4. *Клещев А. С., Артемьева И. Л.* Математические модели онтологий предметных областей. Ч. 2. Компоненты модели // НТИ. Сер. 2. 2001. № 3. С. 19–29.
5. *Калиниченко Л. А.* СИНТЕЗ: язык определения, проектирования и программирования интероперабельных сред неоднородных информационных ресурсов. М.: ИПИ РАН, 1993.
6. *Скотт Д. С.* Области в денотационной семантике // Математическая логика в программировании / Пер. с англ. М.: Мир, 1991. С. 58–118.

С. Д. Кулик, А. В. Жижилев, К. И. Ткаченко

АВТОМАТИЗИРОВАННЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВАЛЮТНОГО И ФОНДОВОГО РЫНКОВ

Введение

Некоторые исследования [1, 2, 3] и практика убедительно показывают, что различные «махинации» и *мошеннические действия* (МД) в сфере финансов [4, 5, 6, 8, 9] происходят именно там, где сконцентрировано большое количество денежных средств, например *ценных бумаг* (ЦБ) [12], и информации, связанной с этими средствами. На рынке FOREX (FOReign EXchange market) в рамках margin FOREX участниками торговли реализуются некоторые валютные спекулятивные операции с опорой на текущую информацию о ней. Каждая такая операция обязательно сопровождается актом обмена взаимной информацией (по соответствующим каналам связи), необходимой для выполнения коммерческих операций. Если эта информация (при передаче по каналам связи) подвергается искажению, то соответственно искажается и результат самой коммерческой операции. Искажения коммерческой операции являются целью злоумышленника и направлены в итоге на разорение одного из участников, получающего искаженную информацию, по которой он вынужден принимать неправильные для себя решения. Далее в работе деньги и ценные бумаги (как материальные объекты) не рассматриваются. Основное внимание сосредоточено на информации, связанной с этими объектами, например на информации, передаваемой по каналам связи, и на *автоматизированных средствах обеспечения информационной безопасности* (АСОИБ).

В настоящей работе предпринята попытка предварительного краткого анализа важных информационных проблем, сопутствующих практической торговле на рынке FOREX, а также рассмотрены возможные автоматизированные средства и некоторые пути учета и противодействия искажению информации, которая способствует злоупотреблению (МД) в торговле, на основе использования математических методов, обеспечивающих безопасность информационных технологий.

Человек-оператор, работающий на рынке FOREX, использует (для получения и передачи информации) различное *программное обеспечение* (ПО). Так, существует специальное нейросетевое ПО для получения информации, связанной с результатами прогнозирования состояния *финансового рынка* (ФР). На базе полученной информации человек-оператор принимает значимые для себя решения. Имеются [8] обучающиеся системы принятия *статистически оптимальных торговых решений* (СОТР) на ФР. С целью обучения операторов принятию правильных решений применяются генераторы для различных приложений. Для помощи человеку-оператору (на базе

информации, полученной по каналам связи, о текущем состоянии рынка) в принятии *торговых решений* (ТР) также разработано нейросетевое ПО для работы на ФР. Действуя на рынке и принимая то или иное решение (по искаженной информации), человек-оператор (например, трейдер) рискует потерять вложенные средства. Выполняемые им операции далеко не безопасны для его капитала (или клиента, чей капитал используется в данной финансовой операции на базе полученной информации). Далее под безопасной операцией будем понимать такую операцию, которая обеспечивает заданный уровень получения прибыли, т. е. является устойчивой (эффективной) к некоторым внешним воздействиям, искажающим информацию, передаваемую между участниками рынка и используемую в принятии решения. Методы защиты информации, обеспечивающие работу реализованных в автоматизированной системе алгоритмов с учетом возможных искажений, будем назвать эффективными. Соответственно методы, не обеспечивающие такой возможности работы ключевых алгоритмов, будем называть неэффективными. На практике эти методы обычно реализуются как АСОИБ. Рассмотрим виды *торговых операций* (ТО) рынка FOREX и информацию, связанную с ними, которая передается между участниками рынка по каналам связи и может быть искажена.

