Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет: Факультет информационных технологий  
Кафедра «Информационная безопасность»

Направление подготовки/ специальность: 10.05.03 Информационная безопасность автоматизированных систем

ОТЧЕТ

по проектной практике

Студент: Ильин Владимир Андреевич Группа: 241-372

Место прохождения практики: Московский Политех, кафедра «Информационная безопасность»

Отчет принят с оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Дата \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель практики: Гневшев Александр Юрьевич

Москва 2025

ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ 3](#_Toc139386418)

[1. Общая информация о проекте 5](#_Toc139386418)

[2. Общая характеристика деятельности организации 7](#_Toc139386418)

[3. Описание задания по проектной практике 9](#_Toc139386419)

[3.1 Общая информация о цифровой централизованной валюте (CBDC) 9](#_Toc139386420)

[3.2 Преимущества цифровой централизованой валюты 10](#_Toc139386421)

[3.3 Основные вызовы и риски внедрения CBDC 11](#_Toc139386422)

[3.4 Внедрение CBDC в мировой экономике:международный опыт 12](#_Toc139386422)

[3.5 Влияние цифровой валюты на граждан и экономику 13](#_Toc139386422)

[3.6 Особенности различных парольных политик 14](#_Toc139386422)

[3.7 Анализ уязвимостей текущих паролей 15](#_Toc139386422)

[3.8 Рекомендации по совершенствованию парольных политик 16](#_Toc139386422)

[4. Описание достугнутых результатов по проектной практике 18](#_Toc139386423)

[4.1 Общие задачи и результаты 18](#_Toc139386421)

[4.2. Посты на тему внедрения центральной цифровой валюты (CBDC) в различных странах и оценке ее влияния на экономику и повседневную жизнь 24](#_Toc139386424)

[4.3 Демонстрация кода на C++, который проверяет пароль на требования сервиса и дает рекомандации 33](#_Toc139386422)

[ВЫВОД 36](#_Toc139386425)

[СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 37](#_Toc139386426)

# ВВЕДЕНИЕ

Учебная практика по теме «Комплексное исследование цифровой централизованной валюты (CBDC) и политики информационной безопасности паролей: анализ преимуществ, вызовов, уязвимостей и разработка рекомендаций» выполнена Ильином Владимиром Андреевичем, ст. гр. 241-372. Практика включает изучение принципов работы CBDC, их влияния на экономику и общество, а также анализ требований к паролям в популярных сервисах с точки зрения информационной безопасности.

Цель учебной практики – получить новые знания и практические навыки в области цифровых валют и информационной безопасности, изучив CBDC и политики паролей, а также продемонстрировать их применение.

Для достижения поставленной цели поставлены и решены следующие задачи:

1. изучение предметной области цифровых централизованных валют (CBDC) и парольных политик;
2. разработать несколько информационных постов по теме CBDC

3) поиск и анализ теоретических источников по выбранным темам;

4) изучение технической документации и международных стандартов (NIST SP 800-63B, ISO/IEC 27001, FIDO);

5) анализ требований к паролям в популярных сервисах (Gmail, Telegram, Госуслуги, Яндекс Почта, Авито, Сбербанк Онлайн) и выявление уязвимостей;

6) разработка рекомендаций по созданию надежных паролей и использованию современных методов защиты;

7) практическая демонстрация навыков управления проектами через установку и настройку Linux-системы

8) создание программы на языке C++, которая проверяет введенный пароль на соответствие требованиям рассмотренных сервисов, и рекомендует изменения (корректировки в соответствии с современным международными стандартами)

Объектами исследования являются цифровая централизованная валюта (CBDC) и политики информационной безопасности паролей в популярных сервисах.

# Общая информация о проекте

Название проекта: CBDC и Парольные политики: анализ и практика

Цели и задачи проекта: Этот проект посвящён цифровым валютам центральных банков (CBDC), анализу их преимуществ и вызовов, а также сравнительному анализу требований к паролям популярных сервисов.

Изучение CBDC:

Цель практики:

Разработать контент, который освещает ключевые аспекты цифровой централизованной валюты (CBDC), включая её преимущества, вызовы и примеры внедрения в разных странах. Кроме того, практикой ставились задачи изучения влияния цифровой валюты на экономику и повседневную жизнь граждан, а также анализ популярности и степени принятия CBDC.

Задачи практики:

Исследовать цифровые наличные (CBDC) и их принцип работы, включая теоретические и практические аспекты.

Изучить преимущества и недостатки цифровой валюты, сравнить с традиционной валютой и другими электронными платежными системами.

Проанализировать влияние цифровой валюты на граждан и экономику в разных странах.

Разработать несколько информационных постов по теме CBDC, предоставляющих актуальную и полезную информацию.

Установить и изучить проект Plane для управления проектами, выбрать оптимальный способ установки, осуществить развертывание и провести тестирование.

Провести установку и настройку Linux-системы для последующего развёртывания инструментов.

Парольные политики:

Цели и задачи практики

Целью практики является детальный анализ требований к паролям в популярных сервисах с целью оценки их безопасности и соответствия современным международным стандартам, а также подготовка рекомендаций для пользователей по созданию надежных паролей.

Основные задачи:

Проанализировать требования к паролям в 5-10 популярных сервисах (Gmail, Telegram, Госуслуги, Яндекс Почта, Авито, Сбербанк Онлайн и др.).

Проверить соответствие этих требований современным стандартам безопасности паролей, например, NIST SP 800-63B.

Выявить потенциальные уязвимости, такие как ограничения максимальной длины пароля, использование простых паролей или недостатки в проверках.

Составить краткое руководство с рекомендациями по созданию надежных паролей для пользователей.

# Общая характеристика деятельности организации

**Наименование заказчика**

Федеральное государственное автономное образовательное учреждение высшего образования «Московский политехнический университет» (Московский Политех).

**Область деятельности университета**

Московский Политех осуществляет подготовку специалистов в технических и IT-направлениях, реализует проекты в сфере цифровых технологий и информационной безопасности, регулярно организует образовательные мероприятия с участием экспертов и практиков отрасли.

**Описание взаимодействия с заказчиком в рамках проектной деятельности**

В рамках курса «Введение в специальность» мой вуз выступал не только заказчиком, но и образовательной площадкой для формирования ключевых компетенций, используемых далее в проектной работе по темам:

— «Изучение и анализ цифровой централизованной валюты (CBDC): преимущества, вызовы и внедрение в мировой экономике»

— «Сравнение парольных политик: анализ уязвимостей и рекомендации»

Взаимодействие включало участие в специальных лекциях, встречах с приглашёнными экспертами и работе с опытными студентами-старшекурсниками. Особенно значимый вклад в развитие моих компетенций и формирование концепции проектных исследований внесли следующие мероприятия:

- Лекция по низкоуровневой безопасности с директором по информационной безопасности (03.04.2025). Ключевые выводы были использованы при анализе угроз для инфраструктуры CBDC и оценки стойкости реализованных политик аутентификации.

