УДК 004.056

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА ПРИ ОБЕСПЕЧЕНИИ ЗАЩИЩЕННОСТИ СИСТЕМ ИНТЕРНЕТ-БАНКИНГА

М.В. ТУМБИНСКАЯ,
кандидат технических наук, доцент кафедры систем информационной безопасности
E-mail: tumbinskaya@inbox.ru
Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань, Российская Федерация

Предмет/тема. *На сегодняшний день большинство банковских организаций используют в своей деятельности информационные системы интернет-банкинга или системы дистанционного банковского обслуживания. Это просто и удобно как для клиентов банковских организаций, так и для самих банков, но не всегда безопасно.*

Цели/задачи. *Вопросы информационной безопасности интернет-банкинга актуальны, ведь число мошеннических операций (атак) со стороны киберпреступников (хакеров) только растет. Причем реальное количество киберпреступлений намного выше, чем данные официальной статистики, банковские организации не спешат раскрывать информацию об успешно реализованных атаках киберпреступников. Статья посвящена вопросам защиты информации в информационных системах интернет-банкинга и нацелена на сохранение целостности конфиденциальной информации.*

Методология. *В работе предложена обобщенная структурная схема информационной системы интернет-банкинга, которая отражает модульную архитектуру системы, взаимосвязи пользователей и контур управления. Предложена модель информационной системы интернет-банкинга, использование которой позволит минимизировать количество атак киберпреступников, оптимизировать и совершенствовать комплексную систему информационной безопасности организаций экономической и социальной сферы, повысить эффективность использования защищенной информационной системы интернет-банкинга, выбрать правильную стратегию развития услуги интернет-банкинга.*

Результаты. *Модель информационной системы интернет-банкинга позволит оценить уровень защищенности системы, который определяется путем решения задачи поддержки принятия решений в слабо структурированной предметной области, характеризующейся разнотипными показателями. Предложена теоретико-множественная модель поддержки принятия решений при управлении информационной безопасностью информационных систем интернет-банкинга, позволяющая накапливать аналитическую информацию о реализуемых угрозах киберпреступниками, обеспечить автоматизированную поддержку принятия решений по вопросам нейтрализации атак киберпреступников, обеспечения мер защиты конфиденциальной информации, облегчить процесс выработки управляющих воздействий. В статье описана семантическая обобщенная схема хищения конфиденциальной информации в информационных системах интернет-банкинга, представлена формализация модели киберпреступника, характеризующаяся личностными параметрами нарушителя и сценариями действий по хищению конфиденциальной информации в системе интернет-банкинга. В основу модели киберпреступника заложены типовые образы киберпреступника, которые позволят определить потенциального нарушителя в системе интернет-банкинга.*

Выводы/значимость. *Предложенные решения позволят увеличить мощность информационной безопасности информационной системы интернет-банкинга, увеличить эффективность и качество принятия управленческих решений по защите конфиденциальной информации.*

Ключевые слова: *информационная безопасность, информационная система, интернет-банкинг, киберпреступник, принятие решений, моделирование, атаки и угрозы*

В настоящее время происходит масштабная информатизация и глобализация общества. Современные web-технологии дают возможность пользователям использовать on-line сервисы для распределения и оптимизации своих ресурсов, повышения качества жизнедеятельности, получения нового вида услуг. Между тем реальностью стали угрозы и вызовы в сфере кибербезопасности, на которые надо давать адекватный ответ. Так, на научной конференции по кибербезопасности, которая прошла в марте 2015 г. в Московском государственном университете, заместитель Председателя Правительства РФ Д. Рогозин сообщил о создании системы безопасности и противодействия киберугрозам[1].

Новая система безопасности и противодействия киберугрозам будет основана на применении «умного» оружия. Д. Рогозин выделил 3 типа угроз, которым должна будет противостоять система:

1) угрозы, исходящие от коалиций стран или более сильного противника;
2) угрозы от равных противников в киберпространстве;
3) угрозы от более слабых противников, в частности, от различных террористических организаций.

Российская государственная корпорация «Ростех» (до 23.07.2014 – ГК «Ростехнологии») выступала с подобной инициативой и ранее. Так, в январе 2015 г. было создано специальное подразделение CERT (Computer Emergency Response Team, команда реагирования на компьютерные угрозы), которое выполняет функцию центра компетенции по информационным технологиям, информационной безопасности и телекоммуникациям.

Интернет-банкинг – это новый вид услуги современной социально-экономической сферы, которая обладает множеством преимуществ, за ней – большое будущее. Популярность данной услуги не вызывает сомнения. Согласно имеющимся данным, существует прямая зависимость между полнотой функциональных возможностей и удобством использования информационных систем интернет-банкинга (чем большим функционалом обладает система интернет-банкинга, тем более дружественнее ее интерфейс)[2]. Обладатели *систем интернет-банкинга* (банковские организации) заинтересованы в их совершенствовании, повышении качества обслуживания, расширении функциональных возможностей, информационной безопасности. Заинтересованность банковских организаций в развитии собственных систем интернет-банкинга[3] показана на рис. 1.

Массовое использование информационных систем интернет-банкинга порождает проблему киберпреступлений. Интернет-банкинг – легкая «добыча» для киберпреступников. Первые попытки кибероперацией по хищению денежных средств были сделаны мошенниками еще в 2009 г. Киберпреступники находят все более оригинальные алгоритмы по реализации атак на информационные системы интернет-банкинга и хищению денежных средств. На сегодняшний день при удачной атаке киберпреступник может получить практически неограниченные возможности по управлению уязвимой информационной системой интернет-банкинга. Анализ литературы [1, 2] свидетельствует о том, что, несмотря на интенсивные исследования в области разработки систем защиты информации, проблема обеспечения информационной безопасности остается чрезвычайно актуальной, требует разработки новых подходов к ее решению.

Анализ литературных источников [3, 5–9] показал, что киберпреступления в системах интернет-банкинга имеют тенденцию к росту. Динамика статистических данных за 2014 г. представлена на рис. 2. Среднее значение количества персональных компьютеров, атакованных вредоносным программным обеспечением при использовании информационных систем интернет-банкинга, составило 244 380 шт.

