А.М. Сычев
канд. техн. наук, доцент
E-mail: zi@bmstu.ru
Е.В. Вайц
канд. техн. наук, доцент
Р.А. Цой
аспирант
А.А. Ушакова
аспирант
(Московский государственный технический университет им. Н.Э. Баумана)
К.С. Скрыль
канд. юридических наук
(Объединение «РОИСИНКАС» Центрального банка России)
Москва, Российская Федерация

Системология и модели оценки характеристик эффективности мер обеспечения безопасности электронного банкинга

Рассматривается вероятность снижения уровня угроз безопасности электронного банкинга в качестве интегрального показателя, характеризующего возможности механизмов защиты информации сервисов дистанционного банковского обслуживания (ДБО). Обосновывается системообразующий характер данного показателя по представлению эффективности мер обеспечения безопасности электронного банкинга. Описывается процедура преобразования множества характеристик возможностей по обеспечению состояний защищенности информации в среде ДБО в систему характеристик эффективности мер обеспечения безопасности электронного банкинга. Обосновываются функциональная модель противоправных действий в отношении сервисов ДБО и функциональная модель реагирования на такого рода действия в качестве классификационных оснований для систематизации этих характеристик. Приводится вариант систематизации характеристик эффективности мер обеспечения безопасности электронного банкинга. Рассматривается система математических моделей для оценки временных и вероятностных характеристик мер обеспечения безопасности электронного банкинга.

Ключевые слова: *безопасность электронного банкинга; механизмы защиты информации сервисов дистанционного банковского обслуживания; эффективность мер обеспечения безопасности электронного банкинга; классификационные основания для систематизации характеристик мер обеспечения безопасности электронного банкинга; математические модели для оценки временных и вероятностных характеристик мер обеспечения безопасности электронного банкинга.*

A.M. Sychev
Cand. of Techn. Sciences, Associate Professor
E-mail: zi@bmstu.ru
E.V. Vayts
Cand. of Techn. Sciences, Associate Professor
R.A. Tsoy
Postgraduate Student
A.A. Ushakova
Postgraduate Student
(Bauman Moscow State Technical University)
K.S. Skryl'
Cand. of Juridical Sciences
(Association «ROISINKAS» of the Central Bank of Russia)
Moscow, Russian Federation

Systemology and Model Performance Evaluation the Effectiveness of Security Measures in Electronic Banking

The probability of reducing the level of threats to the security of electronic banking as an integral indicator characterizing the possibility of mechanisms of information protection of remote banking services (DBS) is considered. Justifies the strategic nature of this indicator for reporting the effectiveness of measures ensuring the security of electronic banking. The article describes the procedure of transformation of a set of characteristics of opportunities to ensure the state of information security in the environment of BW by the system of characteristics of the effectiveness of measures to ensure the security of electronic banking. The functional model of illegal actions in relation to the RBS services and the functional model of response to such actions as the classification grounds for the systematization of these characteristics are substantiated. The variant of systematization of characteristics of efficiency of measures of safety of electronic banking is given. The system of mathematical models for estimation of time and probabilistic characteristics of electronic banking security measures is considered.

Keywords: *safety of electronic banking; the mechanisms of information security of remote banking services; the effectiveness of security measures in e-banking; classification of grounds for the systematization of the characteristics of the measures to ensure the security of electronic banking; mathematical models to assess the temporal and probabilistic characteristics of the security measures in electronic banking.*

Сформировавшаяся к настоящему времени в теории и практике информационной безопасности терминология не дает однозначного определения понятия «эффективность мер обеспечения безопасности электронного банкинга». Это обусловлено, главным образом, отсутствием возможностей раскрытия содержания данного понятия в рамках общих требований к понятийному аппарату защиты информации, установленных отечественными и международными стандартами. Это в свою очередь не позволяет установить тот перечень показателей, который является характерным для такого рода угроз. Основной причиной этого является широта содержания термина «электронный банкинг» как категории, отражающей значительное число различным образом связанных между собой аспектов процесса накопления, обработки и передачи информации в среде дистанционного банковского обслуживания (ДБО) [1].

