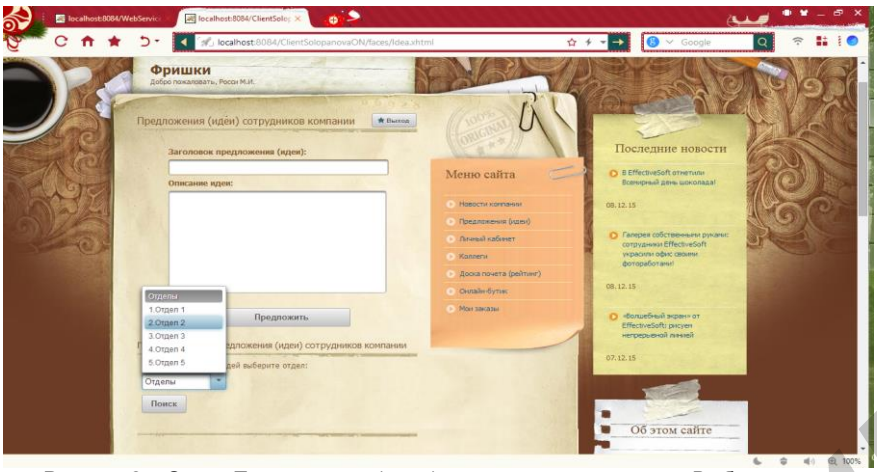

Рисунок 2 – Окно «Предложения (идеи) сотрудников компании». Выбор отдела

Вся используемая информация хранится в базе данных, разработанной для данного проекта. Доступ к базе данных был реализован с помощью фраймворкаHibernate на стороне сервера. Данная структура использована для быстрого отображения объектно-ориентированной модели данных.

Безопасность данных обеспечивается за счет системы авторизации. При выполнении аутентификации поступает запрос на серверную часть приложении, которая в свою очередь проверяет учетные данные содержащиеся в базе данных. Для повышения безопасности хранимых данных, пароль к базе данных меняется каждые 3 дня.

Таким образом, разработанный программный продукт решает задачу хранения и представления данных нематериальном мотивации как конкретного сотрудника, так и структурного подразделения в целом. Информация представлена в доступной и наглядной форме: разнообразные статистики, графики и диаграммы, – анализ которых способен улучшить работу сотрудников компании.

Список использованных источников:

1. Управление персоналом / П.Э. Шлендер [и др.]. М.: ЮНИТИ-ДАНА. 2005. 320 с

МОБИЛЬНАЯ ОНЛАЙН СИСТЕМА ВНУТРИКОРПОРАТИВНОГО ОБЩЕНИЯ С ЭЛЕМЕНТАМИ КРИПТОГРАФИИ

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

Цецерский А.С.

Унучек Т.М. – ст.преп.

Информация всегда имеет стоимость. Чем больше ее уникальность, сложность получения, тем выше желание третьих лиц завладеть ею. Главная тенденция, характеризующая развитие современных информационных технологий – рост числа компьютерных преступлений и связанных с ними хищений конфиденциальной и иной информации, а также материальных потерь.

По данным антивирусной компании BitDefender из 130.000 популярных приложений около 13% из них собирают и передают на сторону номера мобильных телефонов пользователей без явного уведомления. Столько же передают данные о местонахождении владельца, почти 8% собирают адреса электронной почты, 6% получают доступ к журналу браузера, а некоторые даже к личным фотографиям. Далеко не всем приложениям нужны эти данные для своей работы [1]. Эти цифры говорят о важности защиты личной информации.

Сегодня разработано значительное количество надежных алгоритмов шифрования. Стойкость большинства применяемых шифров основывается на секретности ключа, используемого для расшифровки, сам же шифрующий алгоритм предполагается известным. Следовательно, криптосистема поддается взлому путем перебора ключей, причем технические возможности для этого со временем расширяются. В ход пускаются системы распределенного взлома, когда перебором занимается множество компьютеров, объединенных в сеть. В этом случае криптографическая устойчивость повышается за счет усложнения алгоритмов и увеличения размера секретного ключа. Но человеческая память отличается от компьютера, и не в состоянии хранить длинные цифровые комбинации, поэтому хранение таких ключей, в большинстве случаев, происходит непосредственно на компьютере или электронном носителе. Передача секретного цифрового ключа также осуществляется с помощью телекоммуникационных средств. Эти проблемы открывают новые способы по несанкционированному доступу к зашифрованной информации. Кроме математического и технического взлома можно попробовать получить секретный ключ у его хранителей различными методами, такими как похищение, обман, взлом компьютера, на котором хранится код, перехват информационных сообщений, в которых передается ключ другим лицам и так далее [2].

