MINISTERUL EDUCAȚIEI, CULTURII ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software şi Automatică

Admis la susţinere
Șef departament:
Ion Fiodorov, conf. univ., dr.

_____

„____”_____ 2021

Психологические аспекты в разработке, имплементации и исполнении политик информационной безопасности

Teză de master

Student: **Bunescu Ivan, TIA-191M**

Conducător: **Zgureanu Aureliu, conf. univ., dr.**

Chişinău, 2021

РЕЗЮМЕ

Тема: Психологические аспекты в разработке, имплементации и исполнении политик информационной безопасности.

Автор: Бунеску Иван.

Данная работа включает введение, три главы, заключение, оформлена на 46 страницах основного текста, содержит 28 рисунков.

Ключевые слова: Физическая безопасность, логическая безопасность, меметика, нейролингвистическое программирование, психология сотрудников.
На сегодняшний день в Республике Молдова зарегестрированны 660 активных резидентов в парке высоких технологий “Moldova IT Park” [1]. На рынке не хватает достаточное количество специалистов, что вынуждает компании бороться между собой и переманивать специалистов из других компаний. Это порождает, легкомысленное отношение сотрудников к нормам, и уставам этих компаний, что негативно может повлиять на взаимоотношения между компаниями и их клиентами. В этих условиях рынка, некоторые компании стараются создать определённый положительный психологический климат для своих сотрудников.

Целью данной работы, является анализ, психологических аспектов в обеспечении информационной безопасности на различных её этапах.

Главными задачами являются: обозначение уровней физической и логической безопасности; установление круга лиц ответственных за реализацию политик безопасности и лиц сопутствующих её реализации; выработка новых непрямых методов воздействия на сотрудников IT компаний с целью повысить уровень информационной безопасности; создание конкретной модели по обеспечению информационной безопасности в отдельно взятой IT компании.

Были использованы следующие *методы*: Анализ, классификация, обобщения, сравнение, моделирование, прогнозирования и наблюдения.

Благодаря, данной работе, были созданы примеры мемов для обеспечения физической и логической информационной безопасности и было предложено два метода практической реализации в отдельно взятой компании, посредством групповых политик настройки операционной системы Windows. Также установлено, что данная модель может получить разностороннее развитие и, может быть, разными способами реализовано в виртуальной и объективной реальности.

REZUMAT

Tema: Aspecte psihologice în elaborarea, implementarea și executarea politicii de securitate informațională.

Autor: Bunescu Ivan.

Prezenta lucrare include introducere, trei capitole, concluzii și este realizată pe 46 pagini text de baza, si conține 28 de imagini.

Cuvinte cheie: securitatea fizică, securitatea logică, memetică, programare neuro-lingvistică, psihologia angajaților.

Scopul acestei lucrări reprezintă analiza aspectelor psihologice în asigurarea securității informațională în diferite etape.

Principalele obiective ale acestei lucrări sunt: determinarea nivelelor de securitate fizică si logică; determinarea cercului de persoane care sunt responsabile de executarea politici de securitate informațională și determinarea cercului de persoane care contribuie la asigurarea securității informaționale; elaborarea noilor metode de influență indirectă asupra angajaților companiilor IT în vederea fortificării nivelului/ gradului de securitatea informațională; crearea modelului concret de asigurarea securității informaționale în cadrul unei companii IT concrete.

În cadrul studiului au fost aplicate următoarele *metodele*: analiză, clasificare, generalizare, comparare, modelare, prognozare și observare.

Ca urmare a cercetărilor efectuate au fost create exemple de memuri îndreptate spre asigurarea securității informaționale. Totodată, au fost recomandate două căi de implementare tehnică a aplicării memurilor într-o companie prin setările politicilor de grup al Windows. La fel, a fost demonstrat că acest model ar putea fi extins în spațiul virtual și cel real prin diferite metode.

SUMMARY

Topic: Psychological aspects in the elaboration, implementation and execution of information security policies.

Author: Bunescu Ivan.

This work includes an introduction, three chapters, a conclusion, framed on 46 pages of the main text, contains 28 figures.

