МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Новоуральский технологический институт –
филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»
(НТИ НИЯУ МИФИ)
Колледж НТИ

Цикловая методическая комиссия информационных технологий

ОТЧЕТ №9
ПО ПРАКТИЧЕСКОМУ ЗАНЯТИЮ НА ТЕМУ

«ПРОЦЕДУРА АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ НА ОСНОВЕ ПАРОЛЯ»

ПМ.05 «Разработка программного обеспечения компьютерных сетей»
МДК.05.01 «Защита информации в КС»

Специальность СПО 09.02.03
«Программирование в компьютерных системах»

очная форма обучения
на базе основного общего образования

Выполнил
студент группы КПР–47 Д
Егорушкин И.А. _____11.12.2020_____ _____
дата подпись

Проверил
преподаватель _____ _____
Горницкая И.И. дата подпись

Новоуральск 2020

Цель работы: Анализ рисков информационной безопасности

Оборудование:

AMD Ryzen 5 3550U

ОЗУ 8 Гб

Программное обеспечение:

Windows 10 Professional 64 бит;

Ход работы:

Работа была поделена на несколько этапов.

1. Изучение материла
2. Анализ задания
3. Выполнение задания

В ходе изучения материла были выявлены основные задачи шифрации и типы.

В выполнение был выбран язык Java на основе Фреймворка Spring Boot.
Проект должен иметь следующие требования:

Кириллица (строчные буквы) При смене пароля: проверка на совпадение пароля с именем пользователя (если используется идентификационный номер, то в системе должны храниться имена каждого пользователя)

В качестве информационного ресурса использовать любой файл или приложение. 2. Доступ к ресурсу должен быть разрешен только санкционированным пользователям. Для этого в программе должны храниться имена пользователей и их пароли. При попытке доступа пользователя к ресурсу проверяется наличие его идентификатора (имени) в системе и соответствие введенного пароля паролю, который хранится в системе. 3. В системе должна храниться следующая информация о пользователе: ID или имя пользователя, пароль, ФИО, дата рождения, место рождения (город) номер телефона. 4. Пользователь должен иметь возможность поменять пароль (ограничения: см. вариант).

Вывод: В ходже работы были изучены методы авторизация по форме логин пароль.