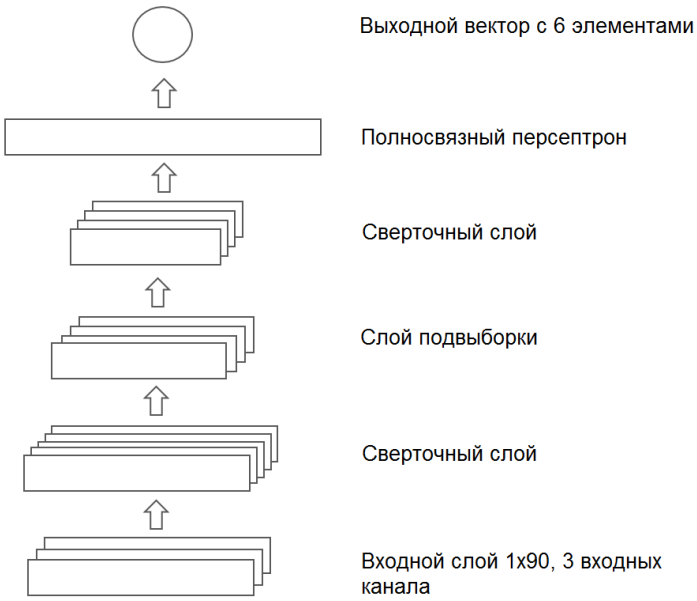

Рис. 1 – Архитектура спроектированной нейронной сети

Процесс тестирования качества нейронной сети заключался в получении результатов классификации для данных, которые не участвовали в процессе обучения. Был произведен подсчет количества случаев, когда результат оказывался правильным. Для этого была использована тестовая выборка. Наилучший результат, который был получен в результате тестирования, - более 80% случаев правильного определения вида деятельности человека.

Таким образом, была решена задача распознавания видов деятельности человека с помощью смартфона с использованием сверточной нейронной сети.

Список использованных источников:

1. Гудфеллоу, Я. Глубокое обучение (серия адаптивных вычислений и машинного обучения) – TheMITPress, 2016 – 534-540 с.
2. Рашка, С. Машинное обучение на языке Python – PacktPublishing, 2015 – 354 с.
3. Баят, А. Исследование по распознаванию человеческой деятельности с использованием данных акселерометра от смартфонов // 11-я Международная конференция по мобильным системам и повсеместным вычислениям– Онтарио, Канада, 2014. – 2-8 с.
4. Лаборатория WISDM. [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.cis.fordham.edu/wisdm/dataset.php Дата доступа: 20.03.2018.

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО ХРАНЕНИЯ ДАННЫХ НА ВНЕШНИХ НОСИТЕЛЯХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пашковский С.М.
Прохорчик Р.В. – ст. преподаватель каф. ПОИТ, м.т.н.

Сегодня стоит острая проблема хранения данных в электронном виде. Основные тому причины человеческий фактор и массовое подключение электронных устройств к глобальной сети Интернет. Под человеческим фактором понимается: беспечность людей, незнание и/или не соблюдение элементарных правил безопасности, возможность обмана человека. Данные факторы сложно решить какими-либо техническими средствами. Проблемы, связанные с массовым подключением к Интернету, можно решить при помощи технических и организационных средств. Одним из таких средств является перенос данных на внешнее хранилище данных.

Перенос информации с компьютера на внешний, съёмный носитель данных является неплохим методом повышения защищенности данных. Обычно человек пользуется секретными файлами (с документами, с личной информацией, с научными разработками и т.д.) редко, поэтому их можно перенести на съёмный носитель и подключать его только в случаях необходимости. Это существенно сокращает время, втечении которого злоумышленник может украсть информацию.

Однако, существуют потенциальные уязвимости, связанные с хранением данных на съемных носителях:

- Хищение или утеря носителя;
- Попытка чтения данных с носителя вредоносной программой в то время, когда носитель подключено

к компьютеру.

Для предотвращения описанных уязвимостей предлагаются следующие методы, повышающие сохранность данных.

Во-первых, шифрование данных на этом носителе. Это позволит предотвратить утечку информации вследствии хищения или утери носителя данных.