Исходя из посылки, что эффективность процесса обеспечения безопасности электронного банкинга может быть адекватно оценена качеством его результата [2], соответствующие меры целесообразно оценивать степенью достижения механизмами защиты информации своих целей при реализации нарушителями основных этапов противоправных действий в отношении клиентов, осуществляющих управление своими счетами через сервисы ДБО. Исходя из общеметодологической (философской) трактовки понятия «эффективность» становится очевидным, что понятие эффективности мер обеспечения безопасности электронного банкинга характеризует совокупность свойств механизмов защиты информации и меру их полезности для среды ДБО, обусловливающих способность такого рода механизмов к реализации своей целевой функции – снижению уровня угрозы безопасности электронного банкинга. Кроме того, исходя из данного определения, предполагается: во-первых, наличие двух групп функциональных характеристик – характеристик угроз безопасности электронного банкинга и характеристик механизмов реагирования на такого рода угрозы[3] и, во-вторых, метрики оценки этих характеристик.

Учитывая системность понятия «целевая функция» возникает необходимость систематизации набора оценочных характеристик степени достижения механизмами защиты информации в среде ДБО своей цели при реализации нарушителями противоправных действий в отношении сервисов ДБО. Вместе с тем приходится констатировать, что, несмотря на достигнутый к настоящему времени относительно высокий уровень теоретической и практической проработки вопросов стандартизации в области информационной безопасности, в сфере безопасности электронного банкинга выработаны лишь общие стандарты качества, обобщенно отражающие весь набор характеристик защищенности информации в среде ДБО [4]. Однако этого недостаточно, так как в указанных стандартах не отражен набор характеристик, определяющий способность механизмов защиты информации к снижению уровня угрозы безопасности электронного банкинга.

Причины этого как минимум две:

- первая – отсутствие, в общем случае, формальных методов объективного обоснования такого набора характеристик, который бы трансформировал показатели возможностей по обеспечению состояний защищенности среды ДБО в системные свойства, направленные на снижение уровня угрозы безопасности электронного банкинга;
- вторая – отсутствие требований к метрике оценки этих свойств.

Первая причина обусловлена недостатками существующего представления возможностей механизмов защиты информации в среде ДБО совокупностью несвязанных между собой показателей обеспечения защищенности данной среды как информационной. В теоретическом плане подобная ситуация обусловлена отсутствием системной классификации такого рода характеристик, а в практическом – различной степенью адекватности восприятия специалистами качества обеспечения безопасности информации в среде ДБО.

Вторая причина обусловлена главным образом качественным характером восприятия возможностей обеспечения безопасности электронного банкинга, связанным как с организационно-технической природой такого рода информационной технологии и динамичностью информационных процессов в среде ДБО, так и с широким диапазоном пользовательских требований в данной сфере [3].

Таким образом, решение проблемы оценки характеристик мер обеспечения безопасности электронного банкинга связано с обоснованием множества характеристик механизмов защиты информации в среде ДБО, отражающих меры обеспечения безопасности и разработкой соответствующих моделей для оценки этих характеристик.

В общем случае множество характеристик возможностей по обеспечению состояний защищенности информации в среде ДБО формально представляется в виде [4]:

$$D = \{\{d_{(к)}\}, \{d_{(ц)}\}, \{d_{(д)}\}\}, \quad (1)$$

где $\{d_{(к)}\}$ – подмножество характеристик, определяющих возможности по обеспечению конфиденциальности информации; $\{d_{(ц)}\}$ – подмножество характеристик, определяющих возможности по обеспечению ее целостности; $\{d_{(д)}\}$ – подмножество характеристик, определяющих возможности по обеспечению доступности информации.

Систематизация множества характеристик D возможностей по обеспечению состояний защищенности информации в среде ДБО с целью формирования множества характеристик эффективности мер обеспечения безопасности электронного банкинга предполагает упорядочение их множественного представления в соответствии с заданными основаниями:

$$R(D) \rightarrow C,$$

где R – оператор упорядочения, вносящий отношение порядка в неупорядоченный набор (1) характеристик возможностей по обеспечению состояний защищенности среды ДБО.

