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

изучением слов — перевод слова). Так можно изучать и запоминать не только иностранные слова, но всё, что вам необходимо. Когда вы начинаете забывать слово (имеются различные исследования, которые устанавливают периоды времени, через которое это происходит) — программа предоставляет вам карточку с ним, вы отвечаете и, в случае правильного ответа карточка с данным словом будет предложена вам через больший, по сравнению с предыдущим, период времени. Так как в нашей жизни присутствуют всяческие стрессы и другие помехи работы нашего мозга, то некоторые карточки будут забываться до того, как программа предложит вам их повторить. В этом случае, время следующего повторения будет меньше — предыдущий период.

Существуют хорошие программы, которые используют данный метод. Например, “Anki” и “Memrise”. Но имеется один минус в их работе. Если вы пропусти ли несколько дней и у вас скопилось много карточек, то вам, возможно, не захочется их изучать, и вы просто закончите использовать данную программу и на этом ваше изучение остановится.

Для его преодоления, в разрабатываемом приложении, будет введён рейтинг слова, который будет использовать интервальный метод. Рейтинг будет напрямую связан с периодами интервального метода. Пользователь может регулярно повторять слова и тогда, рейтинг будет возрастать. При своевременном повторении слово будет оставаться в памяти, а его рейтинг возрастать, увеличивая периоды повторения. Если пользователь не повторил карточку, то её рейтинг будет уменьшен и с ним, уменьшиться период, через который пользователю будет необходимо его повторить.

Пользователю не будет знать, нужно ли именно сейчас повторить данное слово. Он будет пользоваться программой тогда, когда ему это удобно. Это снижает эффективность интервального метода, но при этом, мотивация пользователя не будет снижена. При повторении слова, ему лишь будет показан рейтинг. Если же пользователь будет повторять слово раньше, чем наступит период следующего повторения, то рейтинг будет изменяться на меньшее значение. При слишком частом повторении слова, ему будет выведено сообщение о том, что слово усвоено им достаточно на данном этапе, и он может пока не концентрироваться на нём.

Для поддержания мотивации в приложение необходимо ввести разнообразные варианты повторения слова:

- Тесты;
- Рукописный ввод слова;
- Экзамен, главной особенностью которого будет ограниченное время;

Для английского языка будет присутствовать режим изучения неправильный глаголов.

Все эти варианты будут так же изменять рейтинг слов, но по своим правилам.

Данное приложение, основываясь на интервальном методе, предоставляет пользователю возможность нерегулярного изучения слов, что позволит не терять мотивации и продолжать изучать слова в удобном ему режиме.

Списокиспользуемыхисточников:
1. «Human Memory: Theory and Practice», Alan D. Baddeley, 1997
2. Spitzer, H. F. (1939). Studies in retention. Journal of Educational Psychology, 30, 641—657

АЛГОРИТМ ПРИМЕНЕНИЯ СЕМАНТИЧЕСКОЙ СЕТИ ДЛЯ ПОИСКА ОТВЕТА НА ВОПРОС

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

Потараев В.В.

Серебряная Л.В. – к.т.н., доцент

Семантический анализ является довольно эффективным методом обработки информации. Семантическая сеть позволяет осуществлять различные способы обработки данных. Рассмотрим представление текстовых данных в виде семантической сети и алгоритм получения ответа на вопрос, основанный на использовании данной сети.

В современных автоматизированных системах хранятся и обрабатываются значительные объёмы информации. Поэтому актуальным является повышение эффективности автоматизированной обработки данных, как по скорости, так и по точности обработки. Одним из инструментов улучшения эффективности обработки данных является учёт их смысловой структуры, то есть семантический анализ.

Многие информационные системы предназначены для поиска ответа на запрос [1]. Рассмотрим задачу ответа на вопрос, сформулированный на естественном языке. В русском языке выделяют пять основных видов вопросов: закрытые, открытые, риторические, переломные, вопросы для обдумывания [2].

Целью данной работы является разработка алгоритма поиска ответа на открытый вопрос.

Открытый вопрос – это вопрос, требующий разъяснения [2], например: «что?», «кто?», «где?», «как?», «сколько?», «почему?». Алгоритм, позволяющий отвечать на различные типы вопросов, может быть использован для упрощения работы с информационной системой. Если система способна найти ответ на различные типы вопросов, то у пользователя есть больше возможностей сформулировать вопрос в удобной для него форме.