символьной строки и невозможности ее однозначного прочтения стандартными техническими средствами производится основательная обработка этого носителя информации.

Наиболее часто на первоначальном этапе предполагается проведение посимвольной сегментации строки. Как правило, сегментация строки проводится на основе анализа ее проекции на параллельную ось, вертикальной или горизонтальной проекции [1]. С целью определения и исправления зашумленных фрагментов непосредственно на этапе сегментации проекции оправдано использование своего рода фильтра. Он позволяет преобразовать зашумленный сегмент проекции символа к его шаблону (скелету), не имеющему помех [2]. Определение и устранение шумов на начальном этапе распознавания значительно ускорит процесс распознавания в целом, а также позволит использовать менее мощные вычислительные устройства.

Модифицированный алгоритм фильтрации, совмещенный с сегментаций, основывается на идее, что значение проекции на определенном фрагменте для отдельного символа может быть четко сопоставлена с конечным набором модельных проекций. В таком случае каждый элемент набора модельной проекции характеризует только один единственный символ алфавита с некоторой допустимой погрешностью. Если этап распознавания, следующий за этапом сегментации, не дал удовлетворительных результатов, возможна повторная сегментация.

В докладе подробно рассматриваются детали и процедура фильтрации – нового этапа в распознавании символьных строк.

Список литературы

1. Sawaki M., Hagita N. Text-Line Extraction and Character Recognition of Document Headlines With Graphical Designs Using Complementary Similarity Measure // IEEE Trans. PAMI. 1998. Vol. 20, № 10. P. 1103–1109.

2. Заерко Д.В., Липницки В.А. Применение модифицированных алгоритмов JavaANPR для автоматического распознавания номеров автомобилей // Матер. междунар. науч. конф. «Информационные технологии и системы 2018». Минск, 25 октября 2018 г. С. 286–287.

АГРЕГАЦИЯ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ SCRIPTRUNNER В СИСТЕМЕ JIRA

А.Д. Зайков

Лучшим решением для организации безопасной работы, отличным инструментом планирования, отслеживания ошибок или этапов итеративного процесса в современной ИТ-компании является система JIRA. При разработке программного обеспечения всегда важно помнить не только о деталях, но и об общей концепции. Особенность JIRA состоит в том, что проект разбивается на задачи, работа над каждой из которых ведется обособленно. Система умело акцентирует внимание администратора на деталях проекта. В конкретном ИТ-проекте всегда следует завершить одни задачи, и затем переходить к следующим. Цикл жизни каждой задачи напоминает принцип работы каскадной модели: спецификация, разработка, улучшение, тестирование, релиз. Однако, в целом, можно отметить отход от каскадной модели к гибкой методологии разработки, и один большой каскад заменяется тысячами поменьше [1, 2].

В работе предлагается организация новых технических решений для автоматического подсчета текущего курса валюты Национального Банка Республики Беларусь, который использует REST API Национального Банка Республики Беларусь, для получения данных о курсах в момент закрытия задачи в системе JIRA (или последнего трекинга в ней). Полученные данные агрегируются с ограничением доступа; для реализации такого функционала используется плагин ScriptRunner, позволяющий встраивать Groovy-скрипты в настраиваемые поля, а также работать с событиями задач в JIRA. Данные о курсах валют используются в дальнейшем для автоматического подсчета себестоимости ИТ-проекта и оценки трудозатрат на нем. Для этого были созданы дополнительные пользовательские поля с использованием языка Groovy. Доступ к редактированию данных полей ограничен для всех пользователей. Для администраторов и группы top-management в системе JIRA настроен доступ просмотра данных полей, согласно полученному техническому заданию. В дальнейшем

в проекте будет разработан функционал для генерации дополнительных отчетов для оценки загруженности сотрудников, а также обновления текущие отчетов в eazyBI.

Список литературы

1. JIRA documentation // Atlassian [Электронный источник]. URL: https://confluence.atlassian.com/jiracoreserver071/jira-core-documentation-802172329.html/ (дата обращения: 12.04.2019).

2. JIRA Software // TOPSAAS [Электронный источник]. URL: http://topsaas.ru/jira.html/ (дата обращения: 19.04.2019).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Д.В. Зезина, А.Ю. Хохлов

В работе рассматриваются основные меры, которые необходимо учитывать при проектировании системы защиты данных на предприятии. Обеспечение информационной безопасности должно быть направлено прежде всего на предотвращение рисков, а не на ликвидацию их последствий. Именно принятие предупредительных мер по обеспечению конфиденциальности, целостности, а также доступности информации и является наиболее правильным подходом в создании системы информационной безопасности. Популярные инструменты и технологии современной повседневной жизни, такие как мобильные телефоны, веб-почта, службы мгновенных сообщений, съемные носители и беспроводной доступ к Интернету дали каждому возможность легко переносить и обрабатывать большое количество данных. Наряду с возможностью переноса данных многие организации создали информационные системы вокруг своих продуктов и услуг на основе открытых стандартов и интерфейсов совместимых с популярными устройствами. Кроме того, организации способствуют легкому доступу к данным как для персонала, так и для широкой публики через Интернет. Но недостатком этого удобства является большая вероятность передачи конфиденциальных корпоративных данных посторонним лицам. Поэтому актуальность рассматриваемой темы в том, что в наше время остро встает вопрос о необходимости защищать информацию своего предприятия различными методами, но многие не знают, что следует делать, дабы сохранить те или иные сведения в тайне, с выгодой реализовать их и не понести убытки от их утечки или утраты. Данные являются одним из наиболее важных активов любой организации и люди обычно считаются самым слабым звеном в цепи безопасности. Крайне важно чтобы сотрудники полностью осознавали свои обязанности, их ограничения на доступ к информации и дисциплинарные меры, которые будут приняты за любое нарушение безопасности. Все это может служить движущей силой для самосовершенствования с точки зрения безопасности данных.

УПРАВЛЯЕМОЕ КОДИРОВАНИЕ КОМБИНАЦИОННЫХ СХЕМ

Л.А. Золоторевич, А.В. Павлова

В последнем десятилетии значительно возрос ущерб от пиратства и других угроз в области производства аппаратного обеспечения и составляет около 4 млрд. долларов в год, что примерно в 10 раз превышает ущерб от пиратства в области ПО. Для решения проблемы в работе [1] предлагается подход к проектированию Design for-Trust (DfTr) как развитие теории контролепригодного проектирования (Design-for-Testability – DfT), который дополнительно включает средства для контроля и предотвращения аппаратных атак при проектировании и изготовлении СБИС.

В работе [2] проанализированы различные модели процесса злонамеренного искажения проекта, описывающие условия, при которых подобное искажение может внедриться в цифровую систему. В числе возможных источников искажений рассматриваются поставщики базовых функциональных блоков интеллектуальной собственности (IP's), которые приобретаются разработчиками СнК, собственно разработчики СнК, а также кремниевые фабрики – изготовители СнК.