Потенциальных нарушителей можно разделить на внутренних нарушителей из числа сотрудников банковской организации и внешних нарушителей – киберпреступников информационной системы

[1] В России создают новую систему противодействия киберугрозам. URL: https://hi-tech.mail.ru/news/new-syber-security-system-in-russia.html.

[2] Системы дистанционного банковского обслуживания (ДБО). URL: http://tadviser.ru.

[3] Крупные компании не защищены даже от неквалифицированных киберпреступников. URL: http://crn.ru/news/detail.php?ID=87552.

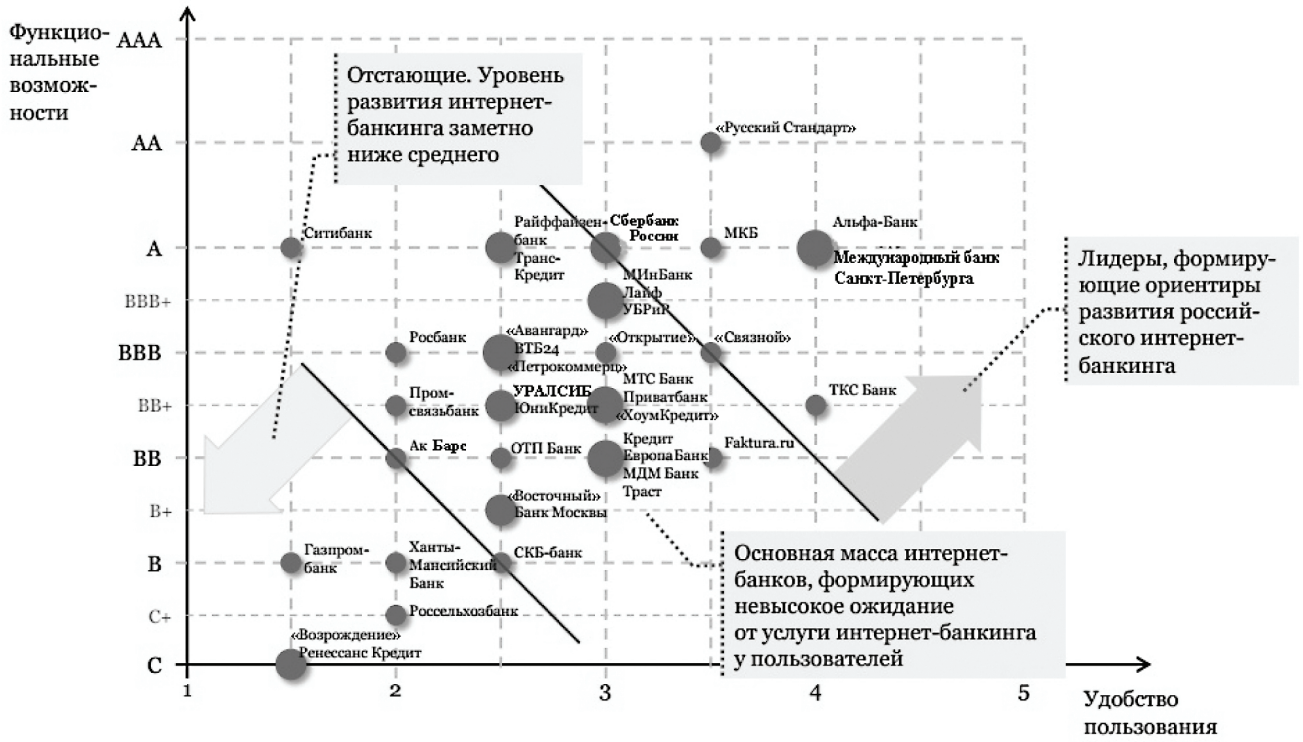

Рис. 1. Распределение банковских организаций по качеству систем интернет-банкинга

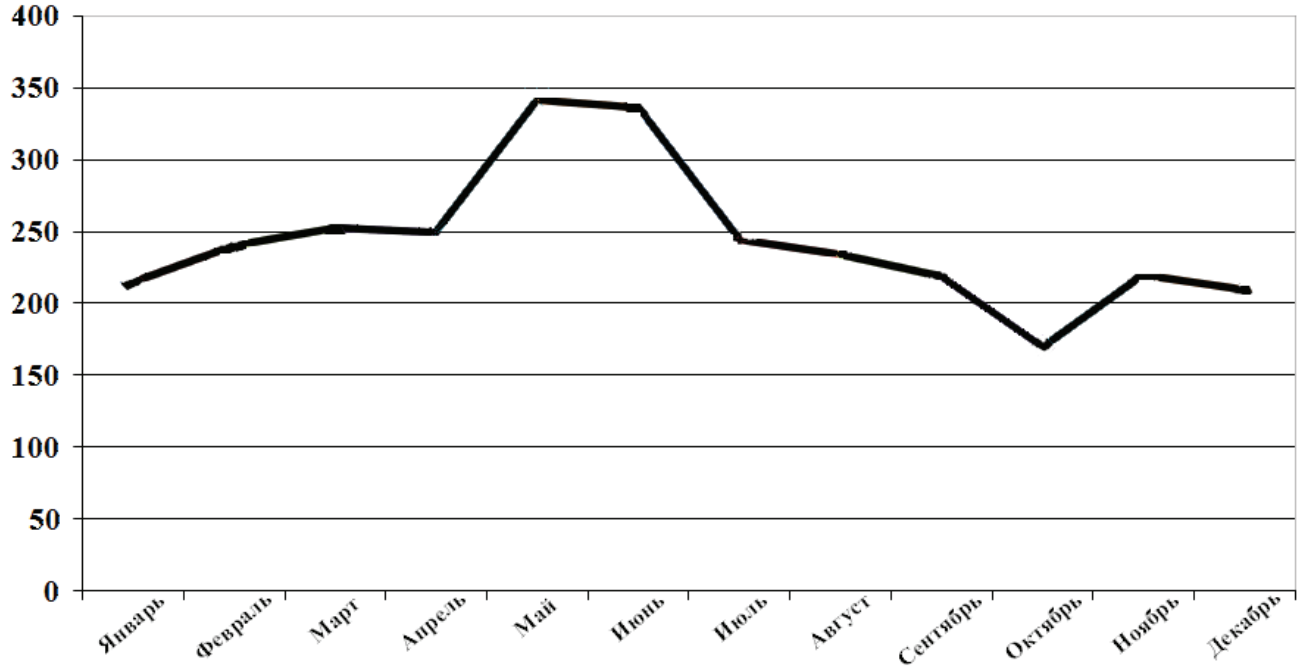

Рис. 2. Количество киберпреступлений в системах интернет-банкинга за 2014 г., тыс. ед.

