АСТІСТОВА Т. І., УНГУР`ЯН С.Д.

ДОСЛІДЖЕННЯ АЛГОРИТМІВ ТА МОДЕЛЕЙ ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

ASTISTOVA T. I., UNGUR'YAN S. D.

RESEARCH OF ALGORITHMS AND MODELS OF CYBER SECURITY TECHNOLOGIES

Annotation. The life of society, its information security depends on the stable functioning, reliability, readiness of telecommunication networks to reflect the uncontrolled impact of unauthorized access.

To investigate existing models of cyber security technologies, algorithms of cryptographic methods of encryption, key distribution, practical aspects of next-generation networks is the main goal of the work.

The protection of information transmitted and processed in networks consists in creating and maintaining a system of technical (engineering, software and hardware) and non-technical (legal, organizational) measures that allow preventing or complicating the possibility of threats, as well as reduce potential losses.

In their classification, cyber security technologies are grouped by categories, based on the goals they achieve. According to the methods of achieving the goals of a set of categories, cyber security technologies are combined into technical methods and techniques of cyber security

Keyword: algorithms, telecommunication networks, software, cyber security technologies.

ВСТУП

Життєдіяльність суспільства, його інформаційна безпека залежить від стабільного функціонування, надійності, готовності телекомунікаційних мереж до відображення неконтрольованого впливу несанкціонованого доступу.

Виникнення комп'ютерних вірусів та інших загроз викликають необхідність у забезпеченні кібербезпеки, яка є головною частиною національної безпеки в цілому, пов'язаною із захистом та безпекою інформаційних ресурсів організації або користувача.

Дослідити існуючі моделі технологій кібербезпеки, алгоритми криптографічних методів шифрування, розподілу ключів, практичні аспекти мереж наступних поколінь і є основною метою роботи.

Основним об'єктом дослідження є архітектура системи кібербезпеки інфокомунікацій, відповідно до вимог безпеки, модель довіри кібербезпеки та система існуючих сервісів програмно-апаратного забезпечення.

Основний розділ

Теоретичною основою при вирішенні науково-технічної проблеми є праці провідних науковців у галузі кібербезпеки та захисту від кібератак, теорії мереж, математичного моделювання, математичного та програмного забезпечення. У теоретичних дослідженнях використано методи та

алгоритми технології криптографії на прикладі цифрових підписів, шифрування, розподілу ключів.

Захист інформації, що передається та обробляється в мережах, полягає у створенні та підтримці в дієздатному стані системи заходів як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки.

Іншими словами, захист інформації спрямовано на забезпечення кібербезпеки оброблюваної інформації в NGN- мережах майбутнього покоління в цілому, тобто такого стану, який забезпечує збереження заданих властивостей інформації. Система зазначених заходів, що забезпечує захист інформації у NGN, є комплексною системою захисту інформації.

Технологія кібербезпеки - це опис процесів забезпечення кібербезпеки, інструкції з їх виконанням, технологічні вимоги до кібербезпеки, а також операції проєктування, створення, експлуатації, менеджменту, які є основою процесу забезпечення кібербезпеки.

У своїй класифікації технології кібербезпеки групуються за категоріями, за ознаками цілей, що ними досягаються. За методами досягнення цілей сукупності категорій технології кібербезпеки поєднуються в технічні прийоми та техніки кібербезпеки.

Логіку забезпечення безпеки доцільно доповнити технологіями кібербезпеки, які зручно описувати ієрархічною послідовністю – (Рис.1).

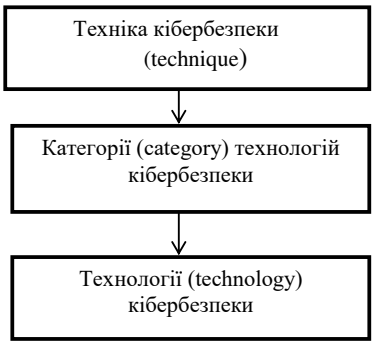

Рисунок 1 – Ієрархічна послідовність технологій кібербезпеки

Концепція трьох базових властивостей інформаційної безпеки (ІБ) називається моделлю КЦД (конфіденційність, цілісність та доступність). CIA model: confidentiality, integrity and availability). Вона була запропонована Зальцером та Шредером (Saltzer and Schroeder).

Суть цієї концепції досить проста - три виміри куба відображають три ключові напрямки ІБ:
• мета безпеки (класична тріада - конфіденційність, цілісність та доступність)
• стан інформації (обробка, зберігання, передача)
• захисні заходи (персонал, політики та практики, технології).