1. Виды торговых операций, проводимых на рынке FOREX, и передаваемая информация

На рынке FOREX осуществляются два вида ТО [4, 5]: реальные конверсионные (валютно-обменные) ТО; «финансовые игры», или же маржинальные ТО. На практике участниками реальной торговли валютой являются банки (именно они — активные участники рынка). Банки ставят перед собой не только цель купли-продажи валюты, но и цель ее реальной поставки. Заметим, что цели конверсионных сделок могут быть различными [6]. Для реализации спекулятивных целей достаточно хорошо подходит маржинальная торговля как на рынке FOREX, так и на рынке ЦБ [4, 5, 6, 9]. Маржинальная торговля на рынке FOREX осуществляется при взаимодействии в процессе торговли следующих пяти составных элементов [6]: трейдер; *дилинговый центр* (ДЦ); брокер; банк *маркет-мейкер* (БММ); международный *валютный рынок* (ВР) FOREX. Рассмотрим кратко схему их взаимодействия и передаваемую информацию.

А. Трейдер взаимодействует с ДЦ. К трейдеру на его *автоматизированное рабочее место* (АРМ) от ДЦ (по каналам связи) достаточно регулярно поступает информация о котировках *финансовых инструментов* (ФИ) (т. е. информация на АРМ трейдера о котировках валют). Трейдер на основе своей финансовой стратегии $\mathbf{S_Т}$ с учетом опыта предыдущей работы на рынке и текущей информации о котировках производит (путем выдачи управляющей информации по каналам связи) открытие (закрытие) своих позиций (т. е., собственно, и принимает текущее ТР). ДЦ имеет свою стратегию $\mathbf{S_{ДЦ}}$ и информацию по договорным обязательствам и выполняет своевременную передачу (по каналам связи) информации о ТР от трейдера к брокеру и передачу (по каналам связи) информации о результатах самих торгов к трейдеру.

Б. ДЦ взаимодействует с брокером. ДЦ, как правило, в режиме реального времени (по каналам связи) передает информацию о ТР от трейдеров к брокеру (например, банку-брокеру или же компании-брокеру). Брокер (имея свою стратегию $\mathbf{S_Б}$ и информацию по своим договорным обязательствам) принимает (по каналам связи) к исполнению ТР трейдеров, а также передает (по каналам связи) информацию о результатах торгов для ДЦ.

В. Брокер взаимодействует с БММ. Брокер в режиме реального времени (по каналам связи) получает информацию от ДЦ о ТР трейдеров, собирает их в торговые информационные пакеты по признаку типа сделки (продажа/покупка) и затем передает их (по каналам связи) в БММ. БММ (имея свою стратегию $\mathbf{S_{БММ}}$ и информацию о своих договорных обязательствах) на основе полученных пакетов ТР совершает взаимные виртуальные купли-продажи (без поставки

базовых активов, которые лежат в основе сделки), возвращает итоги торгов, причем дисбаланс по пакетам ТР он покрывает самостоятельно, так как имеет обязательства перед клиентами по обеспечению ликвидности рынка.

Таким образом, видно, что при торговле по каналам связи передается важная и очень значимая информация.

2. Искажения информации, передаваемой по каналам связи на рынке margin FOREX

Практика показывает, что деньги тех, кто выигрывает на рынке FOREX, — это деньги тех, кто их проигрывает. Причиной этого может являться именно искажение информации, которая доступна трейдеру. При этом важно отметить, что в настоящее время имеется достаточно слабая законодательная база, связанная хоть как-то с регламентом работы на ВР margin FOREX [3, 6].

Проведенный даже беглый анализ схемы взаимодействия информационных элементов рынка показывает, что возможно наличие некоторых «узких мест», которые на практике могут привести к искажению наиболее значимой информации (что и будет являться итогом в виде «разорения» трейдера), т. е. информационная безопасность трейдера может быть нарушена (поставлена под угрозу).

Существуют следующие 3 класса возможных методов искажения информации, которые открывают саму возможность злоупотреблений на margin FOREX:

I. Метод манипулирования информацией о стоимости ФИ маркет-мейкерами.

II. Метод манипулирования информацией о ФИ, подаваемых только на АРМ трейдеров.

III. Другие методы искажения информации.

Остановимся на этой классификации подробнее и рассмотрим классы **I** и **II**.