интернет-банкинга. Предполагается, что потенциальный киберпреступник обладает высокой квалификацией, знаниями в IT-сфере, программно-аппаратными средствами реализации атаки. В связи с этим возникает необходимость в комплексном выборе мер и средств обеспечения защиты информации в системах интернет-банкинга от умышленного ее разрушения, кражи, порчи, несанкционированного доступа, чтения и копирования киберпреступниками.

Предлагается модель системы поддержки принятия решений при управлении информационной

безопасностью в информационных системах интернет-банкинга, использование которой обеспечит противодействие атакам киберпреступников, оптимизацию и совершенствование информационной безопасности, повышение эффективности использования защищенной информационной системы интернет-банкинга.

Программная реализация модели системы поддержки принятия решений может являться автономным модулем информационной системы интернет-банкинга, которая позволит вырабатывать рекомендации по обеспечению информационной безопасности системы интернет-банкинга. Модель системы поддержки принятия решений взаимодействует с моделью угроз, моделью киберпреступника на базе существующих (действующих) средств защиты информации и нормативных документов ФСБ и ФСТЭК России[4]. Структурная схема информационной системы интернет-банкинга, которая отражает модульную архитектуру системы, взаимосвязи пользователей и контур управления, представлена на рис. 3.

Системную модель информационной системы интернет-банкинга можно представить в виде:

$$S^{ib} = \left\langle User, Tr, M^{p}, Pr, T_r^u \right\rangle, \quad (1)$$

где $User$ – пользователи (клиенты) информационной системы интернет-банкинга, $User = user_i \cup user_j$;

$user_i = \{user_1,\ user_2,\ ...,\ user_m\}$ – легальные пользователи информационной системы интернет-банкинга;

$user_j = \{user_1, user_2, ..., user_s\}$ – киберпреступники информационной системы интернет-банкинга;

$Tr = \{tr_1,\ tr_2,\ ...,\ tr_\gamma\}$ – множество транзакций от пользователей $User$;

M^p – теоретико-множественная модель поддержки принятия решений;

Pr – параметр, характеризующий электронную банковскую деятельность;

$T_r^u = \{0;\ 1\}$ – выходной параметр S^{ib}, причем $T_r^u = 1$ в случае если транзакция выполнена успешно, $T_r^u = 0$ в противном случае.

Теоретико-множественная модель поддержки принятия решений M^p применяется при управлении информационной безопасностью информационных систем интернет-банкинга:

$$M^{p} = \left\langle L, N, \Theta \right\rangle, \quad (2)$$

[4] Федеральная служба по техническому и экспортному контролю (ФСТЭК России). URL: http://fstec.ru.

где L – входной параметр модели M^p;

N – обобщенный параметр модели M^p, характеризующий процесс поддержки принятия решений;

Θ – выходной параметр модели M^p, представляет собой рекомендации по обеспечению информационной безопасности информационной системы интернет-банкинга:

$$\Theta = \{\theta_\phi \mid \phi = \overline{1,\omega}\};$$

θ_1 – рекомендации по совершенствованию аппаратной защиты информации;

θ_2 – рекомендации по совершенствованию программной защиты информации;

θ_3 – рекомендации по совершенствованию организационно-правовой части защиты информации;

θ_4 – рекомендации по совершенствованию физической защиты информации.

Использование системной модели информационной системы интернет-банкинга позволит минимизировать количество атак киберпреступников, оптимизировать и совершенствовать комплексную систему информационной безопасности организаций экономической и социальной сферы, повысить эффективность использования защищенной информационной системы интернет-банкинга, выбрать правильную стратегию развития услуги интернет-банкинга.

Предложенная теоретико-множественная модель поддержки принятия решений при управлении информационной безопасностью информационных систем интернет-банкинга позволит накапливать аналитическую информацию о реализуемых угрозах киберпреступниками, обеспечить автоматизированную поддержку принятия решений по вопросам нейтрализации атак киберпреступников, обеспечения мер защиты конфиденциальной информации, облегчить процесс выработки управляющих воздействий.

Входной параметр модели M^p можно представить в виде выражения:

$$L = \left\langle Z^{user}, M^{ug}, S_z, Y, M^k, ND \right\rangle, \quad (3)$$

где Z^{user} – запрос (проблемная ситуация);

M^{ug} – модель угроз, на основе которой определяется вероятность реализации угроз p^j в информационной системе интернет-банкинга;

$\beta : M^{ug} \to p^j$;

$p^j = \{p^1, p^2, p^3\}$;

$p^1 = \{0;1\}$;

$p^1 = 1$ в случае если вероятность угроз в информационной системе интернет-банкинга очень высокая;

