СПИСОК ЛИТЕРАТУРЫ:

1. *Темников В. А., Шарий Т. В., Темникова Е. Л., Конфорович И. В.* Голосовая аутентификация операторов, использующих в процессе работы нормативно установленную фразеологию // Інформаційна безпека. 2011. № 1 (5). С. 126–131.
2. Федеральный закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
3. *Ложников П. С.* Распознавание пользователей в системах дистанционного образования: обзор // Образовательные технологии и общество (Educational Technology & Society). 2001. № 4 (2). С. 211–216.
4. *Финько О. А., Елисеев Н. И.* Установление подлинности информации, полученной из недоверенной среды // Информационные технологии, связь и защита информации МВД России. 2012. № 2. С. 53–55.
5. *Петраков А. В.* Защитные информационные технологии аудиовидеоэлектросвязи. Учебное пособие. М.: Энергоатомиздат, 2010. – 616 с.

Н. А. Евстифеева, Г. О. Крылов, В. Е. Рябков

ФОРМИРОВАНИЕ ПРИЗНАКОВОГО ПРОСТРАНСТВА ДЛЯ РЕШЕНИЯ ЗАДАЧ АНАЛИЗА РЕПУТАЦИОННЫХ РИСКОВ КРЕДИТНЫХ ОРГАНИЗАЦИЙ КАК СУБЪЕКТОВ ФИНАНСОВОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Важнейшее условие обеспечения национальной безопасности государства — стабильность его экономической системы. Одним из основных элементов этой системы в любом развитом государстве являются кредитные организации.

Вместе с тем перманентно остро стоит вопрос борьбы с коррупционными проявлениями и теневым сектором экономики. Необходимыми условиями их функционирования являются каналы, обеспечивающие значительные объемы наличных денежных средств, мобильных финансовых инструментов, а также вывод денежных средств за рубеж, в частности в оффшорные зоны. Обеспечение достаточного объема этих потоков возможно только при непосредственном участии в процессе отдельных сотрудников банков либо целиком конкретных кредитных организаций. Таким образом, своевременное выявление проблемных кредитных организаций оказывается важным аспектом поддержания стабильности и оздоровления экономики государства.

К эффективным решениям задачи выявления неблагонадежных кредитных организаций следует отнести проведение их анализа в терминах теории распознавания образов. Адекватность такого анализа существенно зависит от формирования признакового пространства.

Для целей всесторонней оценки благонадежности кредитной организации как ячейки экономической системы страны необходимо провести оценку трех основных аспектов их функционирования:

1) собственные экономические показатели банка;

2) объем и состав клиентского портфеля банка;

3) качество системы внутреннего контроля банка.

Каждый из перечисленных аспектов характеризуется своим набором показателей. Оптимальным представляется описанный ниже состав.

I. Собственные экономические показатели банка:

1) Активы. Характеризуют объем имеющихся в распоряжении банка объектов собственности. Позволяют оценить благонадежность и устойчивость кредитной организации. Помимо абсолютного показателя целесообразно также задействовать показатель прироста относительно предыдущего периода.

2) Капитал. Характеризует объем всего имеющегося в распоряжении банка имущества в денежном эквиваленте. Помимо абсолютного показателя целесообразно также задействовать показатель прироста относительно предыдущего периода.

3) Ценные бумаги. Характеризуют объем выпущенных организацией ценных бумаг. Для обеспечения сопоставимости величин у организаций различного размера целесообразно проводить нормирование данной величины на размер капитала банка.

4) Обороты средств в банкоматах. Показывают интенсивность операций в банкоматах, могут служить косвенным индикатором операций с наличными денежными средствами, проводимых в организации. Для обеспечения сопоставимости величин у организаций различного размера целесообразно проводить нормирование данной величины на размер капитала банка.

II. Объем и состав клиентского портфеля банка:

1) Кредиты предприятиям. Позволяют оценить объемы, в которых востребованы услуги данной организации у юридических лиц. Для обеспечения сопоставимости величин у организаций различного размера целесообразно проводить нормирование данной величины на размер капитала банка.

2) Потребительские кредиты. Характеризуют объемы услуг, оказываемых физическим лицам. Для обеспечения сопоставимости величин у организаций различного размера целесообразно проводить нормирование данной величины на размер капитала банка.