I. Возможные манипуляции информацией о курсах ФИ на уровне БММ

Дисбаланс реальных ТР у БММ обязан на практике покрываться самостоятельно. Это приводит к тому, что у операторов банка может появиться некоторый экономический интерес к деньгам своих клиентов. Рассмотрим такую возможную простую ситуацию на следующем условном примере. Допустим, брокер предоставил БММ два информационных пакета ТР трейдеров на продажу и на покупку по какой-то конкретной *валютной паре* (ВП). Пусть информационный пакет ТР на продажу — это **400** млн долларов, а информационный пакет ТР на покупку — это **500** млн долларов. Тогда БММ (который имеет обязательства по обеспечению ликвидности сделок) необходимо реально покрыть разницу в ТО в **100** млн долларов. Может случиться так, что БММ окажется выгодным **реально опустить** курс ФИ таким образом, чтобы дисбаланс открытых клиентами **длинных позиций** (в **100** млн долларов) обратился в проигрыш клиентов, т. е. в выигрыш самого БММ. Указанная схема, лежащая в основе «механизма» изменения информации о курсах валют, является достаточно идеализированной. Это связано с тем, что на рынке FOREX одновременно присутствует достаточно много БММ и у каждого из них есть свои собственные интересы по отношению к деньгам своих клиентов. На практике банки вынуждены вести «некоторую борьбу» и пытаться «относительно честным» путем завладеть деньгами своих клиентов (в приведенном выше примере — это **100** млн долларов).

БММ, в отличие от трейдеров, имеют реальные рычаги воздействия на текущие курсы ВП.

II. Возможные манипулирования информацией о курсах ФИ при их отображении на АРМы трейдеров (по инициативе БММ или ДЦ)

Этот вариант искажения информации (позволяющий реализовывать МД) на практике менее затратный, так как в этом случае не нужно манипулировать именно информацией о курсах ФИ в масштабах всего рынка, а достаточно лишь подавать только на АРМы своих клиентов искаженные, т. е. «выгодные или удобные» для себя, котировки. В подобных схемах МД могут участвовать не только ДЦ, но и БММ. На практике БММ может дорожить своей репутацией и лицензией,

однако ДЦ может и не стремиться к этому. Потому возможно, что действия (по искажению информации) подобных ДЦ иногда могут быть направлены именно на разорение своих клиентов (т. е. трейдеров). В такой ситуации реальные котировки валют могут, например, пропускаться через специальный фильтр, который будет **сужать** коридор прибыли путем повышения/понижения волатильности курса ВП. Также текущие котировки ВП могут дополняться некоторыми искусственными «скачками» их значений (т. е. фактически искажается информация), которые приводят к неоправданным срабатываниям STOP LOSS (ограничениям потерь) у трейдеров, что на практике сопровождается реальным закрытием их позиций с убытком. Также ДЦ могут прибегать к другим способам злоупотреблений («махинациям»), таким как намеренный обрыв связи с клиентом, многократные необоснованные переспросы о намерениях трейдера в случае его желания «усилить» выигрышную позицию или закрыть убыточную позицию и т. п. действия, которые при определенных обстоятельствах можно рассматривать (квалифицировать) как МД.

3. Математическая постановка задачи при разработке АСОИБ с учетом возможных искажений информации

Кратко рассмотрим проблему выбора показателя эффективности *технической системы* (ТС), в том числе и АСОИБ, используемой при торговле на рынке FOREX. Оценивать в АСОИБ эффективность можно как отдельной операции, так и всей ТС. На практике реальная ТС может быть представлена только одной операцией или совокупностью из целого ряда операций, которые выполняются в ТС.

Для того чтобы можно было судить об *эффективности* ТС (ЭТС) и сравнивать различные варианты, необходимо ввести совокупность *показателей эффективности* (ПЭ) и сформулировать критерии (или критерий) ЭТС. Обычно для каждого класса ТС применяют свои показатели эффективности с учетом специфики и *целевого назначения* ТС.

Опираясь на работы [17 и др.], сформулируем требования к показателю эффективности ТС, который должен: быть достаточно простым, понятным и обозримым; иметь ясный и однозначный физический смысл; быть чувствительным к варьируемым параметрам, значение которых необходимо определить для повышения ЭТС; соответствовать реальному процессу работы системы; допускать его оценку по экспериментальным данным и с помощью моделирования (по возможности, эти оценки должны быть *состоятельными*, *несмещенными* и *эффективными*).