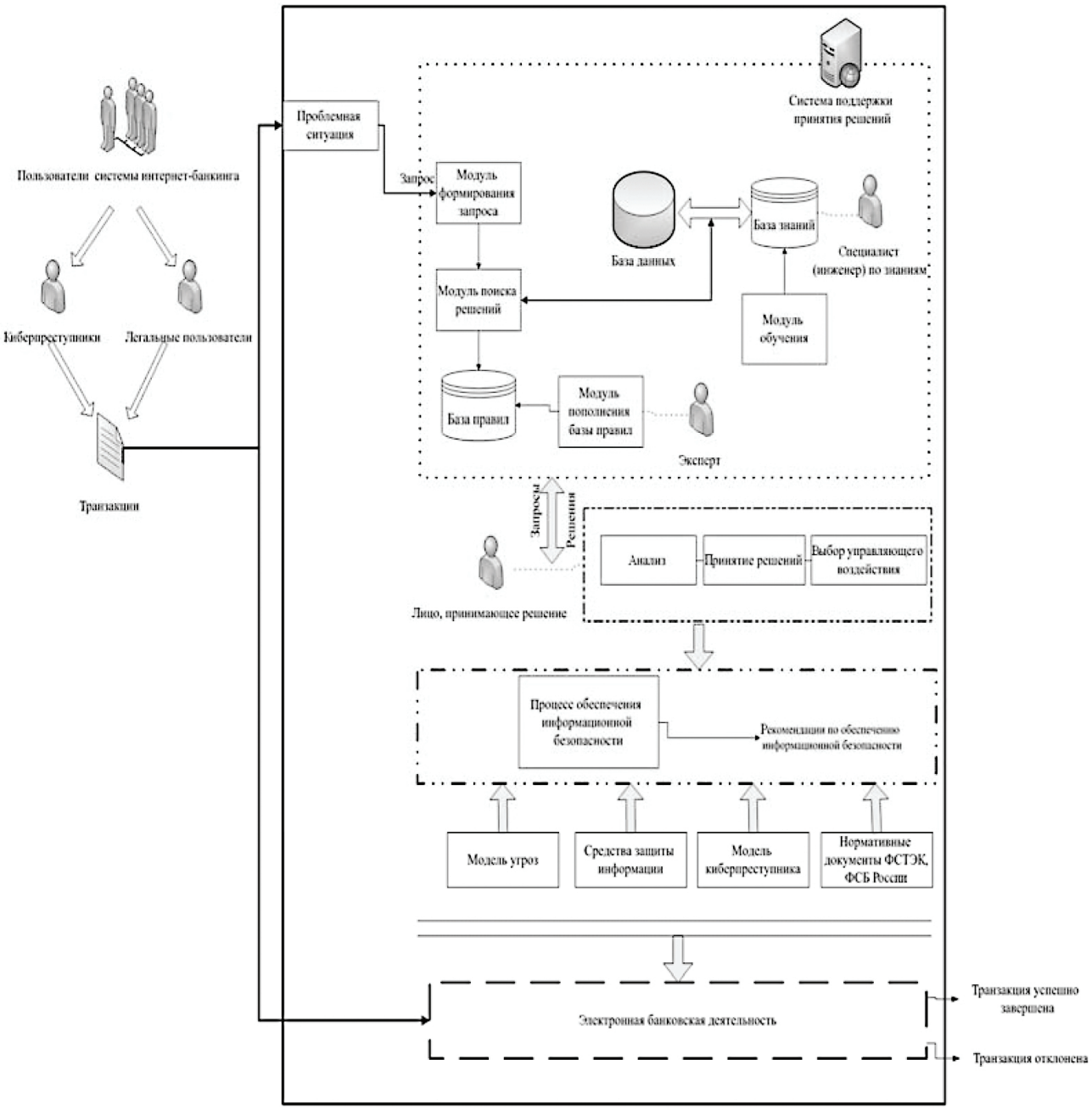

Рис. 3. Структурная схема информационной системы интернет-банкинга

$p^1 = 0$ в случае если вероятность угроз в информационной системе интернет-банкинга очень низкая;

$p^2 = \{0;1\}$;

$p^2 = 1$ в случае если вероятность угроз в информационной системе интернет-банкинга высокая;

$p^2 = 0$ в случае если вероятность угроз в информационной системе интернет-банкинга низкая;

$p^3 = \{0;1\}$;

$p^3 = 1$ в случае если вероятность угроз в информационной системе интернет-банкинга соответствует среднему значению;

$p^3 = 0$ в случае если вероятность угроз в информационной системе интернет-банкинга ниже среднего значения;

S_z – наличие средств защиты информации;

$S_z = \{s_{z_1}, s_{z_2}, s_{z_3}\}$;

где s_{z_1} – положение, когда средства защиты информации имеются в достаточном объеме;

s_{z_2} – положение, когда средства защиты информации имеются в ограниченном объеме;

s_{z_3} – положение, когда средства защиты информации отсутствуют;

Y – предполагаемый ущерб от реализации угроз в информационной системе интернет-банкинга;

M^k – модель киберпреступника, в основу которой заложены типовые образы киберпреступника, позволяющие определить потенциального нарушителя в информационной системе интернет-банкинга;

$$\xi : M^{ug} \times M^k \to Y;$$

$ND = \{nd_i \mid i = \overline{1,t}\}$ – нормативные документы ФСБ и ФСТЭК России, причем $ND = \{nd_i\}$.

Обобщенный параметр N модели M^p можно представить в виде выражения:

$$N = \left\langle M^{sp}, B^{sp}, Z, R, User^{sp} \right\rangle, \quad (4)$$

где $M^{sp} = \{M^z, M^{pr}, M^{pbp}, M^{ob}\}$ – множество модулей модели M^p;

где M^z – модуль формирования запроса;

M^{pr} – модуль поиска решений;

M^{pbp} – модуль пополнения базы правил;

M^{ob} – модуль обучения;

$B^{sp} = \{B^d, B^z, B^p\}$ – множество баз данных, правил и знаний модели M^p,

где B^d – база данных;

B^z – база знаний;

B^p – база правил;

$Z = \{z_\phi \mid \phi = \overline{1,s}\}$ – запросы;

$R = \{r_\alpha \mid \alpha = \overline{1,w}\}$ – решения;

$User^{sp} = \{user_1^{sp}, user_2^{sp}, user_3^{sp}\}$ – пользователи системы поддержки принятия решений;

где $user_1^{sp}$ – специалист (инженер) по знаниям;

$user_2^{sp}$ – эксперт;

$user_3^{sp}$ – лицо, принимающее решение;

$$\chi : Z^{user} \to M^z;$$
$$\delta : M^z \times M^{pr} \to B^p;$$
$$\varepsilon : M^{pbp} \times user_2^{sp} \to B^p;$$
$$\varphi : M^{ob} \times user_1^{sp} \to B^z;$$
$$\sigma : B^z \to B^d;$$
$$\psi : B^z \times (B^d \times M^{ob}) \to M^{pr};$$
$$user_3^{sp} = \{\eta, \tau, \sigma\};$$

где η – процесс анализа;

τ – процесс принятия решений;

σ – процесс выбора управляющего воздействия;

$$\pi : Z \times \eta \times \tau \times \sigma \to R;$$
$$\upsilon : R \to \Theta.$$

Наряду с ростом популярности использования информационных систем интернет-банкинга растет и число хищений, преследующих определенные цели. Реальностью стало мошенничество киберпреступников [6]. Как правило, мошенничество в информационных системах интернет-банкинга осуществляется по сценариям, заданным киберпреступниками. Семантическая обобщенная схема хищения конфиденциальной информации в информационных системах интернет-банкинга представлена на рис. 4.