3) Расчетные счета. Характеризуют размеры клиентского портфеля организации. Помимо абсолютного показателя целесообразно также задействовать показатель прироста относительно предыдущего периода.

4) Вклады физических лиц. Характеризуют объем денежных средств населения, имеющихся в распоряжении банка. Помимо абсолютного показателя целесообразно также задействовать показатель прироста относительно предыдущего периода. Для обеспечения сопоставимости величин у организаций различного размера целесообразно проводить нормирование данной величины на размер капитала банка.

III. Качество системы внутреннего контроля банка:

1) Качественный состав предоставляемой подразделением информации. Оценивается соотношение количества сообщений, переданных организацией по кодам обязательного контроля и по результатам работы внутреннего контроля (подозрительных операций). Причем целесообразно проводить оценку как по количеству сообщений, так и по общей сумме проводимых операций. При эффективной работе подразделения внутреннего контроля организации данные показатели должны составлять более 50 %, что при минимальном количестве нарушений свидетельствует об интенсивной работе организации по выявлению и информированию о подобных фактах.

2) Количество нарушений. Характеризует качественную составляющую предоставляемой информации. К таковой относится количество операций обязательного контроля по коду 6001, количество сообщений с существенным искажением информации и сообщений по кодам обязательного контроля на сумму ниже пороговой. Количество нарушений целесообразно нормировать через отношение к общему числу сообщений, переданных организацией.

3) Количество непредставленных сообщений. Сообщения, не представленные организацией, выявляются путем проведения перекрестного анализа информации. Данный показатель также целесообразно рассматривать как относительный и нормировать на общее количество сообщений, переданных организацией.

Таким образом, имеем численные показатели, позволяющие получить всестороннюю характеристику надежности кредитной организации и оценить ее устойчивость

СПИСОК ЛИТЕРАТУРЫ:

1. *Фомин Я. А.* Распознавание образов. Теория и применение. М.: ФАЗИС, 2010

Е. В. Елистратова, М. В. Мамаев

МЕТОДИКА ПРОВЕДЕНИЯ ТЕСТА НА ПРОНИКНОВЕНИЕ В ЗАЩИЩЕННЫЕ ХРАНИЛИЩА ОС GOOGLE ANDROID МОБИЛЬНЫХ УСТРОЙСТВ

В настоящее время мобильные устройства под управлением операционной системы (ОС) Google Android в силу своих характеристик и сфер применения являются централизованными хранилищами персональных данных, потенциально представляющих интерес для злоумышленника [1]. В связи с этим важной задачей является оценка защищенности информации в рассматриваемых устройствах.

Выявление угроз защищенности проводится с использованием методов и средств, предназначенных для всестороннего исследования систем с целью обнаружения «слабых мест», которые могут привести к нарушениям безопасности данных. Эффективным способом обнаружения угроз является метод «тестирование на проникновение», основанный на моделировании несанкционированной атаки [2].

В докладе представлена разработанная автором методика проведения теста на проникновение во внутренние хранилища ОС Google Android мобильного устройства для выявления угроз безопасности персональных данных. Тестирование на проникновение основано на моделировании действий злоумышленника, имеющего физический доступ к мобильному устройству, и осуществляется по следующей схеме:

1) анализ общей информации о мобильном устройстве;

2) извлечение и анализ данных о суперпользователе ОС;

3) исследование приложений, функционирующих в ОС, особенностей хранения ими данных;

4) выбор сценария моделирования атаки (получение доступа к внутренним хранилищам ОС):

–расширенные привилегии предоставлены;

–расширенные привилегии не предоставлены.

Практическая апробация разработанной методики и реализующих ее программных средств подтвердила их пригодность для выявления угроз защищенности данных в хранилищах мобильных устройств. Установлено, что большинство приложений ОС Google Android имеют слабый механизм защиты персональных данных, не предусматривающий шифрование. В силу этого следует использовать дополнительные методы и средства для повышения защищенности хранения данных соответствующими приложениями.

СПИСОК ЛИТЕРАТУРЫ:

1. *Михайлов Д. М., Жуков И. Ю.* Защита мобильных телефонов от атак. М.: Фойлис, 2011. С. 8–10.
2. *Wilhelm T.* Professional Penetration Testing // Syngress. 2009. P. 15–18.