Практика показала следующее. Для того чтобы ПЭ удовлетворяли перечисленным выше требованиям, необходимо [17]: разработать ПЭ так, чтобы они непосредственно отражали специфику ТС и соответствовали ее целевому назначению; выделить в составе ПЭ варьируемые параметры и выполнить с их помощью исследования ЭТС; проверить адекватность модели ТС, которая используется для оценки ТС по выбранным ПЭ; создать средства ускоренной оценки (при заданной точности) ПЭ, требующих чрезмерных затрат для их вычисления.

Известно, что подходящие, удачно выбранные показатели эффективности позволяют оценить качество системы (АСОИБ) с точки зрения ее эффективности и сравнить ее варианты по каждому из них. Наличие единого показателя, являющегося сверткой таких показателей, значительно облегчает разработчику выбор лучшего варианта системы (АСОИБ), обеспечивающего большую эффективность (например, безопасность). При этом состав набора таких показателей эффективности непосредственно вытекает (следует) из особенностей (специфики) систем (АСОИБ) и требований к ней (оперативность, способность правильно отвечать на запросы, небольшие затраты и т. п.).

Из приведенного выше краткого анализа возможных искажений информации, передаваемой по каналам связи при торговле на рынке FOREX, можно сделать вывод, что все искажения информации, в конечном итоге, направлены на то, чтобы трейдер (т. е. инвестор) в процессе

торговли принимал неверные (ошибочные или неэффективные) ТР. Поэтому математическую задачу, связанную с противодействием искажению информации в торговле, можно представить как задачу принятия СОТР, обладающих свойством робастности (т. е. статистической устойчивости) результатов к возможным вариациям (т. е. искажениям) исходных данных, из которых на практике извлекается необходимая информация. Как целевую функцию J, определяющую «качество» принимаемых ТР и АСОИБ с учетом искаженной информации, предлагается рассматривать выражение следующего вида:

$$J = \mathbf{M}\left[F\left(\vec{C}, j, h, \xi, Q\left(\vec{x}, \vec{C}\right)\right)\right] \Rightarrow \max_{\vec{C}}, \quad (1)$$

где M[ ] — *математическое ожидание* (МО) прибыли трейдера; $\vec{C} = (c_1, c_2, c_3, ..., c_m)$ — вектор **варьируемых** параметров *решающего правила* (РП); j — j-й маркет-мейкер (брокер), поставщик информации о котировках валют, где $j = 1, \ldots, M$; h — число шагов информационного прогноза (например, один шаг, т. е. $h = 1$); ξ — набор некоторых специальных параметров; $\vec{x} = (x_1, x_2, x_3, ..., x_n)$ — вектор некоторого случайного процесса, определяющего во времени значения статистических информационных прогнозов минимального и максимального значений курсов валют и фактических случайных значений курсов по отношению к их выполненным $\boldsymbol{h}$-шаговым прогнозам; $Q\left(\vec{x}, \vec{C}\right)$ — некоторая заранее заданная неслучайная функция, которая определяет собой конкретную формулу для оценивания «коридора прибыли».

Для практических целей вместо выражения (1) для оценки эффективности ТР и АСОИБ удобно использовать другое аналогичное выражение (2):

$$J = \mathbf{M}\left[F\left(\vec{C}, j, h, \xi, Q\left(\vec{x}(t_i), \vec{y}(t_i), \vec{C}\right)\right)\right] \Rightarrow \max_{\vec{C}}, \quad (2)$$

где $\mathbf{M}[\ ]$ — некоторая оценка МО прибыли (желательно иметь несмещенную оценку); $\vec{x}(t_i), \vec{y}(t_i)$ — вектора, соответственно, фактических значений курсов и их статистических информационных прогнозов; для каждого момента времени t_i эти вектора имеют одинаковую структуру; набор $\boldsymbol{h}$-шаговых прогнозов курсов по каждой ВП формируется на основании обработки статистической информации по курсам валют; $Q\left(\vec{x}(t_i), \vec{y}(t_i), \vec{C}\right)$ — некоторая заранее заданная неслучайная функция, которая определяет собой конкретную формулу для оценивания «коридора прибыли».