Формализуем модель киберпреступника, которая характеризуется личностными параметрами

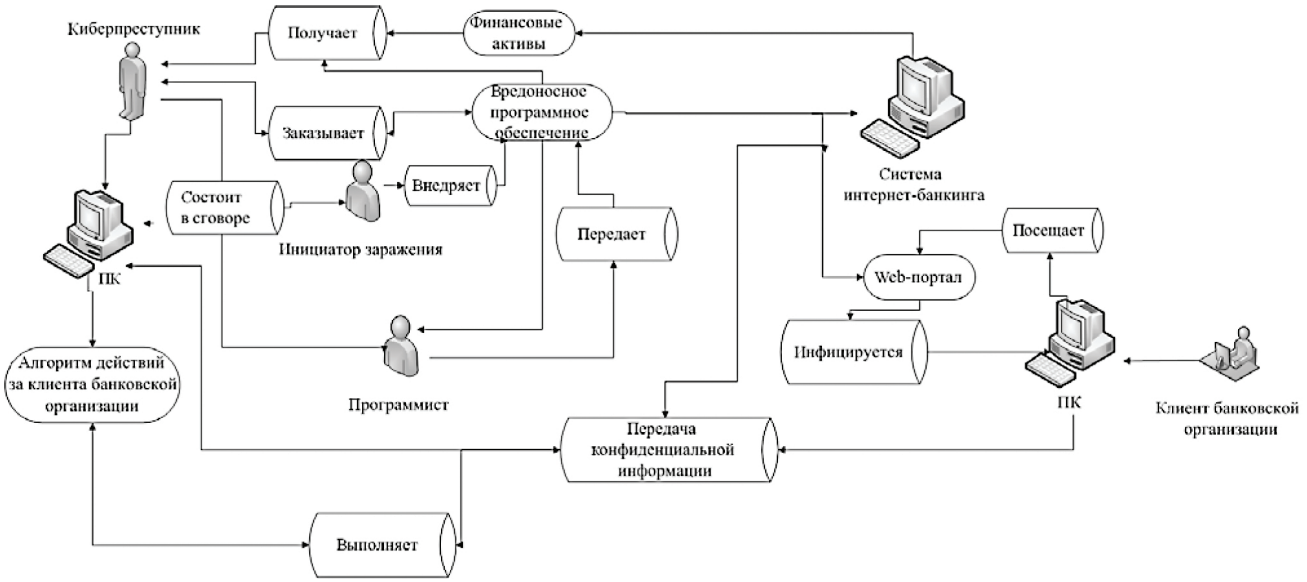

Рис. 4. Семантическая обобщенная схема хищения конфиденциальной информации в информационных системах интернет-банкинга