Во-вторых, контроль программ (процессов), которые имею доступ на чтение, запись информации на защищенный носитель. Т.к. на пользовательском компьютере могут присутствовать вредоносные программы, которые будут пытаться считать данные с подключаемых устройств, необходимо требовать от пользователя подтверждение, о том, что данная программа может работать с носителем.

Для реализации данной концепции защиты данных необходимо разработать соответствующее программное средство. Оно будет состоять из двух отдельных компонентов, способных взаимодействовать между собой: драйвера операционной системы и приложения для ввода пользовательских настроек.

Основным компонентом системы является драйвер. Он осуществляет всю необходимую работу по шифрованию, дешифрованию информации, контролю доступа программ к носителю. Выбор пал на драйвер, а не на простое пользовательское приложение, т.к. получение доступа к драйверу и его модификация сложнее для вредоносных программ [1]. Наличие драйвера позволяет любой программе записывать и читать данные из любой программы, что очень удобно для пользователя. При создании простого приложения пользователь мог бы работать с носителем только из него. Однако, доступность к носителю из любой (потенциально вредоносной) программы является угрозой безопасности. Поэтому необходимо создать механизм контроля доступа программ к носителю.

Контроль доступности носителя будет осуществляться путём хранения разрешенных приложений. При попытке программы (процесса) прочесть или записать данные на защищенный носитель система будет запрашивать разрешение пользователя на эти действия. Драйвер будет хранить разрешенные программы только в течение его работы (следовательно, только в оперативной памяти). После перезагрузки операционной системы эта информация будет стираться, и пользователь снова должен будет дать доступ необходимым программам. Разрешённые программы не будут сохраняться на диск, т.к. у злоумышленника появится возможность изменить эти настройки на диске.

Шифрование данных будет производиться на основе стандарта СТБ 34.101.31-2011 [2]. Выбран симметричный блочный алгоритм шифрования, т.к. он обеспечивает хорошую скорость, а в данном случае скорость имеет большое значение, т.к. может производится чтение/запись больших объемов информации.

Ключ для каждого устройства будет свой. Они будет хранится в файле в хешированном виде. В качестве алгоритма хеширования должен использоваться один из надёжных на данный момент алгоритмов (например, SHA-256).

Список используемых источников:

1. Руссинович М., Соломон Д. Внутреннее устройство MicrosoftWindows. 6-е изд. – СПб.: Питер, 2013 – 800с.

2. СТБ 34.101.31-2011 "Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности".

3. WindowsDriverKitDocumentation [Электронный ресурс]. – Режим доступа: https://docs.microsoft.com/windows-hardware/drivers/index - Дата доступа: 22.03.2018.

МОБИЛЬНОЕ ПРИЛОЖЕНИЕ ИЗУЧЕНИЯ ИНОСТРАННЫХ СЛОВ НА ОСНОВЕ ИНТЕРВАЛЬНОГО МЕТОДА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Подлужный П.Н.

Хмелева А.В. – канд. техн. наук, доцент

В наше время, знать иностранный язык жизненно необходимо. Для некоторых – это возможность расширения кругозора, а для других – необходимое условие для работы. Но изучение языка требует достаточно много времени и усилий, которые можно сэкономить, если использовать методы и техники, которые эффективнее всего используют эти ресурсы. Возможно, не самым лучшим, но одним из лучших методов для изучения новой информации является интервальный метод.

Интервальные повторения — техника удержания в памяти, заключающаяся в повторении запомненного учебного материала по определённым, постоянно возрастающим интервалам [1]. Идея, что интервальные повторения можно использовать для улучшения процесса обучения, впервые была предложена в книге «Психология обучения», написанной профессором Алеком Мейсом в 1932 году. В 1939-м Spitzer протестировал эффект методики на студентах в Айове [2]. Spitzer исследовал метод на более чем 3600 студентах и доказал его эффективность. Это достигается за счёт того, что повторение слова происходит в тот момент, когда оно вот-вот будет забыто.

Наиболее известным и распространённым методом, реализующим метод интервального повторения для запоминания различной информации, являются карточки. Т.е. на одной стороне находится вопрос (в случае с изучением слов — слово на иностранном языке), а на другой стороне — ответ на него (в случае с