Частный показатель эффективности АСОИБ показывает некую характеристику системы, а критерий эффективности является, по сути, некоторым правилом, позволяющим по набору показателей принять решение об эффективности или неэффективности этой системы. В качестве частных показателей эффективности могут быть выбраны: $\boldsymbol{h}$, стратегии $\mathbf{S_Т}$, $\mathbf{S_{ДЦ}}$, $\mathbf{S_Б}$, $\mathbf{S_{БММ}}$, t_i и ряд других показателей.

Необходимо отметить, что число $\boldsymbol{h}$ шагов информационного прогноза в общем-то тоже является некоторым параметром РП. Далее можно полагать, что число шагов уже как-то предварительно выбрано, например, $h = 1$. Выражения (1) и (2) зависят в разной степени от стратегий $\mathbf{S_Т}$, $\mathbf{S_{ДЦ}}$, $\mathbf{S_Б}$, $\mathbf{S_{БММ}}$, применяемых на ранке FOREX, и эффективности АСОИБ. В соответствии со сформулированной выше математической задачей (1, 2), для поиска РП СОТР, одновременно отвечающего условию робастности оценок, требуется найти экстремум выражения (2) по вектору параметров в РП, при этом необходимо рассматривать «расширенную» модель задачи для j=1,2,…,M брокеров — поставщиков информации о котировках валют. Применительно к выражению (2) решение этой задачи фактически сводится к поиску экстремума функции регрессии (которая в данном случае представлена случайными оценками МО прибыли), в зависимости от вектора параметров $\vec{C} = (c_1, c_2, c_3, ..., c_m)$ в РП с учетом возможных искажений передаваемой по каналам связи информации и эффективности АСОИБ.

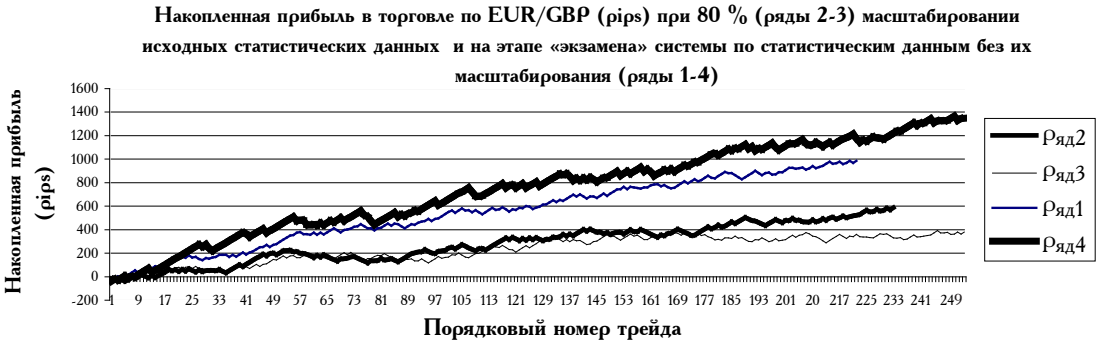
В свою очередь, «оценки» МО прибыли и их статистические характеристики зависят от статистических свойств информационных прогнозов и собственно статистических свойств

случайных процессов, с которыми отождествляются случайные изменения курсов валют (при возможном наличии искажений в передаваемой и получаемой информации). Вместе с тем если руководствоваться целью повышения точности информационного прогнозирования как «базы» для принятия СОТР, то современная теория [7, 10] дает исследователю ответ на этот вопрос. В частности, для повышения точности информационного прогнозирования следует использовать «оптимальные» алгоритмы, например фильтры Калмана, фильтры Винера — Колмогорова, а также другие математические фильтры на их основе. Максимально достижимая точность информационного прогнозирования подобных алгоритмов достигается за счет предварительной настройки их структуры и параметров на статистические свойства прогнозируемых случайных процессов. Необходимость учета большого объема априорной информации в «оптимальных» алгоритмах является естественным препятствием их использованию на практике. Поэтому для целей практики был выбран другой путь поиска экстремума выражения (2), основанный на использовании концепции обучающихся кибернетических систем [11].