Наиболее распространенным и стойким алгоритмом шифрования на сегодняшний день является RSA. В настоящее время система RSA используется для защиты компьютерного программного обеспечения и в схемах цифровой подписи. Внедрение такой системы защиты в мобильное программное обеспечение позволяет вывести защиту информации на мобильных устройствах на новый уровень.

В мобильных устройствах по умолчанию есть несколько способов общей защиты информации: графический пароль, pin-код, простой пароль, некоторые устройства поддерживают проверку отпечатка пальца пользователя и т.д. Все эти способы призваны защитить телефон от несанкционированного доступа, при этом защита в самих приложениях упразднена, и, зачастую, её вовсе нет. Вдобавок, все вышеуказанные способы защиты не предусматривают защиту информации непосредственно при передаче её через Интернет, при работе пользователя в приложении. А ведь передаваться таким способом может и корпоративная информация.

Стремление компаний иметь более надежные способы обмена информацией хорошо прослеживаются в развитии компании Slack. Slack — корпоративный мессенджер. Запущен в тестовом режиме в августе 2013 года, публичный релиз состоялся 12 февраля 2014. В первый день тестирования зарегистрировались 8 тысяч компаний. По данным компании на июнь 2015, Slack ежедневно используют 1,1 миллиона пользователей. Благодаря своему развитию Slack стал самым быстрорастущим бизнес-приложением в истории. В феврале 2014 Slack запускали 16 человек, через год команда расширилась до 105. Сейчас в Slack работают 180 сотрудников. На данный момент приложение Slack для устройств с ОС Android скачали уже более 1 миллиона раз. Сами цифры, отражающие рост аудитории, говорят о стремлении компаний к более новым способам обмена корпоративной информацией. И, конечно же, надежность передачи информации один из важнейших критериев при выборе средств взаимодействия.

Таким образом, совмещая стойкие системы шифрования с потребностями современного рынка обмена информацией, можно получить конкурентоспособный программный продукт. Ниша защищенных мобильных систем для общения еще только развивается и потому имеет большие перспективы, в частности, в сфере внутрикорпоративного общения.

Автором спроектирована и разработана мобильная онлайн система, позволяющая, используя существующие подходы к защите информации, повысить уровень защиты передаваемой информации внутри компании.

Список использованных источников:

1. Защита информации на Android-устройствах встроенными средствами ОС // Интернет-блог «Быть, а не казаться (о безопасности и не только)»

2. Усиление защиты от взлома данных, передаваемых через Интернет: Е. А. Карасик, Минск, 2007. – 186 с.

ЭКСПЕРТНАЯ СИСТЕМА ДИАГНОСТИКИ И МОНИТОРИНГА ФИНАНСОВОГО СОСТОЯНИЯ ПРЕДПРИЯТИЯ

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

ЛобанН. А.

Поттосина С. А. − канд. физ.-мат. наук, доц.

В современных условиях динамичное, эффективное и рациональное развитие предприятия невозможно без управления его финансовым состоянием, конечной целью которого является повышение конкурентоспособности хозяйствующего субъекта. Только при эффективном управлении финансовой деятельностью организации возможно добиться преимуществ на рынке.По мере роста и развития информационных технологийпредприятия столкнулись с проблемой обработки и анализа больших массивов информации.В связи с этим возникает необходимость в разработке экспертной системы, которая позволяет проводить диагностику и мониторинг финансового состояния предприятия.

Разработана экспертная система, котораяпозволяет осуществлять диагностику и мониторинг финансового состояния предприятия.Целью работы является совершенствование диагностики и мониторинга финансового состояния предприятия за счет разработки соответствующей экспертной системы. Основной задачей системы является обеспечениеподсчёта, анализа и прогнозирование показателей финансового состояния предприятия согласно существующим алгоритмам и моделям.

Объектом исследования является финансовое состояние предприятия.Предметом – методы диагностики и мониторинга финансового состояния предприятия.

Для достижения поставленной цели была разработана экспертная система.

Экспертная система – это набор программ, выполняющий функции эксперта при решении задач из некоторой предметной области. Экспертные системы выдают советы, проводят анализ, дают консультации, ставят диагноз. Практическое применение экспертных систем на предприятиях способствует повышению эффективности работы.

Экспертные системы имеют ряд свойств, обуславливающих их широкое распространение и большой интерес со стороны пользователей.

Основными отличиями экспертных систем от других программных продуктов являются использование не только данных, но и знаний, а также специального механизма вывода решений и новых знаний на основе имеющихся. Знания в экспертных системах представляются в такой форме, которая может быть легко обработана на ЭВМ. В экспертных системах известен алгоритм обработки знаний, а не алгоритм