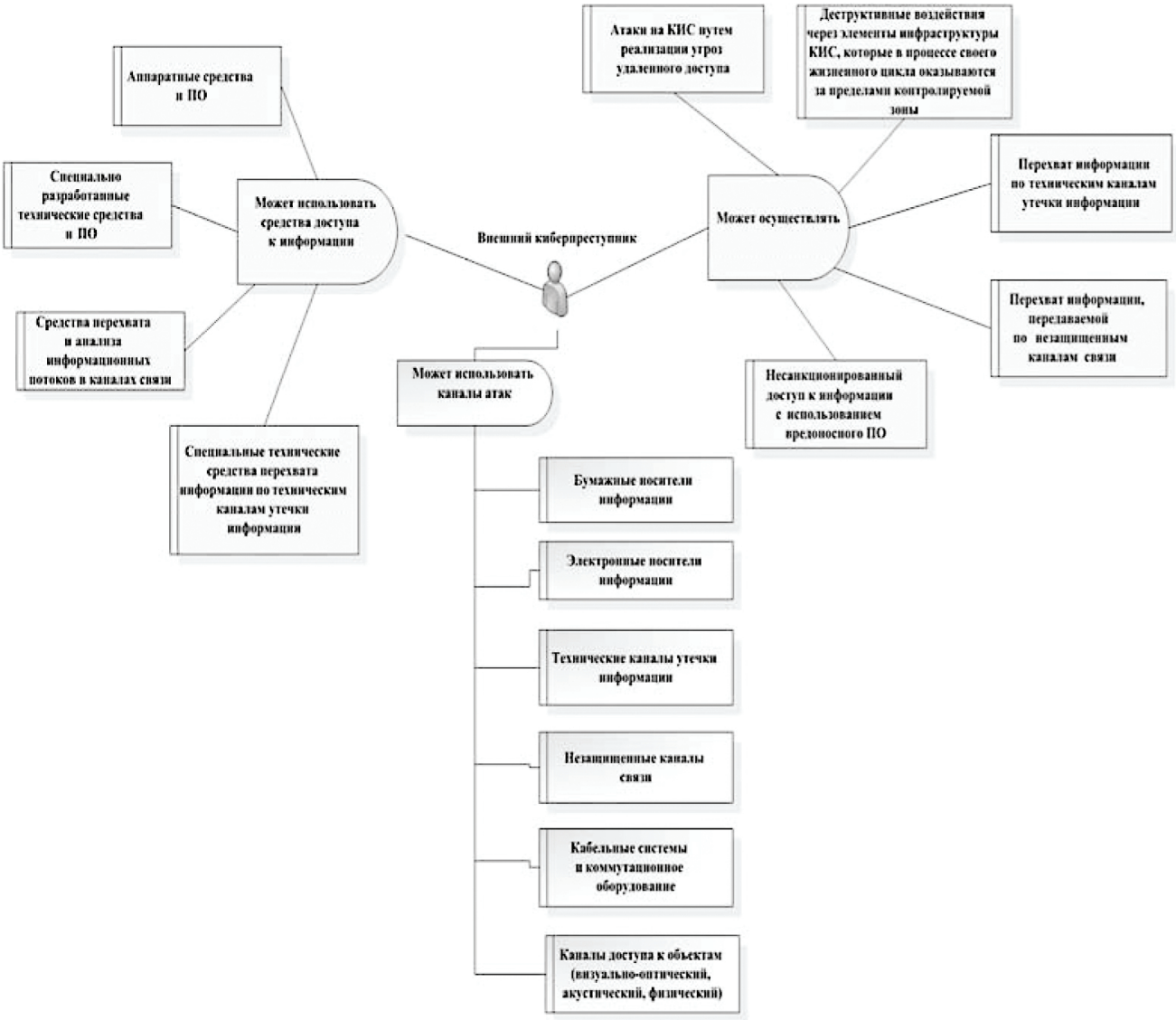

Рис. 5. Возможности внешнего киберпреступника

нарушителя и сценариями действий по хищению конфиденциальной информации в информационной системе интернет-банкинга. В основу модели киберпреступника заложены типовые образы киберпреступника, которые позволят определить потенциального нарушителя в информационной системе интернет-банкинга.

При использовании информационной системы интернет-банкинга будем рассматривать только внешнего киберпреступника, который может реализовать атаки на систему различными алгоритмами с использованием современных методов и средств получения конфиденциальной информации (рис. 5).

Модель киберпреступника можно представить в виде выражения:

$$M^k = \left\langle P^l, A^{ck}, Obr \right\rangle; \qquad (5)$$

где P^l – личностные параметры киберпреступника;
A^{ck} – сценарий действий хищения информации в информационных системах интернет-банкинга;
Obr – образ киберпреступника, причем $\iota : P^l \times A^{ck} \to Obr$.

$$P^l = \{V^k, W^k, Ch^k, Risk^k, OR^k, Rs^k\},$$

где V^k – возраст;
W^k – пол;
Ch^k – мотивация;
$Risk^k$ – риск;
OR^k – опыт работы (знания) в IT-сфере;
Rs^k – доступные ресурсы для реализации угрозы;
$A^{ck} = \{a_1^{ck}, a_2^{ck}, ..., a_f^{ck}\}$ – множество сценариев хищения информации в S^{ib};
$Obr = \{obr_1, obr_2, ..., obr_y\}$.

Предложенные три модели – системная модель информационной системы интернет-банкинга, теоретико-множественная модель поддержки принятия решений при управлении информационной безопасностью систем интернет-банкинга, модель киберпреступника – позволят совершенствовать систему защиты информации, рационально использовать современные методы и средства защиты информации. За счет этого увеличится мощность информационной безопасности информационной системы интернет-банкинга, а также возрастут эффективность и качество принятия управленческих решений по защите конфиденциальной информации.

Список литературы

1. *Безмалый В.* Защита интернет-банкинга // Windows IT Pro/RE. 2012. № 11. С. 22–25.

2. *Богданова М.И.* О роли социальной инженерии при атаках на информационную безопасность предприятия // В мире научных открытий. 2010. № 1–4. С. 145–150.

3. *Быстрова Е.Н., Сараев А.А.* Интернет-банкинг в России: тенденции и перспективы развития // Новый университет. Сер. Экономика и право. 2013. № 1. С. 44–46.

4. *Бикмаев Ш.Р.* Развитие системы интернет-банкинга как необходимое условие модернизации экономики России // Финансовая аналитика: проблемы и решения. 2013. № 23. С. 22–26.

5. *Задорожная И.В.* Интернет-банкинг как основа стратегии модернизации банковских услуг // Проблемы современной экономики. 2012. № 7. С. 208–214.

6. *Закиров М.Р.* Исследование угроз нарушения безопасности в системах дистанционного банковского обслуживания // Информационное противодействие угрозам терроризма. 2014. № 22. С. 43–47.

7. *Игнатенко Ю.П.* Моделирование оптимальной структуры системы защиты информации в распределенной корпоративной информационной системе // Информационные технологии моделирования и управления. 2007. № 9. С. 1029–1032.

8. *Керценбаум К.М.* Информационная безопасность, или просто о сложном // Право и кибербезопасность. 2012. № 1. С. 30–32.

9. *Косенков А.Н., Черный Г.А.* Общая характеристика психологии киберпреступника // Криминологический журнал Байкальского государственного университета экономики и права. 2012. № 3. С. 87–94.

10. *Мытенков С.С.* Информационная безопасность банка // Национальные интересы: приоритеты и безопасность. 2006. № 1. С. 68–75.

11. *Макаров В.В., Колотов Ю.О.* Развитие интернет-коммерции // Экономический анализ: теория и практика. 2009. № 26. С. 60–64.

12. *Петровский В.И., Тумбинская М.В., Петровский М.В.* Оптимизация комплексной системы защиты информации на предприятиях различных форм собственности: монография. Казань: Изд-во «Отечество», 2014. 636 с.

13. *Рудакова О.С., Родина Ю.В.* Анализ угроз информационной безопасности кредитных организаций // Национальные интересы: приоритеты и безопасность. 2009. № 23. С. 61–67.

14. *Сазонов С.П., Белоножкина Е.А.* Информационные технологии и интернет-банкинг как инструменты маркетинга по продвижению банковских услуг на российском рынке // Теоретические и прикладные аспекты современной науки: материалы IV Международной научной конференции, г. Белгород, 31.10.2014. Белгород: АПНИ, 2014. Т. 2. С. 178–181.

15. *Сиротский А.А.* Совершенствование методов обеспечения безопасности при авторизации в системах дистанционного банковского обслуживания // Технологии техносферной безопасности. 2013. № 6. С. 14–19.