- Лекция об основных понятиях информационной безопасности с экспертом практиком отрасли (10.04.2025). Полученные знания применялись при формировании разделов о моделях угроз и анализе устойчивости различных парольных политик.

- Встреча со старшекурсниками (06.05.2025). Практическая часть позволила получить реальные советы по подготовке исследовательских работ и структурировать ход проектной деятельности.

Затраченное время 3-4 часа

**Влияние организации-заказчика на практическую часть проектов**

Благодаря курируемым Московским Политехом занятиям я получил системное представление об угрозах цифровым финансовым платформам, особенностях внедрения международных стандартов ИБ, а также прямую экспертизу по вопросам управления паролями и политики безопасности. Это позволило сформировать обоснованные предложения по совершенствованию защищённости цифровых валют (CBDC) и выработать рекомендации для оптимизации IT-инфраструктуры с точки зрения аутентификации пользователей.

**Вывод**

Таким образом, Московский Политех не только выступил заказчиком, но и обеспечил площадку для глубокого погружения в проблематику информационной безопасности, что существенно усилило прикладную и исследовательскую ценность выполненных проектов

# 3. Описание задания по проектной практике

3.1 Общая информация о цифровой централизованной валюте (CBDC)

Цифровая централизованная валюта (CBDC) представляет собой цифровую форму национальной валюты, выпускаемую центральным банком страны и поддерживаемую государственным финансовым регулятором. CBDC сочетает в себе преимущества наличных денег и цифровых технологий, обеспечивая безопасность, удобство и контроль над денежными потоками в цифровом пространстве. В отличие от криптовалют с децентрализованной природой, CBDC централизована и подконтрольна государству.

Основные особенности CBDC включают возможность осуществления анонимных и безопасных транзакций, повышение эффективности платежных систем и снижение издержек на выпуск и обращение наличных денег. Технологической базой для CBDC часто выступает блокчейн или другие распределённые реестры, обеспечивающие прозрачность и защищенность данных.

3.2 Преимущества цифровой централизованной валюты

Преимущества внедрения CBDC можно выделить следующим образом:

* **Повышение эффективности платежных систем:** цифровая валюта обеспечивает более быстрые и дешевые платежи, уменьшает транзакционные издержки.
* **Улучшение финансовой инклюзии:** CBDC предоставляет доступ к денежным средствам людям без банковских счетов и в регионах с недостаточно развитой инфраструктурой.
* **Прозрачность и борьба с нелегальными операциями:** централизованный контроль позволяет улучшить отслеживание транзакций и снизить уровень мошенничества и уклонения от налогов.
* **Повышение контроля над денежной массой:** центральные банки получают более точные инструменты управления денежной политикой и ликвидностью.
* **Снижение затрат на выпуск и обслуживание физических денежных знаков.**

3.3 Основные вызовы и риски внедрения CBDC

Внедрение цифровой валюты сопряжено с рядом вызовов:

* **Защита персональных данных и обеспечение конфиденциальности:** сохранение баланса между прозрачностью транзакций и правом на анонимность.
* **Кибербезопасность:** необходимость противостояния возможным хакерским атакам и техническим уязвимостям.
* **Техническая инфраструктура:** создание стабильных и масштабируемых систем, способных обслуживать массовые пользовательские запросы.
* **Воздействие на банковскую систему:** потенциальное сокращение роли коммерческих банков и изменение модели кредитования.
* **Регулятивные и правовые вопросы:** адаптация законодательства и обеспечение международной совместимости.

3.4 Внедрение CBDC в мировой экономике: международный опыт

Многие страны уже сейчас экспериментируют с цифровыми валютами центральных банков. Китай стал одним из лидеров в разработке и запуске цифрового юаня, что способствует ускорению безналичных расчетов и усилению контроля государственной монетарной политики. Европейский центральный банк изучает возможности выпуска цифрового евро, фокусируясь на вопросах конфиденциальности и устойчивости системы. Другие страны, такие как Швеция, Багамы и Япония, проводят пилотные проекты, оценивая влияние CBDC на экономику и финансовый сектор.

3.5 Влияние цифровой валюты на граждан и экономику

CBDC может значительно повлиять на повседневную жизнь граждан, упрощая доступ к финансовым услугам, снижая риски хранения наличных средств и расширяя возможности онлайн-торговли. Однако существует и социальное сопротивление переходу на цифровые формы денег из-за опасений по поводу контроля государства и утраты приватности.

На уровне экономики внедрение CBDC способствует повышению прозрачности финансовых потоков, уменьшает коррупцию и способствует более эффективному управлению денежной массой. Тем не менее, необходимо учитывать возможные негативные последствия, такие как усиление цифрового неравенства и технические риски.

3.6 Особенности различных парольных политик

В современных популярных сервисах реализованы различные требования к паролям, которые призваны повысить уровень безопасности учетных записей пользователей. При этом зачастую политики отличаются количеством разрешенных символов, наличием правил по сложности, а также поддержкой двухфакторной аутентификации (2FA).

Ключевые особенности некоторых популярных сервисов:

* **Сбербанк Онлайн** требует длину пароля 8–30 символов с обязательным наличием заглавных и строчных букв, цифр, запретом на использование только букв или только цифр, а также исключением последовательностей и личных данных.
* **Яндекс Почта** минимально требует длину пароля 6 символов, использование латиницы, а также рекомендует добавление цифр и специальных символов.
* **Авито** устанавливает обязательное условие не менее 8 символов с запретом легких последовательностей (например, «abc», «123») и использования простых слов, а также ограничивает повторения символов.
* **Gmail** требует минимум 8 символов, допускает использование латиницы, цифр и знаков пунктуации, запрещает известные простые пароли и поддерживает 2FA (включая аппаратные ключи).
* **Telegram** предоставляет пользователям свободу в выборе пароля без строгих правил по составу, разрешает любые символы и 2FA через SMS, e-mail и дополнительные коды.

3.7 Анализ уязвимостей текущих политик

Несмотря на наличие ряда защитных мер, в анализируемых политиках обнаружены потенциальные слабости:

* Жесткие требования к составу пароля (обязательное использование заглавных, строчных букв, цифр) противоречат современным рекомендациям NIST SP 800-63B, которые рекомендуют акцентировать внимание на длине пароля и отказе от навязывания сложных требований.
* Некоторые сервисы ограничивают использование символов латиницей, не поддерживая полный набор Unicode (например, кириллицу), что снижает потенциальное разнообразие паролей.
* Отсутствие или ограниченная поддержка двухфакторной аутентификации с современными методами (например, аппаратными ключами) в некоторых сервисах увеличивает риск компрометации.
* Отсутствие проверки паролей на наличие в базах скомпрометированных паролей (утечках) у Telegram и некоторых других сервисов.
* Частое применение 2FA через SMS несет определенные риски, связанные с возможностью перехвата сообщений.
* Отсутствие максимальной длины пароля или установление слишком низкого предела (NIST рекомендует минимум 64 символа) ограничивает возможности пользователей создавать достаточно длинные и устойчивые пароли.