Key words: Physical security, logical security, memetics, neurolinguistic programming, employee psychology.

The purpose of this work is to analyze the psychological aspects of ensuring information security at its various stages.

The main tasks are: designation of the levels of physical and logical security; establishing the circle of persons responsible for the implementation of security policies and persons accompanying its implementation; elaboration of new indirect methods of influencing employees of IT companies in order to increase the level of information security; creation of a specific model for ensuring information security in a single IT company.

The following *methods* were applied in the study: analysis, classification, generalization, comparison, modeling, forecasting and observation.

As a result of the research, examples of memes were created aimed at ensuring the security of information. At the same time, two ways of technically implementing memes application in a company through Windows group policy settings were recommended. It has also been shown that this model could be extended to virtual and real space by different methods.

CUPRINS

ВВЕДЕНИЕ

На сегодняшний день в Республике Молдова зарегестрированны 660 активных резидентов в парке высоких технологий “Moldova IT Park” [1]. Разумеется, этим компаниям нужны сотрудники, которые будут работать на проектах, в интересах компании и иностранных клиентов. Однако, на рынке не хватает достаточное количество специалистов, что вынуждает компании бороться между собой и переманивать специалистов из других компаний. Это порождает, уверенность и свободное, порой легкомысленное отношение сотрудников к нормам, традициям, культуре и уставам этих компаний, что негативно может повлиять на взаимоотношения между компаниями и их клиентами. Так как, по большей части, определённые требования, условия, вменяются компаниям как обязанность, за нарушение которых может последовать пеня, неустойка либо разрыв сделки. В этих условиях рынка, некоторые компании стараются создать определённый положительный психологический климат для своих сотрудников, чтобы привлечь их к сотрудничеству, добиться симпатий в отношений этой компании и тем самым обратить внимание сотрудника на то, что условия и требования клиента должны быть соблюдены на 100%.

Таким образом, ***объектом*** исследования данной дипломной работы являются:

- психологическое состояние специалиста в области информационных технологий;

- факторы, влияющие на психологию сотрудника, которые побуждают к соблюдению или несоблюдению политик информационной безопасности;

- методы работы, практические приёмы, используя которые возможно будет влиять на мотивацию сотрудника по исполнению важнейших для компании политик в области информационной безопасности.

Целью данной работы, является анализ, психологических аспектов в обеспечении информационной безопасности на различных её этапах.

Главными задачами являются: обозначение уровней физической и логической безопасности; установление круга лиц ответственных за реализацию политик безопасности и лиц сопутствующих её реализации; выработка новых непрямых методов воздействия на сотрудников IT компаний с целью повысить уровень информационной безопасности; создание конкретной модели по обеспечению информационной безопасности в отдельно взятой IT компании.

Благодаря *методу анализа* удалось исследовать различные теоретические материалы и политики в области информационной безопасности.

Так же, был использован *метод наблюдения* за поведением сотрудников, их взаимоотношения с работодателем и наблюдением за реакцией сотрудников в отношении тех или иных политик информационной безопасности.

Метод *классификации* позволяет классифицировать исследуемые объекты, проблемы и пути их решения с целью формирования системы обеспечения информационной безопасности.

Метод *моделирования* позволяет создать эффективную модель взаимодействия внутри компании с целью повысить качество информационной безопасности.

Метод *прогнозирования* позволяет определить вероятные последствия применения тех или иных мер, а также уменьшить риски и угрозы информационной безопасности.

Используя *метод обобщения и анализа* результатов исследования автору работы, удалось обобщить, систематизировать и разработать ряд рекомендаций, которые позволят на практике убрать негативные психологические аспекты в условиях работы и психологическом состоянии сотрудников компаний.

В первой главе, были рассмотрена процедура создания политик в области физической безопасности, как части информационной безопасности. Также, были установлены лица, которые в той или иной степени являются ответственными за обеспечение физической безопасности, а также лица, сопутствующие осуществлению физической безопасности. Были обозначены уровни/периметры и узлы физической безопасности.

Во второй главе, была рассмотрена процедура создания политик в области логической безопасности, как части информационной безопасности. Также, были установлены лица, которые в той или иной степени являются ответственными за обеспечение физической безопасности, а также лица, сопутствующие осуществлению физической безопасности.