16. *Тедеев А.А.* О проблемах и перспективах развития электронной банковской деятельности (интернет-банкинга) в России // Финансы и кредит. 2010. № 33. С. 55–58.

17. *Томилин А.Н., Крайнева И.А., Трегубов В.М., Тумбинская М.В.* Третья международная конференция «История вычислительной техники и ее программного обеспечения в России и странах бывшего СССР: история и перспективы» (SoRuCom-2014) // Вопросы истории естествознания и техники. 2015. № 1. С. 173–180.

18. *Тулупьева Т.В., Тулупьев А.Л., Азаров А.А.* Психологические аспекты оценки безопасности информации в контексте социоинженерных атак // Медико-биологические и социально-психологические проблемы безопасности в чрезвычайных ситуациях. 2013. № 1. С. 77–83.

19. *Чернявская Е.Ю.* Интернет-банкинг и интернет-эквайринг – экономические аспекты развития // Современные тенденции в экономике и управлении: новый взгляд: материалы научной конференции. Новосибирск, 28.06.2013. Новосибирск: ЦРНС, 2013. Т. 21. С. 153–157.

20. *Чирков Д.К., Саркисян А.Ж.* Преступность в сфере высоких технологий: тенденции и перспективы // Вопросы безопасности. 2013. № 2. С. 160–181.

21. *Царегородцев А.В*. Анализ рисков безопасности данных в корпоративных сетях кредитно-финансовых организаций на основе облачных вычислений // Национальные интересы: приоритеты и безопасность. 2013. № 39. С. 30–41.

22. *Царегородцев Е.И., Смышляева А.Н.* Оценка показателей рисков платежных систем, построенных на технологии интернет-банкинга // Финансы и кредит. 2010. № 1. С. 19–22.

National Interests: Priorities and Security ***Threats and Security***
ISSN 2311-875X (Online)
ISSN 2073-2872 (Print)

INFORMATION SUPPORT WHEN ENSURING THE SECURITY OF INTERNET-BANKING

Marina V. TUMBINSKAYA

Abstract

Importance Currently, most banking institutions use information systems of Internet banking or distance banking. It is simple and convenient for both banks and their customers, though not always safe.

Objectives Information security in Internet banking is relevant and vital since fraudulent and malicious activities (cyber-attacks) of cybercriminals (hackers) become more frequent. In reality, cybercrimes are committed more often than statistics indicates. Banking institutions are reluctant to disclose information about successful cyber-attacks cybercriminals performed. The article addresses issues of data protection in information systems of online banking and pursues preserving the integrity and confidentiality of information.

Methods The research shapes a generalized structure of an information system of Internet banking, which reflects modular architecture of the system, links between users and control loop. I also propose a model of the information system of Internet banking, which, if used, will allow minimizing cyber-attacks, enhancing and improving a comprehensive information security system in economic and social organizations, increasing the efficiency of the protected information system of Internet banking, choosing an adequate strategy for developing Internet banking.

Results The Internet banking system model will allow evaluating the system protection level, which is ensured by supporting the decision-making process in a poorly structured domain with heterogeneous characteristics. I propose a set-theoretical model to support decision-making in managing information security of information systems of Internet banking that allows accumulating analytical information on ongoing cybercriminals' threats, providing automated support to the process of making decisions on suppression of cyber-attacks, setting safeguards for confidential information, facilitating the elaboration of control actions. The article describes a semantic general scheme for stealing confidential information from information systems of Internet banking, presents a formalized model of a cybercriminal featuring personal parameters and scenarios for stealing confidential information from information systems of Internet banking. The cybercriminal model relies on common images and prototypes of cybercriminals, which will enable to detect a probable offender in the information system of Internet banking.

Conclusions and Relevance The proposed solutions will facilitate reinforcing information security of the information system of Internet banking, increasing the effectiveness and quality of managerial decisions on confidential information protection.

Keywords: information security, information system, Internet banking, cybercriminal, decision-making, modeling, attacks, threats

References

1. Bezmalyi V. Zashchita internet-bankinga [Protection of Internet banking]. *Windows IT Pro/RE*, 2012, no. 11, pp. 22–25.

2. Bogdanova M.I. O roli sotsial'noi inzhenerii pri atakakh na informatsionnuyu bezopasnost' predpriyatiya [On the role of social engineering in attacks against information security]. *V mire nauchnykh otkrytii = In World of Scientific Discoveries*, 2010, no. 1-4, pp. 145–150.

3. Bystrova E.N., Saraev A.A. Internet-banking v Rossii: tendentsii i perspektivy razvitiya [Internet Banking in Russia: development trends and prospects].

Novyi universitet. Seriya Ekonomika i pravo = New University. Economics and Law Series, 2013, no. 1, pp. 44–46.

4. Bikmaev Sh.R. Razvitie sistemy internet-bankinga kak neobkhodimoe uslovie modernizatsii ekonomiki Rossii [The development of Internet banking as a necessary condition for modernizing the Russian economy]. *Finansovaya analitika: problemy i resheniya = Financial Analytics: Science and Experience*, 2013, no. 23, pp. 22–26.

5. Zadorozhnaya I.V. Internet-banking kak osnova strategii modernizatsii bankovskikh uslug [Internet banking as a basis of the strategy for modernizing banking services]. *Problemy sovremennoi ekonomiki = Problems of Modern Economics*, 2012, no. 7, pp. 208–214.

6. Zakirov M.R. Issledovanie ugroz narusheniya bezopasnosti v sistemakh distantsionnogo bankovskogo obsluzhivaniya [Investigation of security threats in distance banking systems]. *Informatsionnoe protivodeistvie ugrozam terrorizma = Information Counteraction to Terrorism Threats*, 2014, no. 22, pp. 43–47.

7. Ignatenko Yu.P. Modelirovanie optimal'noi struktury sistemy zashchity informatsii v raspredelennoi korporativnoi informatsionnoi sisteme [Modeling the optimal structure of an information security system in a distributed corporate information system]. *Informatsionnye tekhnologii modelirovaniya i upravleniya = Information Technologies of Modeling and Management*, 2007, no. 9, pp. 1029–1032.