3.8 Рекомендации по совершенствованию парольных политик

Основываясь на стандартах безопасности (в частности NIST SP 800-63B) и выявленных уязвимостях, можно сформулировать следующие рекомендации:

1. **Сосредотачиваться на длине пароля**, предлагая минимум 12 символов или больше, вместо жестких требований по составу (где сложно соблюдать заглавные, строчные буквы, цифры и спецсимволы).
2. **Разрешать использование любых символов Unicode**, включая кириллицу и другие алфавиты, что расширит пространство паролей и повысит их стойкость.
3. **Внедрять проверку паролей по базам скомпрометированных паролей** для быстрого выявления слабых или утекших паролей.
4. **Обеспечить поддержку современных методов двухфакторной аутентификации**, включая аппаратные ключи (FIDO, U2F) и отказ от SMS, либо дополнительно информировать пользователей о безопасности 2FA.
5. **Устанавливать адекватные ограничения по максимальной длине пароля (не менее 64 символов)**, чтобы не ограничивать возможность использования длинных фраз.
6. **Отказаться от жестких ограничений на последовательности и повторяющиеся символы**, если вместо этого реализована проверка на слабые паттерны и утечки.
7. **Рекомендовать пользователям использование менеджеров паролей** для генерации и хранения сложных и длинных паролей.
8. **Растить осведомленность пользователей** о регулярном обновлении паролей и осторожности при использовании подозрительных ссылок и кодов из сообщений.

# 4. Описание достигнутых результатов по проектной практике

4.1 Общие задачи и результаты

Задача 1

Изучить цифровые наличные, чтобы понять их принцип действия. Цифровые наличные представляют собой форму валюты, которая комбинирует преимущества наличных и криптовалют, предоставляя возможность осуществления анонимных и безопасных транзакций в цифровом пространстве.

Что сделал

1. Теоретическая часть

- Ознакомился с основными принципами работы цифровых наличных, включая их архитектуру, безопасность и технологические аспекты.

- Проанализировал существующие модели цифровых наличных, такие как Digicash и современные аналогии.

2. Практическая часть

- Познакомился с ключевыми технологиями, такими как блокчейн, которые лежат в основе функционирования цифровых наличных.

- Провел анализ преимуществ и недостатков цифровых наличных по сравнению с традиционными формами валюты и другими электронными платежными системами.

Затраченное время: 4-6 часов

Задача 2

Установить Linux и провести настройку системы для последующего развертывания необходимых инструментов.

Что сделано

1. Установка Linux

- Выбрана оптимальная версия дистрибутива на основе требований и задачи.

- Загружен установочный образ и подготовлен носитель для установки системы.

- Успешно произведена установка Linux на выбранное оборудование.

2. Базовая настройка системы

- Установлены все обновления и исправления безопасности.

- Настроены пользовательские учетные записи и права доступа.

- Установлены базовые утилиты и инструменты, необходимые для дальнейшей работы.

3. Подготовка окружения

- Проведена оптимизация системы для стабильной работы.

- Настроена сеть и подключение к интернету.

- Проверена готовность системы для последующего развертывания ПО.

Затраченное время: 3-5 часов

Задача 3

Изучить концепцию цифрового рубля с целью понимания его потенциала и влияния на экономику. Цифровой рубль — это новый механизм от Центрального банка России, который призван обеспечить более безопасные, быстрые и эффективные транзакции в цифровой форме.

Что сделал

1. Теоретическая часть

- Изучил основные характеристики цифрового рубля, его отличия от традиционного и электронного рубля, а также его место среди других цифровых валют.

- Ознакомился с ключевыми документами и стратегиями Центробанка России, касающимися внедрения цифрового рубля.

- Проанализировал международный опыт внедрения цифровых валют центрального банка (CBDC) аналогичные проекты.

2. Практическая часть

- Провел SWOT-анализ цифрового рубля, выявив его сильные и слабые стороны, а также возможности и угрозы для российской экономики.

- Изучил возможные законодательные изменения, которые могут потребоваться для успешной интеграции цифрового рубля.

Затраченное время: 3-6 часов

Задача 4

Установить и изучить проект Plane с целью определить его возможности и преимущества для управления проектами.

Что сделано:

1. Выбор способа установки

- Рассмотрены два варианта установки: через Plane Cloud и самостоятельная установка.

- Для получения полного контроля над данными и инфраструктурой выбран вариант самостоятельной установки.

2. Установка Plane

- Настроено серверное окружение и подготовлена инфраструктура для установки.

- Следуя документации по установке, произведено развертывание Plane на собственных серверах.

- Проведены тесты, удостоверившись в успешной установке и работоспособности системы.

3. Изучение интерфейса и функционала

- Проведена настройка пользовательских интерфейсов.

- Изучены ключевые функции: трекинг задач, управление спринтами, трекинг времени, управление знаниями.

- Особое внимание уделено возможностям аналитики и отчетности для отслеживания прогресса проектов.

Затраченное время: 10-11 часов

Задача 5

Рассмотреть задание «Сравнение парольных политик: анализ уязвимостей и рекомендации» по учебной практике

Достигнутые результаты:

* Проанализированы требования к паролям в популярных сервисах (например, Госуслуги, Авито, Яндекс Почта):
* Была произведена проверка на соответствие современным международным стандартам (например, NIST SP 800-63B):
* Выявлены потенциальные слабые места
* Составлено краткое руководство с рекомендациями для пользователей
* Была составлена программа на C++, которая проверяет введенный пароль на соответствие требованиям рассмотренных сервисов, и рекомендует изменения (корректировки в соответствии с современным международными стандартами)

[Программа на C++](https://github.com/hudmudbbb/-project-practice/blob/dev/src/main.cpp)

В ходе анализа были сопоставлены требования к паролям в популярных сервисах (Gmail, Telegram, Госуслуги, Яндекс Почта, Авито, Сбербанк Онлайн). Большинство сервисов устанавливают минимальную длину от 8 символов и требуют разнообразие символов, внедряют запреты на простые пароли и рекомендуют двухфакторную аутентификацию. Некоторые поддерживают длинные пароли и Unicode.

