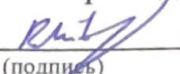


БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет информационных технологий и робототехники
Кафедра «Программное обеспечение информационных систем и технологий»

ДОПУЩЕН К ЗАЩИТЕ

Старший преподаватель

 Н.В. Воюш
(подпись) (инициалы и фамилия)

« 16 » 06 2026 г.

РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
ДИПЛОМНОГО ПРОЕКТА

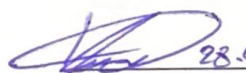
«Кроссплатформенный java-модуль для подписания и проверки
документов с использованием API AVEST»

Специальность 1-40 05 01 «Информационные системы и технологии (по направлениям)»

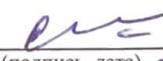
Направление специальности 1-40 05 01-04 «Информационные системы и технологии (в обработке и представлении информации)»

Обучающийся

группы 10702222
(номер)

 28.05.26 Д.В. Ключников
(подпись, дата)

Руководитель

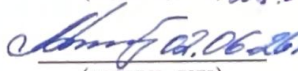
 28.05.26 В.В. Сидорик
(подпись, дата)

Консультанты:

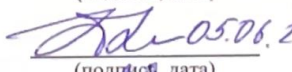
по разделу «Компьютерное проектирование»

 28.05.26 В.В. Сидорик
(подпись, дата)

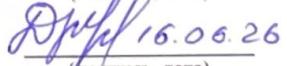
по разделу «Охрана труда»

 12.06.26 М.Л. Калиниченко
(подпись, дата)

по разделу «Экономика»

 05.06.26 Н.В. Комина
(подпись, дата)

Ответственный за нормоконтроль

 16.06.26 Н.С. Домаренко
(подпись, дата)

Объем проекта:

расчетно-пояснительная записка — 102 страниц;

графическая часть — 14 листов;

магнитные (цифровые) носители — 1 единиц.

Минск 2026

РЕФЕРАТ

JAVA-МОДУЛЬ ПОДПИСАНИЕ ДОКУМЕНТОВ, ПРОВЕРКА ДОКУМЕНТОВ, ИСПОЛЬЗОВАНИЕ API AVEST, ДИАГРАММА ВАРИАНТОВ ИСПОЛЬЗОВАНИЯ

Объектом данного дипломного проекта является процесс автоматизации формирования и проверки электронной цифровой подписи (ЭЦП) для документов в формате PKCS#7/CMS с использованием криптопровайдера AVEST в корпоративной среде Белорусского национального технического университета.

Цель проекта – разработка кроссплатформенного Java-модуля и веб-приложения на базе Spring Boot, обеспечивающего подписание и криптографическую проверку документов (строк, файлов, атрибутов ELMA, данных NCIS) через REST API с возможностью работы как в режиме реального криптопровайдера (prod), так и в режиме имитации (stub) для тестирования и демонстрации.

В ходе выполнения дипломного проекта были решены следующие задачи:

1) разработана архитектура кроссплатформенного модуля на Java 8 с использованием Spring Boot 2.6.4;

2) построены диаграммы вариантов использования, компонентная диаграмма и диаграмма последовательности;

3) спроектирован и разработан веб-интерфейс (HTML/CSS/JS) с визуализацией конвейера подписи и экспортом отчётов;

4) реализованы два режима работы: prod (интеграция с AVEST Java SDK и KeyStore AvPersonal) и stub (имитация без реального ключа);

5) проведены тестирование и отладка веб-приложения в обоих режимах. Элементами научной новизны и практической значимости полученных результатов являются:

Областью возможного практического применения является внедрение разработанного модуля в документооборот БНТУ и других учреждений образования Республики Беларусь, использующих электронную подпись в соответствии с законодательством.

Студент-дипломник подтверждает, что приведённый в дипломном проекте расчётно-аналитический материал объективно отражает состояние разрабатываемого объекта, все заимствованные из литературных и других источников теоретические и методологические положения сопровождаются ссылками на их авторов.

