

Университет ИТМО, факультет инфокоммуникационных
технологий Отчетная работа по «Информатике»: аннотация к статье

Выполнила Касьяненко В.М., № группы К3121, дата 19.10.2022, оценка ФИО студента не заполнять

Название статьи/главы книги: Аутентификация пользователей по клавиатурному почерку		
ФИО автора статьи: Аверин А.И., Сидоров Д.П.	Дата публикации: 2015 г.	Размер статьи 5 стр.
Прямая полная ссылка на источник и сокращенная ссылка: https://cyberleninka.ru/article/n/autentifikatsiya-polzovateley-po-klaviaturnomu-pocherku https://goo.su/V61jz		
Тэги, ключевые слова или словосочетания клавиатурный почерк / идентификация / аутентификация / биометрия / защита информации		
Перечень фактов, упомянутых в статье: Защита информации в информационных системах является одной из главных проблем современного мира. Существует три метода аутентификации пользователей в системе: классический (использование пароля), имущественный (использование предмета) и биометрический. Биометрический метод позволяет идентифицировать пользователя по его физиологическим и поведенческим характеристикам, например по клавиатурному почерку. Клавиатурный почерк – это совокупность поведенческих характеристик пользователя при работе на клавиатуре, включающих в себя продолжительность нажатий на клавиши, паузы между нажатиями, скорость набора и другие. При аутентификации данным методом необходимо обучение программы, которое включает в себя накопление информации о характеристиках ввода с клавиатуры, обработку этой информации и расчет эталонных характеристик для дальнейшего сравнения с ними при аутентификации. Тем не менее использование аутентификации по клавиатурному почерку не гарантирует определения пользователя с абсолютной точностью. Для повышения точности следует использовать характеристику продолжительности нажатий на клавиши, а не характеристику пауз между нажатиями, поскольку процесс нажатия является подсознательным процессом мышления. Также не стоит использовать слишком длинные ключевые фразы, так как это приводит к «осознанному» вводу пользователя и снижению качества аутентификации.		
Позитивные следствия и/или достоинства описанной в статье технологии <ul style="list-style-type: none">- технология не требует дополнительного оборудования- невозможна кража аутентификационной информации злоумышленниками, как в случае использования пароля- технология не требует от пользователя дополнительных навыков		
Негативные следствия и/или недостатки описанной в статье технологии <ul style="list-style-type: none">- необходимость обучения программы- невозможность определения пользователя с абсолютной точностью- при замене клавиатуры программу необходимо обучать заново		
Ваши замечания, пожелания преподавателю или анекдот о программистах		