Однако остаются уязвимости: в некоторых сервисах минимальная длина всё ещё низкая, есть ограничения на максимальную длину, а требования к разнообразию символов и современным методам защиты не всегда достаточно жёсткие.

Даны рекомендации по использованию сложных уникальных паролей, менеджеров паролей и двухфакторной аутентификации.

Большинство сервисов реализуют актуальные требования к безопасности паролей, но отдельные недоработки сохраняются. Для надёжной защиты аккаунтов рекомендуется использовать длинные уникальные пароли, дополнительные меры безопасности и следовать советам экспертов и стандартов.

Затраченное время: 15-20 часов

Задача 6

Сделать сайт по CBDC и вариативной части (Сравнение парольных политик)

Выполнено:  
Был создан сайт о CBDC и о вариативной части, а также прикреплены общие результаты работы

[Сайт CBDC и Парольные политики: анализ и практика](file:///C:\Gtihub_local\-project-practice\site\index.html)

Затраченное время: 13-15 часов

4.2. Посты на тему внедрения центральной цифровой валюты (CBDC) в различных странах и оценке ее влияния на экономику и повседневную жизнь граждан

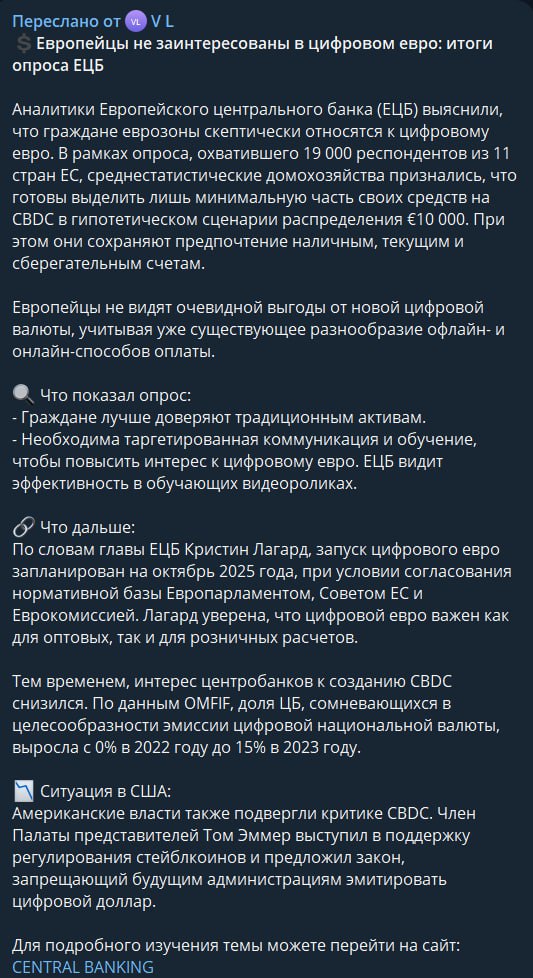


Рис. 1. Пост №1

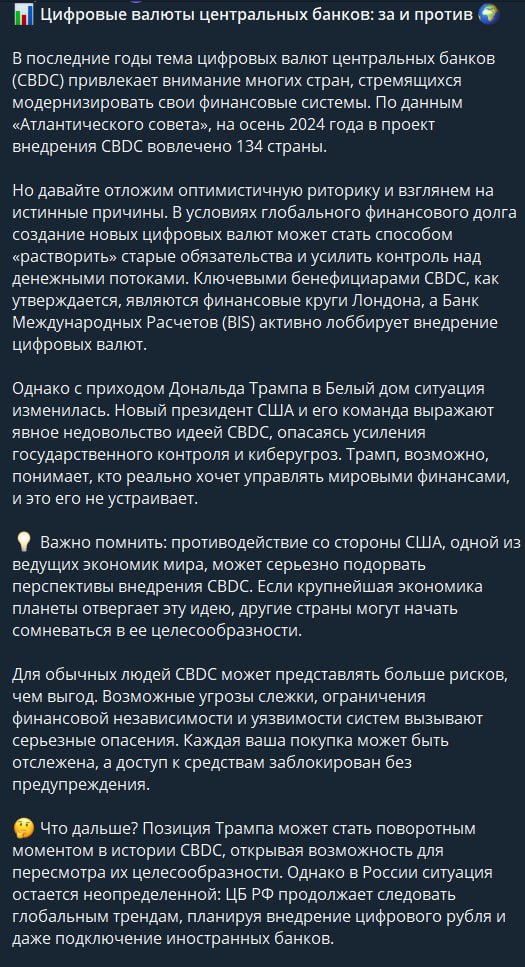


Рис. 2. Пост №2



Рис. 3. Пост №2 часть 2

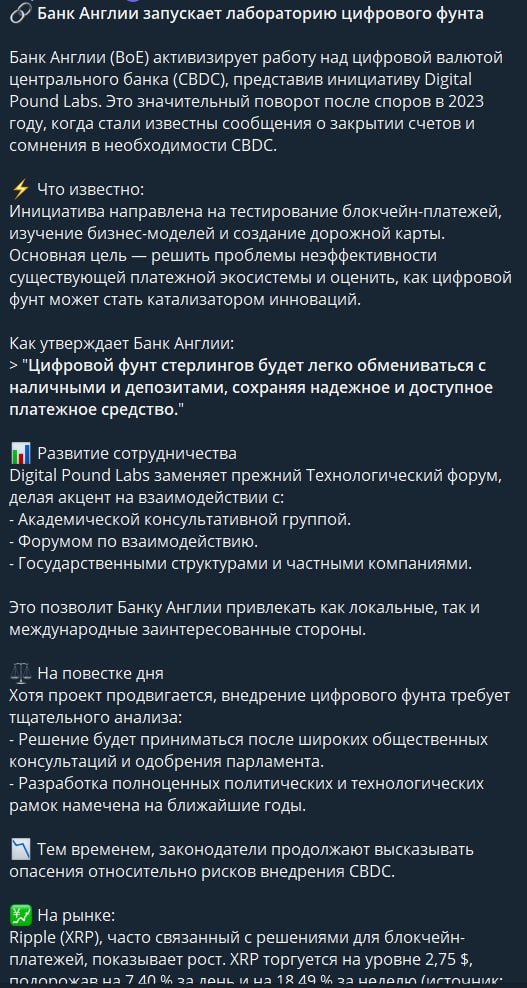


Рис. 4. Пост №3

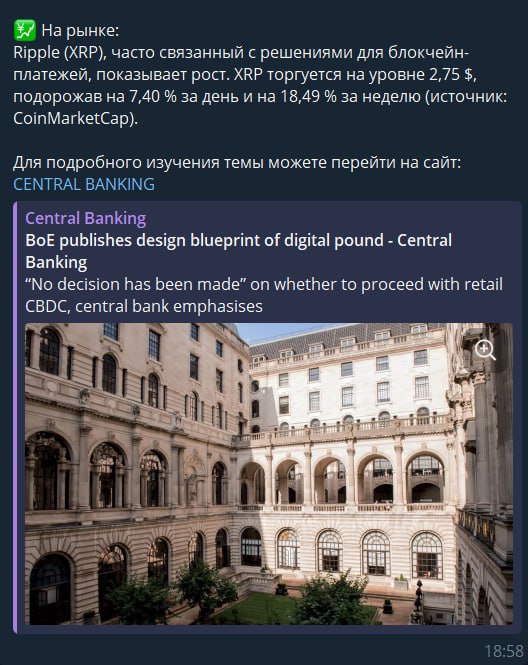


Рис. 5. Пост №3 часть 2

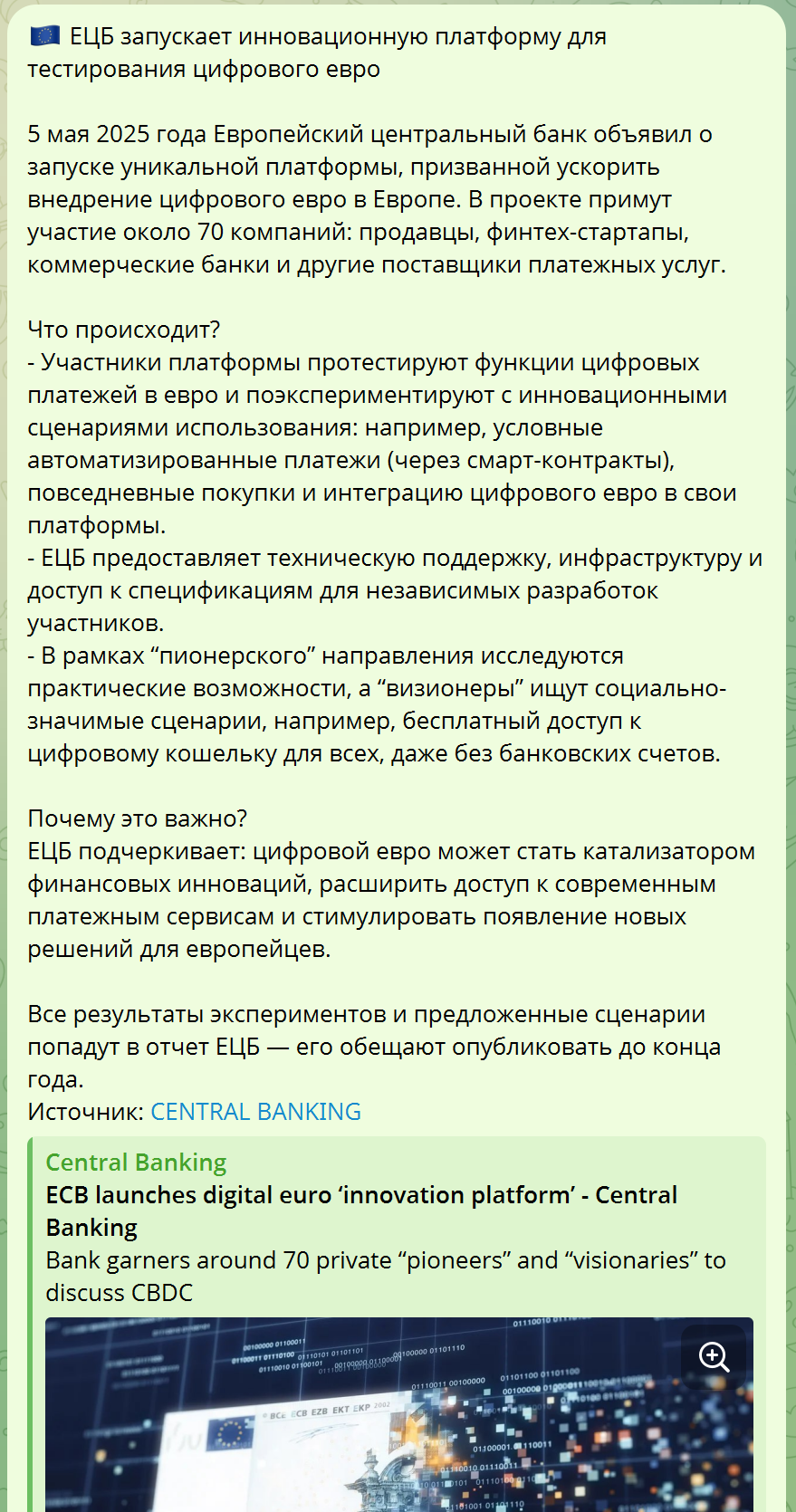


Рис. 6. Пост №4



Рис. 7. Пост №5

Практическая часть отчета посвящена анализу внедрения центральной цифровой валюты (CBDC) в различных странах и оценке ее влияния на экономику и повседневную жизнь граждан. В ходе работы были рассмотрены примеры реализации CBDC в таких странах, как Китай (цифровой юань), Багамские острова (Sand Dollar), Швеция (e-крона) и Нигерия (e-Naira). Эти кейсы позволили оценить реальные преимущества и вызовы, с которыми сталкиваются государства при переходе к цифровым валютам.