8. Kertsenbaum K.M. Informatsionnaya bezopasnost', ili prosto o slozhnom [Information security or simple words about complex things]. *Pravo i kiberbezopasnost' = Law and Cyber Security*, 2012, no. 1, pp. 30–32.

9. Kosenkov A.N., Chernyi G.A. Obshchaya kharakteristika psikhologii kiberprestupnika [General description of the cybercriminal's psychology]. *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava = Criminology Journal of Baikal National University of Economics and Law*, 2012, no. 3, pp. 87–94.

10. Mytenkov S.S. Informatsionnaya bezopasnost' banka [Bank information security]. *Natsional'nye interesy: prioritety i bezopasnost' = National Interests: Priorities and Security*, 2006, no. 1, pp. 68–75.

11. Makarov V.V., Kolotov Yu.O. Razvitie Internet-kommertsii [E-commerce development]. *Ekonomicheskii analiz: teoriya i praktika = Economic Analysis: Theory and Practice*, 2009, no. 26, pp. 60–64.

12. Petrovskii V.I., Tumbinskaya M.V., Petrovskii M.V. *Optimizatsiya kompleksnoi sistemy zashchity informatsii na predpriyatiyakh razlichnykh form sobstvennosti: monografiya* [Optimization of a comprehensive data protection system in entities with different ownership and legal structures: a monograph]. Kazan, Otechestvo Publ., 2014, 636 p.

13. Rudakova O.S., Rodina Yu.V. Analiz ugroz informatsionnoi bezopasnosti kreditnykh organizatsii [An analysis of threats to information security of credit institutions]. *Natsional'nye interesy: prioritety i bezopasnost' = National Interests: Priorities and Security*, 2009, no. 23, pp. 61–67.

14. Sazonov S.P., Belonozhkina E.A. [Information technologies and Internet banking as a marketing tool to promote banking services in the Russian market]. *Teoreticheskie i prikladnye aspekty sovremennoi nauki*: *materialy IV Mezhdunarodnoi nauchnoi konferetsii: g. Belgorod, 31 okt. 2014 g* [Proc. 4th Int. Sci. Conf. "Theoretical and Applied Aspects of Modern Science", Belgorod, October 31, 2014]. Belgorod, Agentstvo perspektivnykh nauchnykh issledovanii (APNI) Publ., 2014, vol. 2, pp. 178–181.

15. Sirotskii A.A. Sovershenstvovanie metodov obespecheniya bezopasnosti pri avtorizatsii v sistemakh distantsionnogo bankovskogo obsluzhivaniya [Improvement of methods for ensuring log-in security in distance banking services]. *Tekhnologii tekhnosfernoi bezopasnosti = Technologies for Technosphere Safety*, 2013, no. 6, pp. 14–19.

16. Tedeev A.A. O problemakh i perspektivakh razvitiya elektronnoi bankovskoi deyatel'nosti (internet-bankinga) v Rossii [On issues and prospects of developing e-banking (Internet banking) in Russia]. *Finansy i kredit = Finance and Credit*, 2010, no. 33, pp. 55–58.

17. Tomilin A.N., Kraineva I.A., Tregubov V.M., Tumbinskaya M.V. Tret'ya mezhdunarodnaya konferentsiya "Istoriya vychislitel'noi tekhniki i ee programmnogo obespecheniya v Rossii i stranakh byvshego SSSR: istoriya i perspektivy" (SoRuCom-2014) [Proc. 3rd Int. Sci. Conf. "History of computer technology and software in Russia and the former Soviet Union: History and Prospects" (SoRuCom-2014)]. *Voprosy istorii estestvoznaniya i tekhniki = Questions of History of Science and Technology,* 2015, no. 1, pp. 173–180.

18. Tulup'eva T.V., Tulup'ev A.L., Azarov A.A. Psikhologicheskie aspekty otsenki bezopasnosti informatsii v kontekste sotsioinzhenernykh atak [Psychological aspects of evaluating information security in the context of social engineering attacks]. *Mediko-biologicheskie i sotsial'no-psikhologicheskie problemy bezopasnosti v chrezvychainykh situatsiyakh = Medi-*

cal and Biological, Social and Psychological Problems of Safety in Emergency Situations, 2013, no. 1, pp. 77–83.

19. Chernyavskaya E.Yu. [Internet banking and online acquiring: economic aspects of development]. *Sovremennye tendentsii v ekonomike i upravlenii: novyi vzglyad*: *materialy nauchnoi konferentsii: Novosibirsk, 28 iyunya 2013* [Proc. Sci. Conf. "Current Trends in Economics and Management: A Fresh Approach", Novosibirsk, June 28, 2013]. Novosibirsk, Tsentr razvitiya nauchnogo sotrudnichestva Publ., 2013, vol. 21, pp. 153–157.

20. Chirkov D.K., Sarkisyan A.Zh. Prestupnost' v sfere vysokikh tekhnologii: tendentsii i perspektivy [Crime in high technologies: trends and prospects]. *Voprosy bezopasnosti = Issues of Security*, 2013, no. 2, pp. 160–181.

21. Tsaregorodtsev A.V. Analiz riskov bezopasnosti dannykh v korporativnykh setyakh kreditno-finansovykh organizatsii na osnove oblachnykh vychislenii [An analysis of data security risks in corporate networks of banking and financial institutions through cloud computing]. *Natsional'nye interesy: prioritety i bezopasnost' = National Interests: Priorities and Security*, 2013, no. 39, pp. 30–41.

22. Tsaregorodtsev E.I., Smyshlyaeva A.N. Otsenka pokazatelei riskov platezhnykh sistem, postroennykh na tekhnologii internet-bankinga [Assessment of risks associated with payment systems based on the internet banking technology]. *Finansy i kredit = Finance and Credit*, 2010, no. 1, pp. 19–22.

Marina V. TUMBINSKAYA
Kazan National Research Technical University
named after A.N. Tupolev – KAI, Kazan,
Republic of Tatarstan, Russian Federation
tumbinskaya@inbox.ru