

БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
МАШИНОСТРОИТЕЛЬНЫЙ ФАКУЛЬТЕТ
КАФЕДРА «ИНТЕЛЛЕКТУАЛЬНЫЕ И МЕХАТРОННЫЕ СИСТЕМЫ»

ДОПУЩЕН К ЗАЩИТЕ
Заведующий кафедрой

А.В. Гулай

« 26 » декабря 2019 г.

**РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
ДИПЛОМНОГО ПРОЕКТА**

«Интеллектуальная система криптографической защиты эталонов базы доступа»

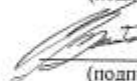
Специальность 1-55 01 01 «Интеллектуальные приборы, машины и производства»

Обучающийся
группы 10306115

 17.12.19
(подпись, дата)

А.В. Бурый

Руководитель проекта

 17.12.19
(подпись, дата)

В.М. Зайцев

Консультанты

по экономическому
разделу

 17.12.19
(подпись, дата)


Н.В. Комина

по охране труда

 17.12.19
(подпись, дата)

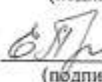
Е.Ф. Пантелеенко

по переводу научно-
технической литературы

 18.12.2019
(подпись, дата)


Ю.В. Безнис

по электронной
презентации

 26.12.19
(подпись, дата)

Е.В. Полюнкова

Ответственный за нормоконтроль

 10.12.2019
(подпись, дата)

З.Н. Волкова

Объем работы:

расчетно-пояснительная записка - 73 страницы;

графическая часть - 8 листов;

магнитные (цифровые) носители - 1 единица.

Минск 2019

РЕФЕРАТ

Дипломный проект: 81 с., 2 ил., 15 табл., 23 источников.

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА. БАЗЫ ДАННЫХ.

Объект исследования: криптографические алгоритмы.

Цель проекта: разработка интеллектуальной системы криптографической защиты эталонов базы доступа.

В результате выполнения дипломного проекта разработана система интеллектуальной криптографической защиты эталонов базы доступа. В состав системы входит центр генерации ключей, внешние носители ключевой информации, абоненты, серверы приложения и серверы базы данных. Система при помощи известных криптографических алгоритмов осуществляет безопасное хранение данных, предназначенных для получения доступа к базам данных.

РЕФЕРАТ

Дипломный проект: 81 с., 2 ил., 15 табл., 23 источников.

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА. БАЗЫ ДАННЫХ.

Объект исследования: криптографические алгоритмы.

Цель проекта: разработка интеллектуальной системы криптографической защиты эталонов базы доступа.

У результаті виконання дипломного проекту розроблена система інтелектуальної криптографічної захисту еталонів бази доступу. У склад системи входить центр генерації ключів, зовнішні носії ключової інформації, абоненти, сервери додатку і сервери бази даних. Система при допомозі відомих криптографічних алгоритмів здійснює безпечне зберігання даних, призначених для отримання доступу до баз даних.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1) Кузнецов С. Д. Базы данных: учебник для студ. учреждений высшего проф. образования / С. Д. Кузнецов. — Москва: Издательский центр «Академия», 2012 — 496 с.
- 2) Защита данных в СУБД Oracle [Электронный ресурс] – Режим доступа: https://www.aladdin-rd.ru/company/pressroom/articles/russskaa_versia_indijskoj_zasity_ili_zasita_dannyh_v_subd_oracle свободный. – Загл. С экрана. – Яз. Рус.
- 3) Техническая документация по SQL Server [Электронный ресурс] – Режим доступа: <https://docs.microsoft.com/ru-ru/sql/sql-server/?view=sql-server-2016> свободный. – Загл. С экрана. – Яз. Рус.
- 4) Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич – Минск/Москва: «Новое Знание», 2003. - 381 с.
- 5) Хорев П.Б. Образовательная сеть доверия на основе сертификатов стандарта x.509 / П.Б. Хорев. – Минск: Национальный исследовательский университет "МЭИ", 2016 – 248 с.
- 6) СТБ 34.101.65- Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS), 2014.
- 7) eToken для обеспечения безопасности данных в СУБД Oracle Режим доступа: http://www.infosecurity.ru/_eshop/detail/etoken_ora3.pdf свободный. – Загл. С экрана. – Яз. Рус.
- 8) Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си/ Б.Шнайер — Москва: Триумф, 2002. — 816 с.
- 9) ГОСТ 34.12-2018 Информационная технологи. Криптографическая защита информации. Блочные шифры, 2019
- 10) ГОСТ 34.13-2018 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, 2019

- 11) Расширенный стандарт шифрования [Электронный ресурс] – Режим доступа: <https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf> свободный. – Загл. С экрана. – Яз. Англ.
- 12) Анатомия ядра Linux [Электронный ресурс] – Режим доступа: <https://www.ibm.com/developerworks/ru/library/l-linux-kernel/> свободный. – Загл. С экрана. – Яз. Рус.
- 13) Расчет параметров серверного оборудования Linux [Электронный ресурс] – Режим доступа: <https://its.1c.ru/db/metod8dev#content:5810:hdoc> – Загл. С экрана. – Яз. Рус.
- 14) Бабук И. М. Экономика промышленного предприятия: учеб. пособие/И.М.Бабук, Т.А.Сахнович. – Минск: Новое знание; М.: ИНФРА-М, 2013. – 439с.
- 15) Головачев А. С. Конкурентоспособность организации: учеб. Пособие/А.С.Головачев. – Минск: Выш. шк., 2012. –319с.
- 16) М. Е. Цуцков. Охрана труда. Большая медицинская энциклопедия: в 30 т. / Б.В. Петровский. Москва: Советская энциклопедия, 1982. — 528 с.
- 17) ГОСТ 12.2.032-78 Система стандартов безопасности труда (ССБТ). Рабочее место при выполнении работ сидя. Общие эргономические требования, М.: ИПК Издательство стандартов, 2001
- 18) СанПиН от 28.06.2013 № 59 Требования при работе с видеодисплейными терминалами и электронно-вычислительными машинами. – Мн.: МЗ РБ, 2013
- 19) ГОСТ 12.0.003-74 Система стандартов безопасности труда (ССБТ). Опасные и вредные производственные факторы. Классификация (с Изменением N 1), М.: ИПК Издательство стандартов, 2002
- 20) Типовая инструкции по охране труда при работе с персональными электронными вычислительными машинами №130. – Мн.: Министерства труда и социальной защиты Республики Беларусь, 2013

21) СНБ 4.02.01-03 Отопление, вентиляция и кондиционирование воздуха. – Мн.: Министерство архитектуры и строительства Республики Беларусь, 2004

22) ТКП 474-2013 Категорирование помещений, зданий и наружных установок по взрывопожарной и пожарной опасности. – Мн.: Министерство по чрезвычайным ситуациям Республики Беларусь, 2013

23) ТКП 45-2.02-315-2018 Пожарная безопасность зданий и сооружений. Строительные нормы проектирования. – Мн.: Министерство архитектуры и строительства Республики Беларусь, 2018