о различных уязвимостях компьютерных систем почти за 20 лет развития компьютерных технологий [1]. Каждой уязвимости экспертами выставлены оценки от 0 до 10. Кроме того, содержится краткое словесное описание всех уязвимостей. Современные методы машинного обучения позволяют автоматизировать процесс выставления оценок и могут помочь найти закономерности в появлении наиболее опасных (критических уязвимостей). Использовав векторные представления слов (например, использовав словарь алгоритма GloVe [2], представляющий 400000 слов английского языка в 50-мерном векторном пространстве), получена возможность применения методов машинного обучения к задаче автоматизированного выставления оценок на основе их текстового описания. В частности, разработана модель, использующая в своей основе многослойную нейронную сеть с 2 выходами. На вход подается список из слов в виде соответствующих им индексов из словаря GloVe. Далее следуют три сверточных слоя, после них – 3 полносвязных слоя. Между тремя полносвязными слоями имеется слой, исключающий 40 % данных для лучшего обучения нейронов. По существу, построенная нейронная сеть решает задачу бинарной классификации: выход 0 означает оценку меньше 7,5, выход 1 – оценку от 7,5 до 10 включительно. Таким образом мы решили увеличить точность предсказания, оставив вместо 10 классов всего 2. После 10 эпох обучения точность модели (accuracy) на отложенной выборке составила 85 %, площадь под AUC-ROC кривой – 91 %. Дальнейшие исследования, вероятно, могут улучшить данный результат.

**Литература**

1. National Vulnerability Database [Электронный ресурс]. – URL: https://nlp.stanford.edu/projects/glove/ (дата обращения: 16.05.2018).

2. GloVe: Global Vectors for Word Representation [Электронный ресурс]. – URL: https://nlp.stanford.edu/projects/glove/ (дата обращения: 16.05.2018).

## ВИРТУАЛЬНАЯ ЛАБОРАТОРНАЯ РАБОТА ПО ОЦЕНКЕ УЯЗВИМОСТИ ХРАНЕНИЯ ПАРОЛЕЙ В БРАУЗЕРАХ НА ОСНОВЕ ДВИЖКА CHROMIUM

И.А. Евсеенко

В настоящее время каждый пользователь Интернета имеет пароли для множества учетных записей, начиная от социальных сетей и завершая онлайн-банкингом. Одним из наиболее распространенных способов хранения паролей является система хранения в браузерах. Виртуальная работа рассматривает ситуацию, когда нужно сделать резервную копию всех паролей браузера, или нужно вспомнить давно забытые пароли, которые сохранены в браузере. Однако с другой стороны эта ситуация рассматривается как модель злоумышленника для кражи паролей в браузере.

Браузеры на движке Chromium используют систему шифрования Data Protection Application Programming Interface (DPAPI). В виртуальной лабораторной работе демонстрируются 2 режима: с использованием машинного ключа и с использованием ключа пользователя. Предусмотрена демонстрация принципа работы DPAPI, суть которой заключается в следующем. Приложение обращается к операционной системе задавая параметры Mysecret и Entropy. На выходе получаем BLOB. Приложение сохраняет его, а в дальнейшем, при необходимости, расшифровывает. DPAPI также включает криптопровайдер – это набор алгоритмов для хеширования, шифрования, ключевого обмена и ЭЦП в форме модуля и криптопровайдер объединяет их. Например, в РФ приняты ГОСТовские алгоритмы, поэтому если передать его системе, то вместо стандартных AES, SHA, RSA будут использоваться Российские ГОСТы шифрования. Все это настраивается в реестре. Для DPAPI нет разницы с какими алгоритмами работать, что делает систему универсальной.

Оценка уязвимости по перехвату и расшифровке паролей предусматривает два варианта выполнения: с использование существующих программ и написание студентами программы для расшифровки паролей как на языке высокого уровня, так и на скриптовых языках.

В данной работе рассмотрены возможные негативные последствия использования системы хранения данных в браузерах для авторизации и проведена оценка уязвимости с разработкой специализированного программного обеспечения в рамках лабораторных работ по дисциплине «Защита информации» специальности 09.03.04 «Программная инженерия» БРУ.