ходим доступ на контроллер, а если он стоит удаленно, то выехать и произвести измерения – процесс в ряде случаев достаточно трудоемкий. Вместе с тем, конфигурация приборов такова, что получить трассировку A-bis интерфейсов со всех сот невозможно, а значит, только процесс измерения займет недопустимо большое время. Как и в предыдущем случае, этот метод можно рассматривать лишь как дополнительный. Кроме того, первый и второй методы не позволяют производить оценку всех сот сети одновременно и в реальном масштабе времени.

Наконец, **третьим методом** и основным, является метод, основанный на сборе и обработке статистической информации, получаемой с контроллеров. Этот метод основан на том, что при обмене сигнальной информацией между элементами сети, на контроллере увеличиваются значения определенных счетчиков. Причем эта информация собирается для каждой соты контроллера. Зная по получении какого сигнального сообщения, увеличивается значение того или иного счетчика по нему можно делать соответствующие выводы о качестве работы как любой отдельной соты, так сети в целом. Простейший пример: если наблюдаются большие значения счетчика, показывающего количество хендоверов по причине интерференции на «линии вниз», значит в данной соте есть помеха, мешающая нормально работе мобильной станции. В силу того, что этот метод оценки качества позволяет одновременно для всех сот в реальном масштабе времени отслеживать ситуацию в сети, а также то, что возможность получения данной статистики предоставляется всеми производителями оборудования, данный метод является основным. Среди недостатков можно отметить лишь необходимость иметь программу-обработчик информации получаемой с контроллера, и тот факт, что для разных компаний-производителей оборудования полнота статистики может отличаться, но в любом случае, не блокирует возможность мониторинга основных показателей качества. Необходимо также учитывать и то, что в новых версиях программного обеспечения большинства компаний-производителей оборудования, статистика достаточно богата, т.е. есть возможность оценивать многие параметры сети, даже те, которые раньше могли быть вычислены только на основании результатов драйв-тестов.

Выводы

Таким образом, все рассмотренные методы оценки качества сетей сотовой связи являются важными, дополняют друг друга и позволяют иметь максимально полную информацию о текущей ситуации в сети. Однако из-за рассмотренных выше особенностей каждого из методов, основным является третий – сбор, обработка и анализ данных, получаемых на постоянной основе с контроллера сети. В дальнейшем, под показателями качества будут подразумеваться показатели, полученные при помощи именно этого метода.

ОПЕРАЦИОННЫЕ РИСКИ ИНФОРМАЦИОННЫХ СИСТЕМ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Власов Е.В.
Уфимский государственный нефтяной технический университет
Уфа, Россия

Для современной, качественно организованной экономической информационной системы именно операционные риски часто являются причиной возникновения катастрофических потерь, что подтверждает исследование, проведенное международной информационной группой в области финансовых рынков Risk Waters Group и фирмой SAS [1].

Операционный риск можно определить как риск прямых или косвенных потерь, вызванных ошибками или несовершенством процессов, систем в организации, ошибками или недостаточной квалификацией персонала организации или неблагоприятными внешними событиями нефинансовой природы[2]. Операционные риски отличаются от прочих видов рисков, тем, что их источник чаще всего лежит внутри самой системы. Следовательно, риск может быть снижен за счет устранения порождающих его причин. Методы снижения также являются фактически методами организации внутреннего контроля и, как правило, при разработке информационной системы финансовой организации подразумевают: разделение функций, независимая оценка результатов деятельности, двойной ввод и подтверждение операций, контроль изменения условий операций, подтверждение сделки контрагентом [3, 4, 5].

Целью данной работы является исследование и разработка способа ввода данных, позволяющего принципиально снизить вероятность проявления операционного риска за счет использования превентивных мер.

Следует отметить, что на сегодняшний момент, для снижения операционных рисков в информационной системе финансовой организации, реализуются превентивные методы отражающие, лишь, технологический подход. К таким средствам методам относятся: классификации вводимых данных и их формализация, применение констант с условно постоянной информацией, справочники-классификаторы с нормативно-справочной информацией, шаблоны операций и документов с предварительно заполненными параметрами, управление правами доступа пользователей. Указанные приемы в основном направлены на минимизацию ручного ввода реквизитов за счет использования системой предварительно проверенной информации, хранящейся в базе данных.