У 1991 році МакКамбером (McCumber) була розроблена повна модель ІБ відома як куб МакКамбера Куб складається з 3 граней: стан інформації (зберігання, передача та обробка), характеристики або властивості ІБ (КЦД), контрзаходи безпеки (підготовка та навчання, політики та практики, технології). Таким чином, виходить 3x3x3 = 27 осередків. МакКамбер вийшов з рамок плоских, одно- і двовимірних поглядів і подивився на завдання вже з тривимірної точки зору.
Подальший розвиток моделі куба Маккамбера запропонував Маконахі (МасопасЬу)]. Він розширив список властивостей ІБ, назвавши ці властивості «Сервіси безпеки».

Кількість значень цього виміру збільшилася з 3 до 5 (додалися значення «авторство» та «невідмовність від авторства») і куб став складатися з 3*5*3 = 45 осередків. Такий підхід розширив модель інформаційної безпеки, продемонструвавши розширюваність куба Маккамбера. При цьому існує четвертий вимір «час», а загальна модель є гіперкубом.

Модель куба МакКам-бера і Маконахі була покладена основою еталонної моделі забезпечення безпеки інформації та безпеки (RMIAS)

Складові моделі класифікації технологій кібербезпеки:
- криптографія (Cryptography);
- контроль доступу (Access control);
- цілісність системи (System integrity);
- аудит та моніторинг (Audit and Monitoring);
- менеджмент (Management

Криптографія симетричного ключа використовує алгоритм шифрування RSA, в яких ключ шифрування і ключ дешифрування один і той же алгоритм узгодження ключів, можна реалізувати в системі програмування Visual Studio мовою C #.

RSA став першим алгоритмом криптографії симетричного ключа, , придатним і для шифрування, і цифрового підписуАлгоритм можна реалізувати на мові Pyton 3.

Виводи

Основною вимогою до сучасних інформаційних систем стає забезпечення доступності, цілісності та конфіденційності інформаційних ресурсів. У таких вимогах велику роль відіграє комплексний підхід, що

поєднує в собі заходи законодавчого, організаційного і програмно-технічного характеру. Технології кібербезпеки, це операції проєктування, створення, експлуатації, менеджменту, які є основою процесу забезпечення кібербезпеки. Вони групуються за категоріями, за ознаками цілей, що ними досягаються. Модель куба МакКам-бера і Маконахі була покладена основою еталонної моделі забезпечення безпеки інформації та безпеки (RMIAS).

Література

1. Гончарова Л.Л. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. / Л.Л. Гончарова, А.Д. Возненко, О.І. Стасюк та ін. – К.: ДЕТУТ, 2013. – 435 с.

2. Засіб криптографічного захисту інформації. МагПро КриптоПакет вер. 2.1. Бібліотека libcrypto. Посібник програміста [Електронний ресурс]. – 2012. – Режим доступу: http://www.cryptocom.ua /docs/cryptopack21-libcrypto.pdf

КУЛАГІН В.П., ДЕМКІВСЬКА Т.І.

РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБЛІКУ РОБОЧОГО ЧАСУ РОБІТНИКІВ ПІДПРИЄМСТВА

KULAHIN V.P., DEMKIVSKA T.I.

DEVELOPMENT OF SOFTWARE FOR THE AUTOMATED SYSTEM OF RECORDING THE WORKING TIME OF THE WORKERS IN ENTERPRISE

Annotation. The article presents the analysis and characteristics of the automated system of recording the working time of the workers in enterprise.

The paper version of data entry and storage is no longer relevant, so modernity needs to change. Modern technologies allow the use of electronic databases in enterprises and store all important data in them.

The development of an automated system of recording the working time of the workers in enterprise is a topical issue today, because it facilitates the work of the employees and provides information about workers efficiency. Also, this method is more reliable and practical to use and is to maintain the confidentiality of information.

Keywords: Automated workplace, Database, Information system, Accounting system, Graphical interface.

Вступ

На сьогоднішній день паперовий варіант обліку робочого часу працівників підприємства вже дуже застарілий і не актуальний. Він потребує багато часу для його ведення та для формування різноманітної звітності. Крім того виникають складності з конфіденційністю інформації.

Автоматизація різноманітних процесів на підприємстві дозволяє полегшити роботу працівників та надає можливості для швидкого формування різноманітних звітів. Це дає змогу контролювати ефективність кожного працівника та полегшує багато внутрішніх процесів підприємства. Створюється програмний продукт, який допоможе вести облік працівників, вести облік робочого часу кожного працівника, облік часу