Дипломный проект: 102 с., 34рис., 15 табл., 27 источников, 1 прил.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Fielding, R. T. Architectural Styles and the Design of Network-based Software Architectures : dis. ... Ph.D. / Roy Thomas Fielding. – Irvine : University of California, 2000. – 162 p.
- 2 Spring Boot [Electronic resource] / VMware, Inc. – Electronic data. – Access mode: <https://docs.spring.io/spring-boot/docs/2.6.4/reference/html/>, free. – Title from the screen. – Language: English.
- 3 Spring Framework [Electronic resource] / VMware, Inc. – Electronic data. – Access mode: <https://docs.spring.io/spring-framework/docs/5.3.16/reference/html/>, free. – Title from the screen. – Language: English.
- 4 Java Platform, Standard Edition 8 [Electronic resource] / Oracle Corporation. – Electronic Data. – Access mode: <https://docs.oracle.com/javase/8/docs/>, free. – Title from the screen. – Language: English.
- 5 JSON Web Token (JWT) [Electronic resource] / IETF. – Electronic data. – Access mode: <https://tools.ietf.org/html/rfc7519>, free. – Title from the screen. – Language: English.
- 6 PKCS #7: Cryptographic Message Syntax [Electronic resource] / IETF. – Electronic data. – Access mode: <https://tools.ietf.org/html/rfc2315>, free. – Title from the screen. – Language: English.
- 7 AVEST CryptoProvider [Electronic resource] / AVEST LLC. – Electronic data. – Access mode: <https://avest.by/>, free. – Title from the screen. – Language: Russian.
- 8 AVEST Java SDK Documentation / ООО AVEST. – Minsk, 2021. – 120 p.
- 9 HTML [Electronic resource] / MDN Web Docs. – Electronic data. – Access mode: <https://developer.mozilla.org/en-US/docs/Web/HTML>, free. – Header. – Language: English.
- 10 CSS [Electronic resource] / MDN Web Docs. – Electronic data. – Access mode: <https://developer.mozilla.org/en-US/docs/Web/CSS>, free. – Header. – Language: English.
- 11 JavaScript [Electronic resource] / MDN Web Docs. – Electronic data. – Access mode: <https://developer.mozilla.org/en-US/docs/Web/JavaScript>, free. – Header. – Language: English. – Language: English.
- 12 IntelliJ IDEA [Electronic resource] / JetBrains s.r.o. – Electronic data and programs – Access mode: <https://www.jetbrains.com/idea/documentation/>, free. – Title from the screen. – Language: English.
- 13 Maven [Electronic resource] / Apache Software Foundation. – Electronic data – Access mode: <https://maven.apache.org/guides/>, free. – Title from the screen. – Language: English.

- 14 Chen, P. The Entity-Relationship Model – Towards a Unified Data Representation / P. Chen // DBMS. – 1995. – No. 3. – pp. 4–13.
- 15 Barker, R. CASE Methodology. Modeling Entity-Relationship Relationships / R. Barker. – Moscow: International Center for Financial and Economic Development, 1993. – 216 p.
- 16 McConnell, S. Perfect Code. Master Class / S. McConnell. – Moscow: Symbol-Plus, 2005. – 896 p.
- 17 Myers, G. J. The Art of Software Testing / G. J. Myers, T. Badgett, T. M. Thomas. – 3rd ed. – Hoboken: John Wiley & Sons, 2011. – 256 p.
- 18 Vershina, G. A. Labor Protection: Textbook / G. A. Vershina, A. M. Lazarenkov. – Minsk: Information Technologies Center of the Ministry of Finance, 2020. – 564 p.
- 19 Lazarenkov, A. M. Labor Protection. A textbook and practical guide to labor protection calculations: an electronic guide / A. M. Lazarenkov, T. P. Kot, E. V. Mordik, L. P. Filyanovich. - Minsk: BNTU, 2018. - 11.7 conventional electronic pages.
- 20 Lazarenkov, A. M. Fire Safety: a textbook on the discipline "Labor Protection": an electronic publication / A. M. Lazarenkov, Yu. N. Fasevich. - Minsk: BNTU, 2019. - 14.5 conventional electronic pages.
- 21 Duckett, D. HTML and CSS. Website Development and Design / D. Duckett. - Moscow: Eksmo, 2012. - 480 p. : ill. - Russian language.
- 22 Flanagan, D. JavaScript. Detailed guide / D. Flanagan. – 6th ed. – M.: Symbol-Plus, 2012. – 1168 p. - Yaz. rus.
- 23 H2 Database Engine [Electronic resource] / H2 Group. - Electron. Dan. – Access mode: <https://www.h2database.com/html/main.html>, free. - Cap. from the screen. - Yaz. English
- 24 Lombok [Electronic resource] / Project Lombok. - Electron. Dan. – Access mode: <https://projectlombok.org/features/>, free. - Cap. from the screen. - Yaz. English
- 25 Weisfeld, M. Object-oriented thinking / M. Weisfeld. – M.: liters, 2014. – 288 p. - Yaz. rus.
- 26 Golovach, V. V. HTML5 and CSS3. Web Development by New Generation Standards / V. V. Golovach, Yu. V. Kovalenko. – Donetsk: GLAGOL, 2012. – 736 p.: ill. – Russian language.
- 27 Prokhorenok, N. A. HTML, JavaScript, PHP, and MySQL. Webmaster's Gentleman's Kit / N. A. Prokhorenok, V. A. Dronov. – 5th ed., revised and enlarged. – St. Petersburg: BHV-Petersburg, 2019. – 480 p.: ill. – Russian language.