

«Safety above all else »

**Аутентификация операторов
компьютерных текстов по
цифровому почерку**



Постановка задачи

- **Цель:** исключить несанкционированное использование компьютера при формировании передаваемых через каналы связи текстовых сообщений путем подмены оператора
- **Способ решения:** обеспечить аутентификацию оператора на основе регулярного мониторинга индивидуального «цифрового почерка», который оценивается в процессе передачи текстовых сообщений
- **Общие условия:**
 1. Оператор регистрируется в момент начала работы по логину и паролю или другим способом
 2. Контроль осуществляется в режиме онлайн в течение всей сессии оператора (несколько контрольных проверок незаметных для оператора)
 3. Оператор знает, что его будут контролировать, но не знает точно каким способом и по каким признакам
 4. Контролеру доступны данные об интервалах между нажатиями клавиш во время формирования текстового сообщения
 5. Диалоговые функции между контролером и оператором доступны по запросу контролера
 6. Контроль должен осуществлять онлайн в процессе формирования и передачи текста
 7. Конкретные алгоритмы формирования набора признаков для аутентификации и их использования закрыты для операторов
- **Требования к достоверности результатов**
- Должна быть обеспечена надежность результатов аутентификации не ниже 95% по базовому признаку и возможность дополнительных проверок в случае возникновения обоснованных сомнений в течение сессии формирования документов и вне ее по сохраняемым данным

Принцип работы

- Каждый оператор имеет уникальный **«цифровой почерк»** при наборе текста
- **Показатели**, описывающие «цифровой почерк» инвариантны относительно формата и содержания текста, компьютера, в котором набирается текст, языка (в пределах заданного перечня) и зависят в основном от **личных психофизических данных** оператора
- При первом входе оператор **регистрируется** в системе по заданному алгоритму, включающем заданный набор контрольных данных. При регистрации обеспечивается формирование набора персональных данных, обеспечивающих однозначную идентификацию оператора
- В начале каждой очередной сессии оператор **авторизуется** в системе (как минимум, по логину и пароль, но допускаются дополнительные признаки)
- Для контроля в процессе работы **формируется векторное пространство признаков** на основании поступающих данных о печатаемом тексте (в том числе, временных интервалах между наиболее распространенными в используемом языке (определяется автоматически) сочетания букв (в том числе заглавных) , пробелов, знаком препинания.
- Конкретные наборы признаков формируются для каждого оператора по несколько раз в течение каждой сессии
- Алгоритмы формируются на основании знаний (алгоритмов и статистики языков), накопленных в современной математической лингвистике с обучением на тестовых выборках нейросетевыми и/или другими методами.
- Принятие решения осуществляется на основе регулярного мониторинга с использованием «динамического эталона», который формируется методами робастной статистики на основании «скользящих данных» (от выборки к выборке)
- В случае выявления **«обоснованного сомнения»** (алгоритм и признаки обоснованного сомнения формируются заранее на этапе разработки и настройки системы на основании оценок возможных рисков), проводится дополнительное тестирование (скрытое или открытое для оператора)

Демонстрация

- Ссылка на ресурс, в котором можно продемонстрировать некоторые элементы системы
- Оценка разработки, включающая ТТЗ, дорожной карты, обоснование цены и другое
- Требования к защищенности, конфиденциальности и прочее
- Эксплуатационные требования
- Требования к документации
- Другое

Структура проекта

- Требования конфиденциальности
- Сценарии использования
- Тактико-технические требования
- Дорожная карта
- Требования к эксплуатации
- Требования к рабочей и эксплуатационной документации
- Другие требования

Предложение