В частности, изучение показало, что внедрение CBDC способно повысить прозрачность финансовых операций, снизить уровень финансовых преступлений, а также обеспечить более быстрые и дешевые платежи внутри страны и за ее пределами. Существенное значение имеет и то, что CBDC способствует финансовой инклюзии, что особенно актуально для развивающихся стран, где значительная часть населения ранее не имела доступа к банковским услугам.

Однако во всех случаях отмечаются и определённые сложности. Одним из главных вызовов является обеспечение безопасности данных и защита личной информации граждан. Кроме того, многие жители выражают обеспокоенность по поводу возможного контроля со стороны государства, а также сложностей с освоением новых технологий, особенно среди старшего поколения. В странах с относительно устойчивым банковским сектором отмечается и сопротивление со стороны коммерческих банков, которые опасаются потерь части прибыли и риска оттока средств из их системы.

На практике влияние CBDC на экономику страны зависит от особенностей финансовой системы и степени цифровизации общества. В Китае цифровой юань активно интегрируется в городах, государство организует программы поощрения использования новой валюты, что постепенно расширяет аудиторию пользователей. В то же время, в ряде европейских стран процесс внедрения идет медленнее, что связано с более высокой стабильностью традиционной банковской инфраструктуры и наличием альтернативных цифровых инструментов оплаты.

Исследование выявило, что популярность CBDC будет постепенно расти, но массовый переход на цифровую валюту сдерживает не только отсутствие полной доверенности со стороны граждан, но и привычка пользоваться наличностью и уже существующими электронными средствами оплаты. Люди опасаются утраты анонимности при транзакциях, а также не до конца уверены в надежности цифровых платформ центральных банков.