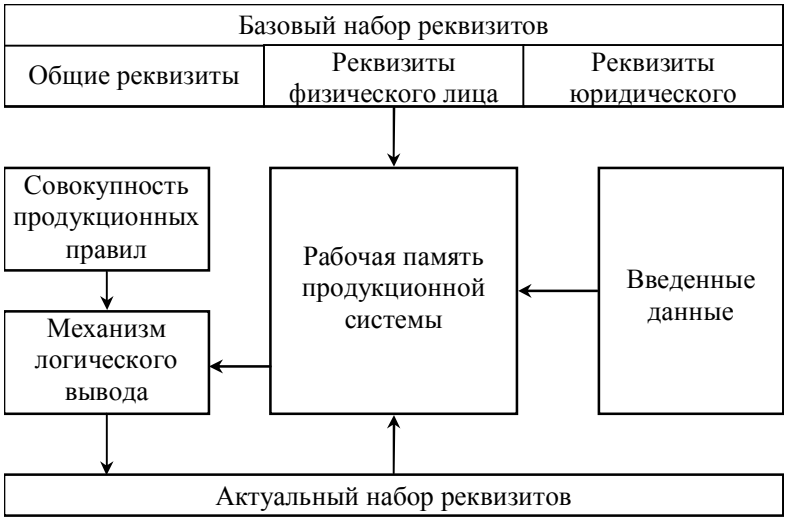

Рис. 1. Концептуальная схема работы механизма динамической адаптации интерфейса пользователя на основе вводимых им данных

Примером реализации данного метода может послужить процесс ввода анкетных данных в информационной системе ведения реестров ценных бумаг (Рисунок 1). Анкета зарегистрированного лица состоит из ряда реквизитов, которые можно разделить на общие, данные физического лица, данные юридического лица. Причем два последних набора реквизитов носят взаимоисключающий характер. На начальном этапе формируется первоначальный (базовый) набор реквизитов. Затем в процессе ввода данных механизм контроля определяет актуальный набор реквизитов, то есть тот набор реквизитов, которые необходимы пользователю в данный момент времени. Механизм контроля вводимых данных представляет собой продукционную систему.

Использование процесса динамической адаптации интерфейса пользователя на основе вводимых им данных позволит учитывать не только факторы технологического подхода, но и за счет продукционной системы, которая является ядром данного механизма, осуществить учет аспектов функционального и методологического подходов.

СПИСОК ЛИТЕРАТУРЫ:

1. Исследование проблем и перспектив финансовых институтов, http://www.sas.com/offices/europe/russia/news/2004/pr20040809_2.html

2. Указание оперативного характера от 23.06.2004 № 70-Т “О типичных банковских рисках”: Вестник банка России. – 2004, №38, - М.: ЗАО "АЭИ "Прайм-ТАСС".

3. Ступаков В.С., Токаренко Г.С. Риск-менеджмент – М.: Финансы и статистика, 2005, 288с.

4. Цифрова Р.М., Андреева О.В. Управление рисками экономических систем – Саратов: Издательство Саратовского университета, 2001, 119с.

5. Чернова Г.В., Практика управления рисками на уровне предприятия – СПб.: Питер, 2000, 176 с.

ОРГАНИЗАЦИЯ ЗАЩИТЫ ДАННЫХ В СТАНДАРТЕ BLUETOOTH

Горягина Т.М., Трунов И.Л., Серогодский Д.И., Котегов М.Г., Лукьянов С.А.
Южный федеральный университет, Таганрогский технический институт

В последнее время технологии беспроводной связи применяются в самых разных областях деятельности человека. Это стало возможным благодаря созданию группы стандартов, отвечающих высоким эксплуатационным требованиям. Одним из них является стандарт Bluetooth. Изначально стандарт был разработан для подключения гарнитур к мобильным телефонам, но благодаря сочетанию хорошей пропускной способности (до 10 Мб/сек) и простоты программно-аппаратной реализации, область его применения очень расширилась. Сейчас системы Bluetooth инсталлируются на коммерческие транспортные средства для обеспечения связи с водителями, поддержки устройств «громкой» связи и для сбора данных, беспроводные устройства контроля физических параметров применяются в медицинских учреждениях. Такая популярность технологии накладывает повышенные требования на надежность и безопасность передачи данных. Существуют три основных типа атак на портативные устройства, оснащенные Bluetooth:

Bluejacking - используется способность устройств Bluetooth опознавать другие, расположенные поблизости устройства и посылать на них незапрошенные сообщения.

Bluesnarfing - используя этот прием, злоумышленник может соединиться с устройством, не сообщив об этом его владельцу, и получить доступ к сохраненным на аппарате данным.