В третьей главе были рассмотрены, основы меметики и нейролингвистического программирования. Были приведены реальные примеры различных видов мемов и примеры нейролингвистического программирования, используемые в бизнесе, государственной безопасности и политике. Также, были выработаны по пять мемов для физической и логической безопасности, в качестве предложения для конкретной IT компании и было описано два способа технической реализации внедрения мемов.

Благодаря, данной работе, были созданы примеры мемов для обеспечения физической и логической информационной безопасности и было предложено два метода практической реализации в отдельно взятой компании, посредством групповых политик настройки операционной системы Windows. Также установлено, что данная модель может получить разностороннее развитие и, может быть, разными способами реализовано в виртуальной и объективной реальности.

БИБЛИОГРАФИЯ

1. Moldova IT Park official web page. Доступен: https://moldovaitpark.md/en/;
2. Кияев В. И., Граичин О.Н.. *Безопасность информационных систем*. Национальный Открытый Университет «ИНТУИТ», 2016, с. 191;
3. M. E Whitman, H. J. Mattord. *Principles of Information Security*, © 2012 Course Technology, Cengage Learning, с. 617;
4. «*Google Data Center Security: 6 Layers Deep*». Видео. [18.06.2020] Доступен: https://www.youtube.com/watch?v=kd33UVZhnAA;
5. John R. Vacca. *Computer and Information Security Handbook*, © 2009 by Elsevier Inc. ISBN: 978-0-12-374354-1, с. 844;
6. Kevin Daimi. *Computer and Network Security Essentials*. © Springer, ISBN 978-3-319-58424-9, с. 618;
7. *Информационные технологии. Свод правил по управлению защитой информации*. ИСО/МЭК 2005. ISO/IEC 27002:2005(E), с. 171. Доступен: https://pqm-online.com/assets/files/lib/std/iso_iec_27002-2005.pdf;
8. *Stuxnet delivered to Iranian nuclear plant on thumb drive*. [12.04.2012] Доступен: https://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/;
9. Внутренний предиктор СССР. *Мёртвая вода. От "социологии" к жизнеречению*, Китеж, державный град России. 2011, с. 484. Доступен: http://lit.md/files/vpsssr-books/mertvaya_voda_tom_1_A5.pdf;
10. *Административные методы управления персоналом*, [05.08.2016] Доступен: https://kontur.ru/articles/4396;
11. Ричард Броуди. *Психические вирусы. Как программируют ваше сознание*., издательство: Поколение, 2007 г., с. 145;
12. Joseph O' Connor, *NLP WORKBOOK*. Thorsons, 2001. ISBN 0-00-710003-5, с. 303. Доступен: https://doc.lagout.org/science/0_Computer%20Science/3_Theory/Neural%20Networks/Neuro%20Linguistic%20Programming%20WorkBook.pdf.
13. D. ILIEVA-KOLEVA, R. VAZOV. *Neuro-linguistic Programming Techniques for Perfecting Presentation Skills*. Conference Paper – October 2014, Доступен: https://www.researchgate.net/publication/283346614_Neuro-linguistic_Programming_Techniques_for_Perfecting_Presentation_Skills;
14. *НЛП: визуал, аудиал, кинестетик, дискрет*. [28.12.2019] Доступен: https://zen.yandex.ru/media/id/5df4df70bd639600b47a256d/nlp-vizual-audial-kinestetik-diskret-5e0717d3433ecc00b14ae1ea;

15. *Киевская киностудия научно-популярных фильмов*, 1971 г, [13.11.2012], Доступен: https://www.youtube.com/watch?v=_LYe58b-3HM;
16. Роберт Чалдини. Психология согласия. Доступен: https://fictionbook.ru/author/robert_chaldini/psihologiya_soglasiya/read_online.html?page=2
17. *Clear desk and clear screen policy – What does ISO 27001 require?* [14.03.2016] Доступен: https://advisera.com/27001academy/blog/2016/03/14/clear-desk-and-clear-screen-policy-what-does-iso-27001-require