В целом, опыт разных государств показывает, что успех внедрения CBDC зависит не только от технологических и финансовых аспектов, но и от активной информационной работы с населением, обеспечения безопасности и стимулирования использования новой формы денег в повседневной жизни.

Затраченное время: 13-14 часов

4.3. Демонстрация работы кода на C++, который проверяет пароль на требования сервиса и дает рекомендации

Запустим код, нам дается выбрать сервис, для которого мы хотим придумать пароль

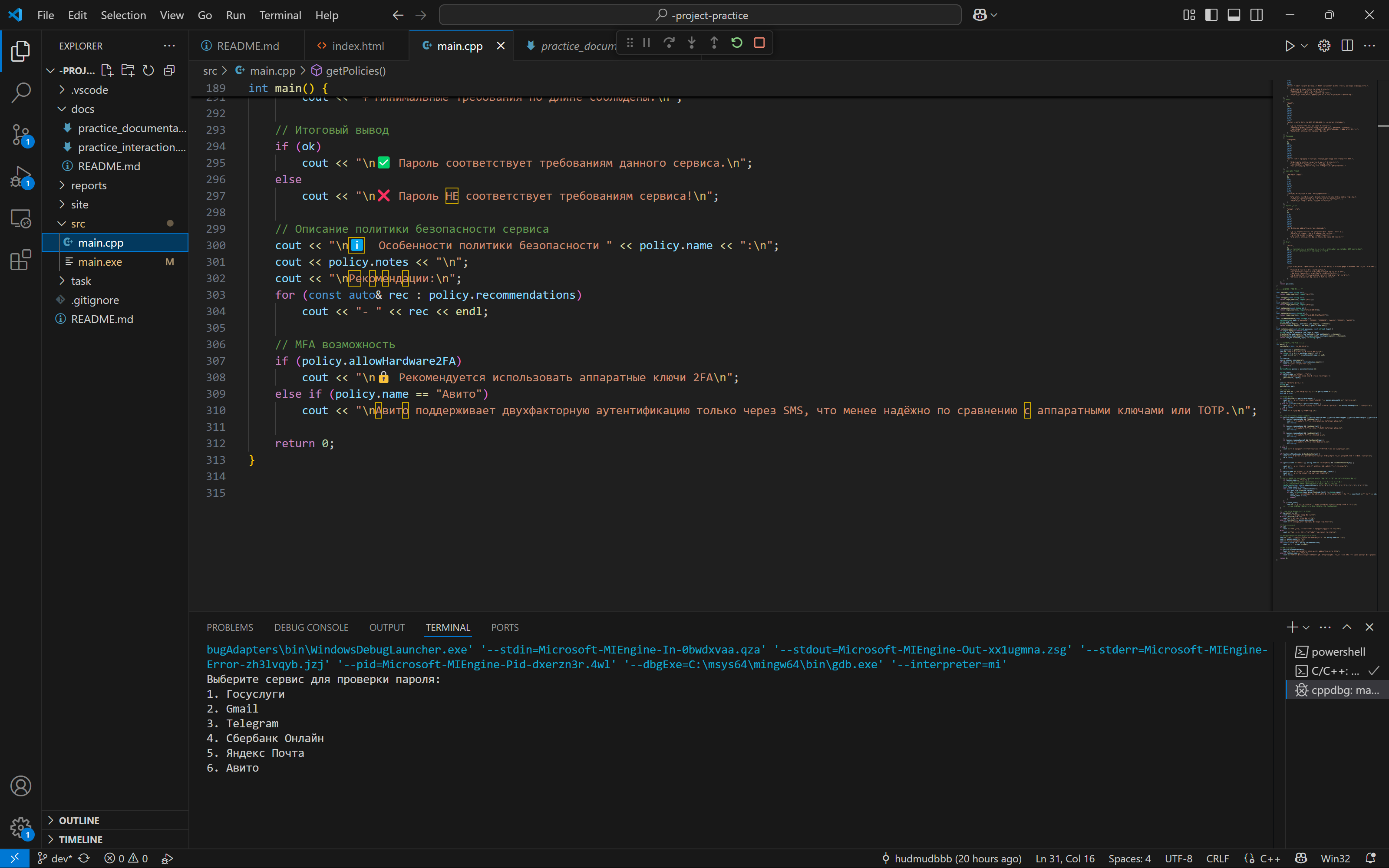