Системообразующим элементом множественного представления характеристик мер обеспечения безопасности электронного банкинга является характеристика «Степень снижения угрозы безопасности электронного банкинга». Будучи системной, данная характеристика определяется возможностями нарушителей по реализации противоправных действий в отношении сервисов ДБО и возможностями механизмов защиты информации в среде ДБО по реагированию на угрозы ее безопасности. По отношению к действиям нарушителей по реализации противоправных действий в среде ДБО, механизмы защиты информации в данной среде характеризуются возможностями по установлению основных этапов противоправных действий – этапа исследования нарушителями среды ДБО с целью получения информации для доступа к информационным ресурсам сервисов ДБО и этапа работы нарушителей в среде ДБО в качестве легитимных пользователей.

Это позволяет определить возможности нарушителей по реализации этапов противоправных действий как соответствующие классификационные основания для систематизации характеристик такого рода действий, а, следовательно, через возможности механизмов защиты по своевременному установлению этих этапов и реагированию на такого рода действия определить классификационные основания для систематизации характеристик этих механизмов [5].

В свою очередь, исходя из возможностей по своевременному реагированию на противоправные действия в отношении сервисов ДБО, можно получить характеристики возможностей по снижению уровня угроз безопасности этих сервисов. Эти возможности могут рассматриваться в качестве соответствующего классификационного основания.

Очевидно, что классификационным основанием для представления интегральной характеристики мер обеспечения безопасности электронного банкинга – соответствующего показателя эффективности, является степень снижения уровня угрозы безопасности электронного банкинга за счет снижения уровня угрозы безопасности сервисов ДБО.

Системный характер множества C предполагает, что процедура упорядочения множества (1) является процедурой структуризации (табл.).

Выражение, формально описывающее множественное представление системы характеристик мер обеспечения безопасности электронного банкинга, представляется в виде:

$$C = c_{1,1} \cap c_{1,2} \cap c_{2,3} \cap c_{2,4} \cap c_{2,5} \cap c_{2,6} \cap c_{2,7} \cap \cap c_{2,8} \cap c_{3,9} \cap c_{4,10} \cap c_{5,11}, \quad (2)$$

где $c_{l,n}$ – подмножество характеристик l-го ($l = 1, 2, \ldots, 5$) уровня, структурированных по основанию h, $h = 1, 2, \ldots, 11$ (см. табл.).

Таблица

Вариант иерархической структуризации характеристик мер обеспечения безопасности банкинга

№ п/п	Уровень	Классификационное основание
1	1	Проявление признаков противоправных действий в среде ДБО
2		Возможности по выявлению признаков противоправных действий в среде ДБО
3	2	Возможности по реализации этапа исследования нарушителями среды ДБО с целью получения информации для доступа к информационным ресурсам отдельного сервиса ДБО
4		Возможности по реализации этапа работы нарушителей в качестве легитимных пользователей в рамках отдельного сервиса ДБО
5		Возможности по установлению этапа исследования нарушителями среды ДБО с целью получения информации для доступа к информационным ресурсам отдельного сервиса ДБО
6		Возможности по установлению этапа работы нарушителя в качестве легитимного пользователя в рамках отдельного сервиса ДБО
7		Возможности по своевременному установлению этапа исследования нарушителями среды ДБО с целью получения информации для доступа к информационным ресурсам отдельного сервиса ДБО
8		Возможности по своевременному установлению этапа работы нарушителя в качестве легитимного пользователя в рамках отдельного сервиса ДБО
9	3	Возможности по своевременному реагированию на противоправные действия в отношении отдельных сервисов ДБО
10	4	Возможности по достижению цели обеспечения безопасности отдельных сервисов ДБО
11	5	Возможности по достижению цели обеспечения безопасности электронного банкинга

Оценка системы (2) характеристик C мер обеспечения безопасности электронного банкинга осуществляется при помощи множества $M(C)$ математических моделей:

$$M(C)=\{m_g\},\ g = 1, 2, \ldots,|M(C)|,$$

Свойство иерархичности системы характеристик мер обеспечения безопасности электронного банкинга позволяет сформировать стратегию структурного синтеза данной системы, в соответствии с которой синтез представляет собой поэтапный процесс композиции, начиная с множества характеристик времени реализации программных компонент защиты информации, обеспечивающих выявление признаков противоправных действий в отношении сервисов ДБО, и заканчивая системной характеристикой, отражающей эффективность мер обеспечения безопасности электронного банкинга – снижение вероятности угрозы за счет реализации такого рода мер.