Таким образом, предложенная постановка задачи позволяет учесть интересы трейдера и, самое главное, учесть наличие возможных искажений в передаваемой и получаемой информации по каналам связи при разработке АСОИБ.

4. Результаты исследований АСОИБ

Для проведения необходимых исследований и экспериментов для АСОИБ было разработано ПО, в частности PInterface [15] и специальная база данных PDB [14].



При «оптимальном» решающем правиле (ряды 2,4). При «робастном» решающем правиле (ряды 1,3).

Рис. 1.

Поиск устойчивого РП принятия решений, способного учитывать возможное наличие искажений в передаваемой и получаемой информации (по каналам связи) на рынке margin FOREX, проводился для известной торговой системы ProfitMaker [6]. Для ее «обучения» (по критерию экстремума целевой функции, аналогичной (2)) использовалась информация в виде массива статистических данных по ВП EUR/GBP за период 2000—2006 г. в двух вариантах: «неискаженная информация в данных» (т. е. 100-процентный масштаб) и в случае искажения информации в данных (т. е. 80-процентный масштаб). Результаты исследований эффективности торговых решений (с учетом искажения информации, передаваемой и получаемой по каналам связи) представлены на рис. 1. Из них можно сделать следующий вывод. Если бы заранее были известны статистические свойства случайных процессов, определяющих информацию о котировках валют, то, применяя необходимые методы для обучения системы ProfitMaker, можно добиться достаточно приемлемых результатов (рис. 1, ряды 4, 2). Использование предварительно найденных «оптимальных» РП по «искаженной информации» в массивах данных приводит к плохим результатам (на рис. 1 этот случай не показан). Для ВП EUR/GBP специальными методами

можно на практике пытаться учитывать искажения в передаваемой и получаемой информации (по каналам связи) и в итоге противодействовать возможным злоупотреблениям за счет синтеза единого статистически устойчивого РП (рис. 1, ряды 1 и 3). Полученные результаты позволили разработать специальное устройство [13], в состав которого (как и в системе ProfitMaker) входит некоторый блок информационного прогноза. В настоящее время уже получено положительное решение о выдачи патента и получен сам патент на устройство в виде полезной модели.

5. Возможные искажения информации на рынке ценных бумаг

Далее под документом понимается не только обычный документ, но и электронный документ. Например, вексель или ценная бумага имеет материальное представление не только в виде бумажного документа, но и в электронном виде. Основное внимание будет уделено не самому документу, а именно информации, содержащейся в нем. Это связано с тем, что искажение именно этой информации в векселе позволяет совершать возможные злоупотребления в торговле на рынке ценных бумаг.

Как сообщает ГИЦ МВД России в своем статистическом сборнике «Преступность и правонарушения 1998» за 1999 г., на территории нашей страны в 1998 г. было выявлено **10,6** тысячи случаев изготовления, сбыта поддельных денег или ЦБ. Отметим, что больше **50 %** ущерба причиняется именно поддельными ЦБ. В общем случае ЦБ может быть представлена не только в бумажном виде, но и в электронном, передаваемом по каналам связи. Сама информация в таком электронном документе может быть целенаправленно искажена злоумышленником. Все это угрожает не только экономической безопасности нашей страны, но и информационной безопасности. Рассмотрим кратко основные виды МД, совершаемых с помощью векселей. Чаще всего МД совершаются со стороны векселедателя (трассанта). Преступники пользуются тем, что в соответствии с действующим законодательством РФ вексель не может быть составлен произвольным способом. Отсутствие или неправильное составление одного из реквизитов векселя (т. е. искажение информации в нем) может повлечь его ничтожность и утрату вексельной силы. В суде такая «*ценная бумага*» не будет рассматриваться уже как вексель. Для совершения обмана преступники заведомо готовят неправильно составленные тексты векселей (т. е. искажают информацию в нем), которые не позволяют их опротестовать и получить по ним причитающиеся средства [18. С. 128]. Специалисты различают две большие группы причин недействительности документа, «*претендующего*» на вексельную силу [19]: дефект формы векселя и дефект содержания векселя. Мы не будем делать никаких *тонких* различий, а будем просто говорить о дефекте векселя. Утрата *вексельной силы* документа может возникнуть в результате следующих его дефектов (будем частично придерживаться терминологии и некоторых идей из работы [19]), представленных в таблице 1. Для того чтобы обучать распознаванию фальшивых векселей будущих экспертов-криминалистов или переобучать (стажировать) имеющихся экспертов, необходимо иметь достаточное число разных образцов поддельных векселей, представленных, например, в виде электронного документа, содержащего искаженную информацию.