Рис. 8. Запуск программы

Выбираем Telegram и вводим пароль

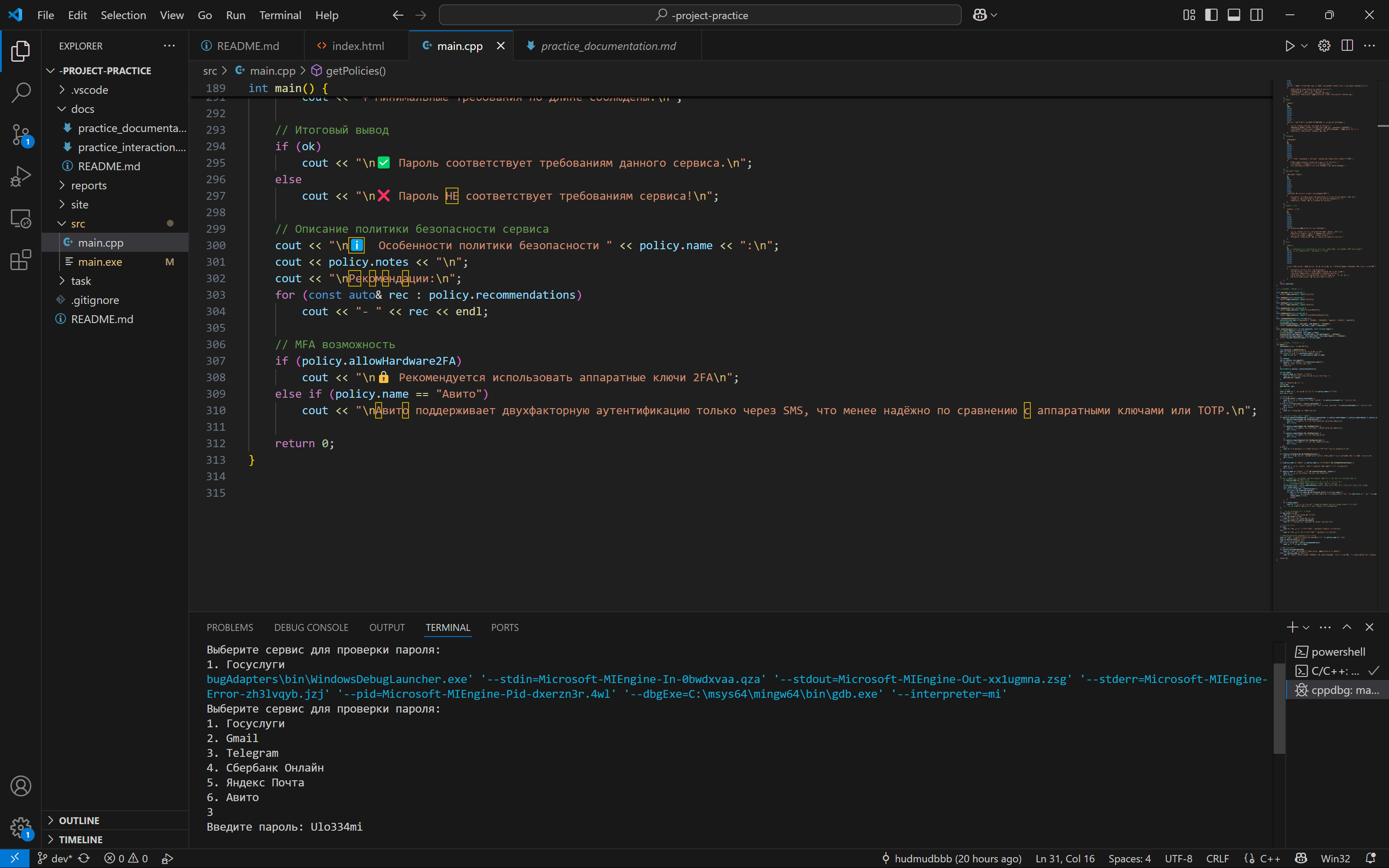


Рис. 9. Демонстрация выбранного сервиса и введенного пароля

Теперь смотрим результат: соответствует ли данный пароль требованиям и какие корректировки лучше внести.

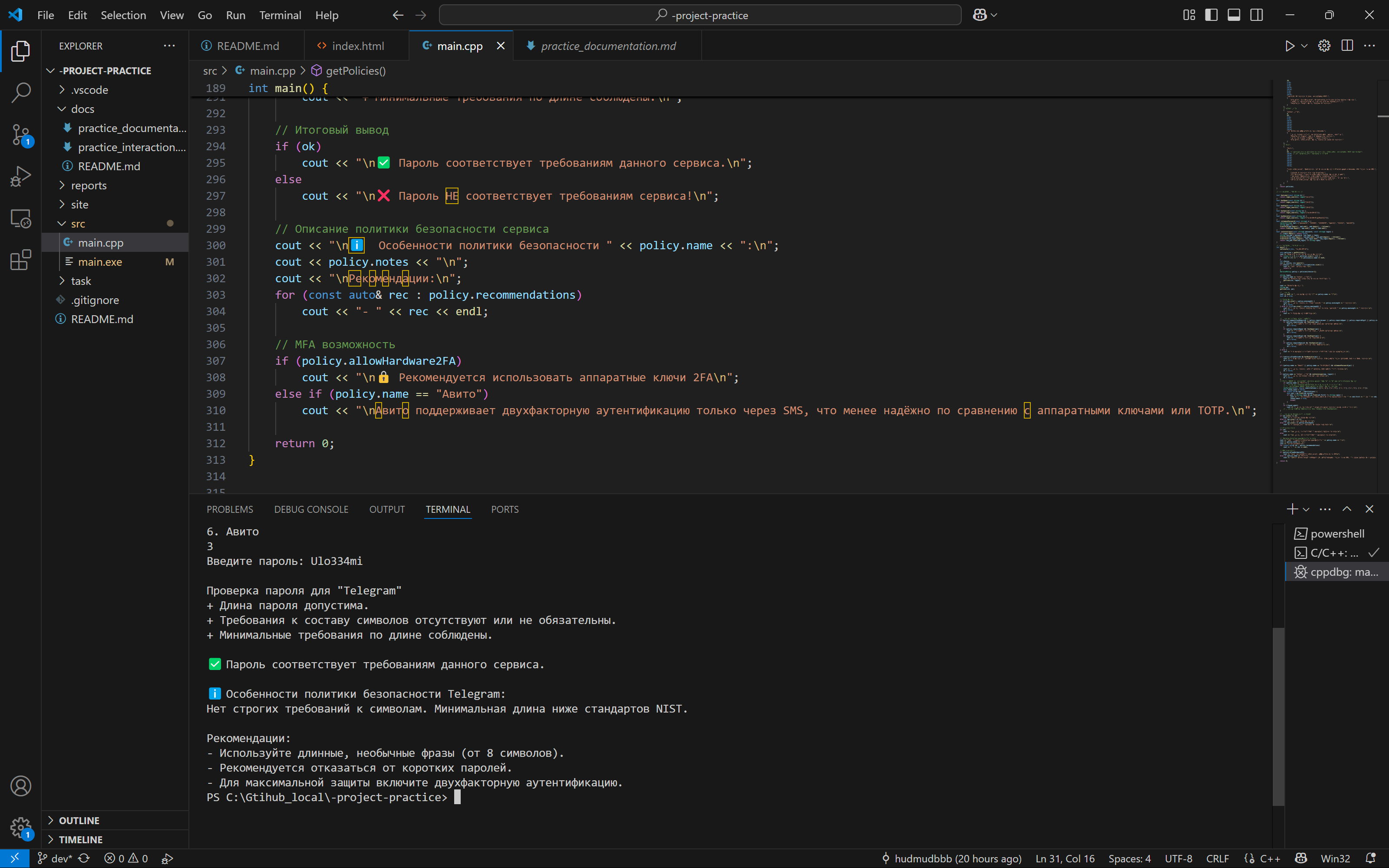


Рис. 10. Демонстрация соответствия требованиям пароля и рекомендаций

Пароль соответствует требованиям, и мы видим рекомендации. Теперь введем пароль не соответствующий требованиям сервиса.

