1. eVineyeardBlog. [Digital resource]. – Digital data. – Access mode: https://www.evineyardapp.com/blog/2015/07/20/how-electronic-calendar-can-help-with-vineyard-management Access date: 24.03.2019.
2. React. [Digital resource]. – Digital data. – Access mode: https://reactjs.org/ Access date: 24.03.2019.
3. Node.js [Digital resource]. – Digital data. – Access mode: https://nodejs.org/en/ Access date: 24.03.2019.
4. Mongo DB. [Digital resource]. – Digital data. – Access mode: https://www.mongodb.com/ Access date: 24.03.2019.
5. Docker. [Digital resource]. – Digital data. – Access mode: https://www.docker.com/ Access date: 24.03.2019.

ПРИЛОЖЕНИЕ ДЛЯ АВТОМАТИЗАЦИИ ОРГАНИЗАЦИИ ЗАДАЧ И РАБОЧЕГО ГРАФИКА ПРЕПОДАВАТЕЛЯ

Арзуманян А.С.

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

Трус В.В. – ст. преподаватель

В рамках интеграции информационных технологий в жизнь человека, преподаватели всё чаще сталкиваются с необходимостью организации рабочего графика с помощью различных сервисов. Они значительно облегчают процесс ведения расписаний и задач, так как позволяют сделать управление рабочим графиком более удобным, а также позволяют в любой момент получить необходимую информацию о расписании. Существует множество мобильных приложений для организации рабочего графика, но большинство из таких сервисов не учитывают преподавательскую специфику, не имеют синхронизаций с веб-сервисами, а также не дают статистическую информацию о затраченном времени.

Ключевым преимуществом использования мобильного приложения для организации расписания является то, что вся необходимая информация легкодоступна и имеет формализованный вид. Пользователь может в режиме реального времени использовать только актуальные данные.

Планирование расписания и задач является важным пунктом в работе преподавателя, которому необходимо держать постоянный контроль над большим объёмом информации, так как профессия преподавателя предполагает работу с широким спектром задач и коммуникацию с людьми, которых обучает преподаватель, и с коллегами по работе[1].

Управление временем – это действие или процесс тренировки сознательного контроля над временем, потраченным на конкретные виды деятельности, при котором специально увеличиваются эффективность и продуктивность. Управление временем может помочь получить ряд навыков, инструментов и методов, используемых при выполнении конкретных задач, проектов и целей. Управление временем включает в себя широкий набор решаемых задач, среди которых:

– постановка целей;
– планирование времени;
– анализ затрат времени;
– определение приоритетов;
– создание списков [2].

Современные мобильные приложения хорошо справляются с вышеупомянутыми задачами. Благодаря интерактивному и интуитивно понятному интерфейсу пользователь в пару кликов может добавлять, редактировать или просматривать необходимую информацию о расписании. Большинство таких приложений организованы согласно клиент-серверной архитектуре. Нередко случается, что приложения используют в качестве серверной части какой-нибудь сторонний сервис. Так, например, многие приложения для управления расписанием используют сервер Google-календаря, имеют синхронизацию с ним и используют его базу данных для хранения. Данный подход является удобным, так как пользователю предоставляется больший функционал, а программисту – простота разработки.

Нередко, так называемые, приложения-планировщики позволяют выставить степень важности задаче. Однако, помимо важности существует другой не менее важный фактор, который не учитывают данные приложения – срочность исполнения. Так, один из президентов Америки изобрёл собственную методику для управления временем, называемую “таблицей Эйзенхауэра”. Суть метода состоит в том, что все задачи делятся на следующие категории:

– срочные (важные) задачи, которые должны выполняться в первую очередь;
– срочные (менее важные) задачи, которые при необходимости можно делегировать;
– менее срочные (важные) задачи, которые некритичны и могут быть выполнены в ближайшее время;
– менее срочные (менее важные) задачи, которые лучше всего сделать при наличии свободного времени или делегировать другому человеку.

Для более эффективного планирования расписания и задач преподавателя, а также для получения статистических данных было разработано мобильное приложение на базе операционной системы Андроид. Таким образом преподаватель сможет удобным ему образом создавать элемент

расписания, просматривать и редактировать его. Ключевыми особенностями являются возможности просмотра статистических данных о затраченном времени преподавателя и выставления степени важности и срочности задачи.

Список использованных источников:

1. [Электронный ресурс]. – Электронные данные. – Режим доступа: https://kinderklub.ru/professiya-uchitel/upravlenie-vremenem-kak-instrument-prepodavatelya/.
2. Википедия [Электронный ресурс]. – Электронные данные. – Режим доступа: https://ru.wikipedia.org/wiki/Управление_временем.

ПРОГРАММНОЕ СРЕДСТВО «KASISKI-BABBAGE FREQUENCY ANALYSIS»

Биткин Н.С., Болтак С.В.

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

Болтак С.В. – ассистент

Современные криптосистемы отличаются своим многообразием, уровнем криптостойкости и сложностью понимания. Поэтому начинающему криптографу необходим более простой и понятный пример для ознакомления с огромным миром шифров и методов взлома. Разработанный программный продукт позволяет провести криптоанализ шифротекста, зашифрованного шифром Виженера с прогрессивным способом генерации ключевой последовательности.

Шифр Виженера может использовать так называемый прогрессивный ключ (дублирование ключевого слова осуществляется с одновременным сдвигом букв ключа на одну позицию при каждом новом повторении) [1]. В этом случае задача взлома становится не совсем тривиальной.

В алгоритм взлома необходимо внести следующие изменения: повторяющиеся последовательности необходимо учитывать только в позициях, чьи номера кратны длине алфавита исходного текста (это очевидно, так как минимально необходимое количество сдвигов ключа для получения исходного равняется мощности алфавита).

Данная работа представляет собой анализ возможностей метода Касиски-Бэббиджа при атаке шифротекста, полученного с использованием шифра Виженера с прогрессивным ключом. Средняя скорость обработки – порядка миллиона символов в минуту. Исходя из полученных результатов можно сделать следующие выводы:

1) метод абсолютно неэффективен на шифротексте, длина которого не превышает произведение мощности алфавита на длину ключа;
2) при достижении определённых размеров шифротекста метод взлома позволяет получить результат с вероятностью более 90% для ключа любой длины;
3) при повторном шифровании ранее зашифрованного текста вероятность успеха стремится к нулю, тоже самое касается шифрования текста, не имеющего смысла;
4) научно-популярная литература более устойчива к рассматриваемой атаке. Из-за насыщенности таких текстов терминами, которые в большинстве своём являются словами с большим количеством букв, вероятность совпадения последовательностей меньше;

Разработанное программное средство позволяет наглядно продемонстрировать работу метода Касиски-Бэббиджа на шифротексте, полученном шифром Виженера с прогрессивным ключом. Как видно из рисунка 1, успешность взлома зависит от длины шифротекста.