Таблица 1. Возможные искажения информации в результате дефекта векселя

№	Описание искажения
Д1	отсутствует или неправильно составлена (ОИНС) «*вексельная метка*»
Д2	ОИНС «*простое и ничем не обусловленное предложение (обещание) уплатить определенную сумму*»
Д3	ОИНС «*наименование того, кто должен платить (плательщика)*»
Д4	ОИНС «*указание срока платежа*»

Д5	ОИНС «*указание места, в котором должен быть совершен платеж*»
Д6	ОИНС «*наименование того, кому или по приказу кого должен быть совершен платеж*»
Д7	ОИНС «*указание даты и места составления векселя*»
Д8	ОИНС «*подпись того, кто выдает вексель (векселедателя)*»
Д9	наличие каких-либо дополнительных сведений, «*приводящих к потере вексельной силы*»

На практике не всегда имеется так много таких разнообразных электронных документов. Было предложено использовать специальный генератор, позволяющий генерировать искаженную информацию, представляющую тексты поддельных векселей (или векселей, которые могут быть оспорены в суде).

Опираясь на ранее разработанные генераторы [16 и др.] и на инструментальные средства, для них был выполнен этап разработки требуемого генератора GCB и алгоритма ALG-B его работы. Область документа разбита на информационные зоны (или поля). В этих полях содержащаяся информация может быть искажена, что и будет отражать возможные признаки подделки (или *дефектов*). Можно полагать, что передаваемая и получаемая информация (по каналам связи) может быть искажена, что и приведет к появлению признаков подделки. Алгоритм ALG-B можно представить в виде 7 шагов (таблица 2).

Таблица 2. Алгоритм ALG-B работы генератора GCB

№ шага	**Описание шага (пункта) алгоритма**
1	Задать число N генерируемых вариантов и поля векселя, которые будут искажаться в процессе генерации, а также служебные параметры (предполагается, что все необходимые шаблоны «фальшивок» для изменения полей векселя уже заданы и находятся в базе данных). Присвоить $i = 0$.
2	Проверить допустимость входных данных для генерации (при необходимости выдать сообщение и если невозможна дальнейшая работа генератора, то прекратить работу).
3	Выполнить $i = i + 1$.
4	Сформировать i-й очередной законченный блок информации (фальшивого векселя) и выдать его пользователю.
5	Если $i < N$, то перейти к шагу 3.
6	Подготовить отчет о генерации информации поддельных векселей (например, номеров векселей с указанием признаков (*дефектов*) подделки) и выдать его пользователю.
7	СТОП.

Полученные результаты позволили разработать устройство [13], в состав которого входит специальный блок генерирования выборки. Это устройство позволяет выявлять фальшивые документы (содержащие искаженную информацию) на русском языке, в том числе и векселя.

Выводы

На рынке FOREX (с точки зрения возможных МД и соответствующих им финансовых операций) осуществляется некоторое перераспределение финансовых ресурсов от одних владельцев в пользу других из-за наличия искажений передаваемой и получаемой информации (по каналам связи). Показано, что задача противодействия возможным МД в торговле может быть представлена как некоторая задача разработки АСОИБ и синтеза СОТР, обладающих свойством робастности

(статистической устойчивости результатов) к возможным вариациям исходных данных, связанных с возможными искажениями передаваемой и получаемой информации (по каналам связи).

Предложены частные показатели эффективности и выбран критерий эффективности с учетом возможных искажений передаваемой и получаемой информации (по каналам связи) для оценки эффективности торговых решений и АСОИБ. Получены данные, свидетельствующие о возможном существовании некоторых робастных решающих правил для принятия торговых решений с учетом искажений передаваемой и получаемой информации, имеющей место на рынке FOREX.

