. [viewed 06.02.2023] Available: https://www.houthoff.com/insights/news-update/data-protection-cybersecurity---nis2-directive-eus-enhanced-cybersecurity-strategy---july-2022

19. The NIS 2 Directive, Final Text. Article 2, NIS 2 Directive: Scope. [viewed 11.02.2023] Available: https://www.nis-2-directive.com/NIS_2_Directive_Article_2.html

20. The NIS 2 Directive, Final Text. Article 3, NIS 2 Directive: Essential and important entities. [viewed 11.02.2023] Available: https://www.nis-2-directive.com/NIS_2_Directive_Article_3.html

21. The NIS 2 Directive, Final Text. Article 7, NIS 2 Directive: National cybersecurity strategy. [viewed 11.02.2023] Available: https://www.nis-2-directive.com/NIS_2_Directive_Article_7.html.

22. SCHWARTZ, Rachael, Business Development Director, CSI. CIS Basic Controls for Organizational Cybersecurity. [viewed 17.02.2023] Available: https://www.csiweb.com/what-to-know/content-hub/blog/cis-controls-the-building-blocks-of-organizational-cybersecurity/

23. SCHWARTZ, Rachael, Business Development Director, CSI. 10 Foundational CIS Controls: Building On The Basics. [viewed 17.02.2023] Available: https://www.csiweb.com/what-to-know/content-hub/blog/10-foundational-cis-controls-building-on-the-basics/

24. RSI Security. WHAT ARE THE FOUR ORGANIZATIONAL CIS CRITICAL SECURITY CONTROLS. July 23, 2020. [viewed 18.02.2023] Available: https://blog.rsisecurity.com/what-are-the-four-organizational-cis-critical-security-controls/