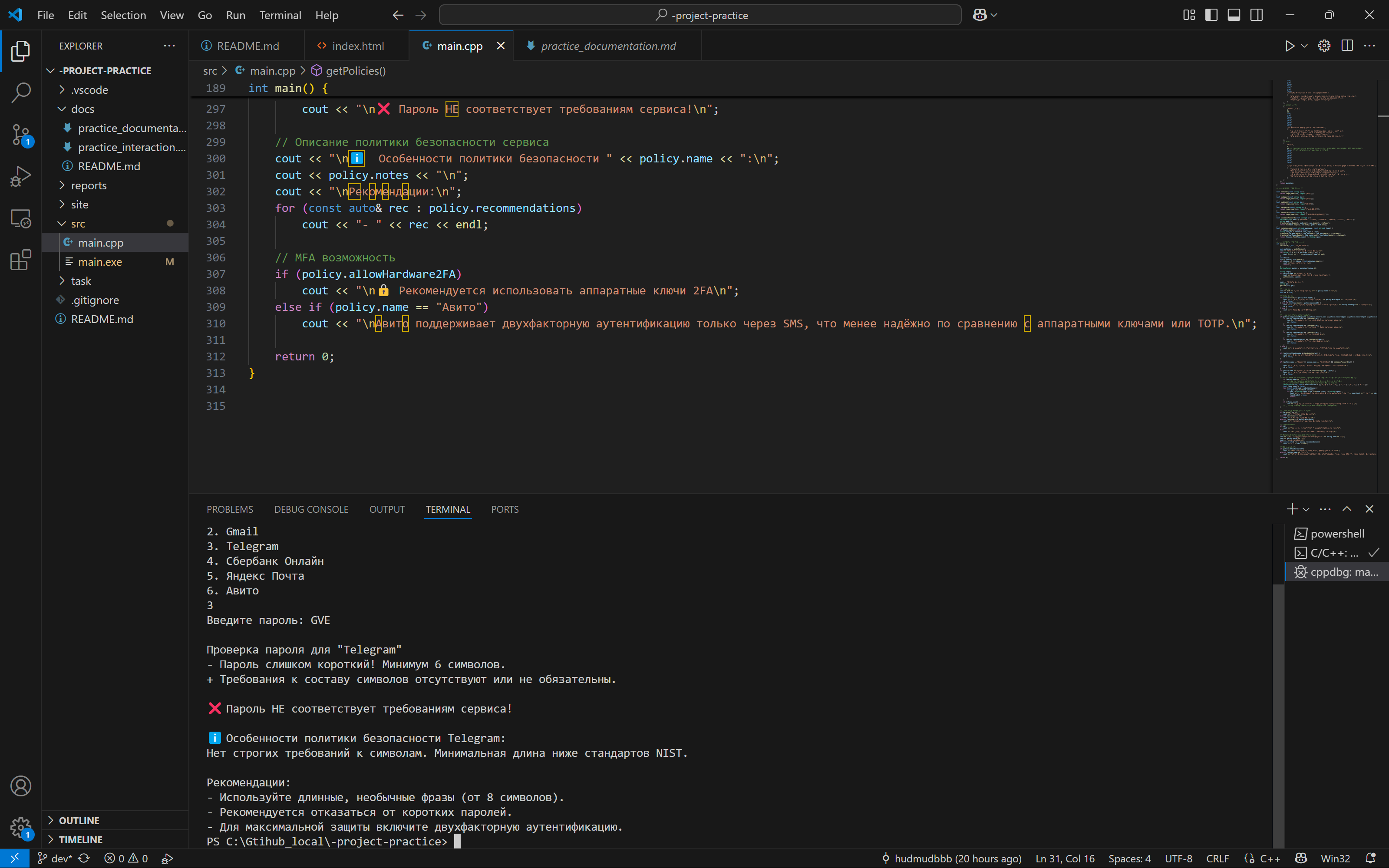


Рис. 11. Демонстрация несоответствия требованиям введенного пароля

Таким образом, созданный инструмент позволяет не только автоматизировать процесс проверки и укрепления паролей, но и способствует распространению современных стандартов информационной безопасности среди широкой аудитории. Подобный подход особенно актуален в условиях роста числа киберугроз, когда даже простая рекомендация по корректировке пароля может существенно снизить риски несанкционированного доступа к персональным данным.

Затраченное время: 6-7 часов

# ВЫВОД

В ходе выполнения данного комплексного исследования цифровой централизованной валюты (CBDC) и политики информационной безопасности паролей, мне удалось получить всесторонние знания о сущности и принципах работы CBDC, а также изучить ключевые преимущества, вызовы и риски, связанные с ее внедрением в мировой экономике. Были подробно проанализированы международный опыт применения цифровой валюты, ее влияние на граждан и экономику, что позволило сформировать целостное понимание данной темы.

Особое внимание было уделено изучению политики информационной безопасности паролей: рассмотрены особенности различных парольных политик, выявлены уязвимости существующих решений, и на основе анализа разработаны рекомендации по совершенствованию средств аутентификации с целью повышения защищенности систем.

Практическая часть включала создание и публикацию информативных материалов о внедрении CBDC в различных странах, а также демонстрацию кода на языке C++, предназначенного для проверки паролей на соответствие требованиям безопасности и предоставления рекомендаций по их улучшению.

В результате проведенной работы я приобрел новые знания и практические навыки в области цифровых валют и информационной безопасности, что позволит более эффективно оценивать риски и разрабатывать меры по обеспечению безопасного и эффективного внедрения CBDC.

Общее затраченное время 70–85 часов.

# СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Официальный сайт Центрального банка РФ (CBDC) Электронный ресурс. URL: https://www.cbr.ru/ (дата обращения: 10.05.2025)

2. Central Banking Электронный ресурс. URL: https://www.centralbanking.com/ (дата обращения: 10.05.2025)

3. Стандарт NIST SP 800-63B Электронный ресурс. URL: https://pages.nist.gov/800-63-3/sp800-63b.html (дата обращения: 10.05.2025)

4. ISO/IEC 27001 Information Security Management Systems (Стандарт) Электронный ресурс. URL: https://www.iso.org/isoiec-27001-information-security.html (дата обращения: 10.05.2025)

5. ISO/IEC 27002 Code of practice for information security controls (Стандарт) Электронный ресурс. URL: https://www.iso.org/standard/75652.html (дата обращения: 10.05.2025)

6. FIDO Alliance Standards (Стандарт) Электронный ресурс. URL: https://fidoalliance.org/ (дата обращения: 10.05.2025)

7. OATH (Initiative for Open Authentication) (Стандарт) Электронный ресурс. URL: https://openauthentication.org/ (дата обращения: 10.05.2025)

8. Gmail Электронный ресурс. URL: https://mail.google.com/mail?hl=ru (дата обращения: 10.05.2025)

9. Telegram Электронный ресурс. URL: https://telegram.org/faq (дата обращения: 10.05.2025)

10. Госуслуги Электронный ресурс. URL: https://www.gosuslugi.ru/help/faq/c-1 (дата обращения: 10.05.2025)

11. Яндекс Почта Электронный ресурс. URL: https://yandex.ru/support/common/ru/troubleshooting/main (дата обращения: 10.05.2025)

13. Авито (Avito) Электронный ресурс. URL: https://support.avito.ru/articles/1870#!& (дата обращения: 04.07.2023)

14. СберБанк Электронный ресурс. URL: https://www.sberbank.ru/ru/person/faqintb (дата обращения: 04.07.2023)