Выполнен краткий анализ возможных дефектов векселей, приводящих к возможным искажениям передаваемой и получаемой информации (по каналам связи). Разработан алгоритм ALG-B работы генератора GCB и сам генератор GCB данных, содержащих заданную искаженную информацию, связанную с поддельными векселями. Этот набор сведений, содержащий заданный набор искажений в информации о векселях, предлагается использовать на практике для обучения курсантов и для переподготовки экспертов по работе с ЦБ.

СПИСОК ЛИТЕРАТУРЫ:

1. *Кулик С. Д., Фролов Д. Б.* Защита АФИПС и правовые вопросы разработки вредоносных программ // Безопасность информационных технологий. 2001. № 3. С. 35–38.
2. *Кулик С. Д., Стариков Е. В., Кузнецов В. В., Белоусов А. Г., Белоусов Г. Г.* Защита денежных знаков и ценных бумаг – фундамент экономической безопасности России // Безопасность информационных технологий. 2002. № 1. С. 52–57.
3. *Кулик С. Д.* Проектирование АФИПС криминалистического назначения // Безопасность информационных технологий. 2002. № 1. С. 78–81.
4. *Шарп У. Ф., Бэйли Д. В., Александер Г. Д.* Инвестиции. М.: Инфра, 1999.
5. *Фаббоци Фрэнк Дж.* Управление инвестициями. М.: Инфра, 2000.
6. *Жижилев В. И.* Оптимальные стратегии извлечения прибыли на рынке FOREX и рынке ценных бумаг. М.: Финансовый консультант, 2002.
7. Фильтрация и стохастическое управление в динамических системах / Под ред. К. Леондеса. М.: Мир, 1980.
8. *Кулик С. Д., Жижилев А. В.* Обучающиеся системы принятия статистически оптимальных торговых решений на финансовом рынке // Актуальные проблемы управления – 2007. Материалы 12-й Международной научно-практической конференции. Вып. 4. М.: ГУУ, 2007. С. 44–47.
9. *Кулик С. Д., Жижилев А. В.* Оценка эффективности статистически оптимальных торговых решений на рынке FOREX // Научная сессия МИФИ – 2008. Сб. науч. трудов в 15 т. М.: МИФИ, 2008. Т. 13. С. 29–30.
10. *Браммер К., Зиффлинг Г.* Фильтр Калмана – Бьюси. М.: Наука, 1982.
11. *Цыпкин Я. З.* Основы теории обучающихся систем. М.: Наука, 1970.
12. *Кулик С. Д.* Как защититься от мошенничества на рынке ценных бумаг // Финансы России. 2001. № 2. С. 42–43.
13. *Кулик С. Д., Никонец Д. А., Ткаченко К. И., Жижилев А. В.* Заявка на выдачу Свидетельства на полезную модель, РФ (RU), кл. МПК7 G 07 D 7/00. Устройство определения фальшивых рукописных документов на русском языке. – Заявка №2007147832/20; Заяв. 25.12.2007; Приоритет от 25.12.2007. – (РОСПАТЕНТ).
14. *Кулик С. Д., Жижилев А. В.* Свидетельство на БД РФ №2007620334 «База данных решателя v.1.0» (PDB). – Заявка № 2007620233; Заяв. 31.07.2007; Зарегистр. 26.10.2007. – (РОСПАТЕНТ).
15. *Кулик С. Д., Жижилев А. В.* Свидетельство на программу РФ №2007614119 «Программа принятия решений и представления данных для лица, принимающего решения на финансовом рынке» (PInterface). – Заявка №2007613119; Заяв. 31.07.2007; Зарегистр. 26.10.2007. – (РОСПАТЕНТ).
16. *Кулик С. Д., Ткаченко К. И.* Генератор изменений текста // Научная сессия МИФИ – 2008. Сб. науч. трудов в 15 т. М.: МИФИ, 2008. Т. 13. С. 83–84.
17. *Кулик С. Д.* Теория принятия решений (элементы теории проверки вероятных гипотез). М.: МИФИ, 2007.
18. *Ларичев В. Д., Спирин Г. М.* Коммерческое мошенничество в России. М.: Экзамен, 2001. – 256 с.
19. *Гудков Ф. А.* Вексель. Дефекты формы. М.: Интеркрим-пресс, 2000.