Исходя из этого очевидно, что базис для построения синтезируемой системы возможно сформировать на основе композиционных функциональных моделей противоправных действий в отношении сервисов ДБО и мер обеспечения безопасности электронного банкинга [5].

В основе иерархии композиционного функционального описания исследуемых процессов [6] лежит набор характерных для противоправных действий в отношении сервисов ДБО признаков проявления такого рода действий в информационной среде ДБО, выявляемых при помощи соответствующих средств диагностирования, идентифицирующих воздействия нарушителя на среду ДБО в процессе реализации мер обеспечения безопасности электронного банкинга [7].

Первый уровень композиционного функционального представления исследуемых процессов формируется путем установления соответствий между признаками противоправных действий в отношении сервисов ДБО и функциональными состояниями $\phi_1^{(1)},\phi_2^{(1)},\ldots,\phi_k^{(1)},\ldots,\phi_K^{(1)}$, характерными для этих признаков. Кроме того, на данном уровне устанавливаются соответствия между этими состояниями и функциями выявления признаков противоправных действий.

При формировании второго уровня композиционного функционального представления исследуемых процессов элементы первого уровня являются подфункциями. Второй уровень композиционного функционального представления противоправных действий в отношении сервисов ДБО образуется путем установления взаимосвязей между функциональными состояниями $\phi_{11}^{(2)},\phi_{12}^{(2)},\ldots,\phi_{ij}^{(2)},\ldots,\phi_{IJ}^{(2)}$ этапов (j = 1, 2) противоправных действий в рамках конкретных сервисов (i = 1, 2, 3, 4) и функциями установления этих этапов. При этом переменная j индексирует этап противоправных действий:

- j = 1 – этап исследования нарушителями среды ДБО с целью получения информации для доступа к информационным ресурсам сервиса ДБО;
- j = 2 – этап работы нарушителей в качестве легитимных пользователей в рамках сервиса ДБО,

а переменная i индексирует сервис:

- i = 1 – сервис платежных систем;
- i = 2 – сервис «Клиент-Банк»;
- i = 3 – сервис «Мобильный банк»;
- i = 4 – сервис предоставления услуг через среду ДБО.

Аналогично образуется третий уровень композиционного функционального представления исследуемых процессов, где в качестве функциональных состояний выступают сервисы ДБО, подверженные угрозам безопасности.

На четвертом уровне композиционного функционального представления исследуемых процессов формируются функциональные состояния, соответствующие целевым функциям эффективности мер обеспечения безопасности сервисов ДБО.

Процедура функциональной композиции завершается формированием функционального состояния, соответствующего целевой функции эффективности мер обеспечения безопасности электронного банкинга.

Результаты проведенной систематизации характеристик мер обеспечения безопасности электронного банкинга, с учетом изложенных методических положений, наглядно представлены на рисунке 1.

Система математических моделей для оценки характеристик мер обеспечения безопасности электронного банкинга имеет структуру, идентичную структуре оцениваемых характеристик (рис. 2).

В основу процедуры формирования математических моделей временных характеристик возможностей нарушителей по реализации противоправных действий в отношении сервисов ДБО и временных характеристик возможностей по установлению сервисов, подвергшихся угрозам безопасности, положена математическая интерпретация функционального представления моделируемых процессов.

Исходя из свойства линейности и аддитивности математического ожидания $\overline{\tau}_s^{(2)}$, s = 1, 2, …, S, композиции случайных величин $\tau_1^{(1)},\tau_2^{(1)},\ldots,\tau_n^{(1)},\ldots,\tau_N^{(1)}$, характеризующих время реализации функций $\Phi_1^{(1)},\Phi_2^{(1)},\ldots,\Phi_n^{(1)},\ldots,\Phi_N^{(1)}$, аналитические модели $\overline{\tau}_s^{(2)}$ формируются на основе обобщенного выражения [8]:

$$\overline{\tau}_s^{(2)} = M\left(\tau_1^{(1)} * \tau_2^{(1)} * \ldots * \tau_N^{(1)}\right) = \sum_{n=1}^{N} \overline{\tau}_n^{(1)},$$

где $\overline{\tau}_n^{(1)}$ – среднее значение случайной величины $\tau_n^{(1)}$; $M(\cdot)$ – математическое ожидание от композиции случайных величин; * – знак композиции случайных величин.

Что касается математического представления вероятностей своевременной реализации функций

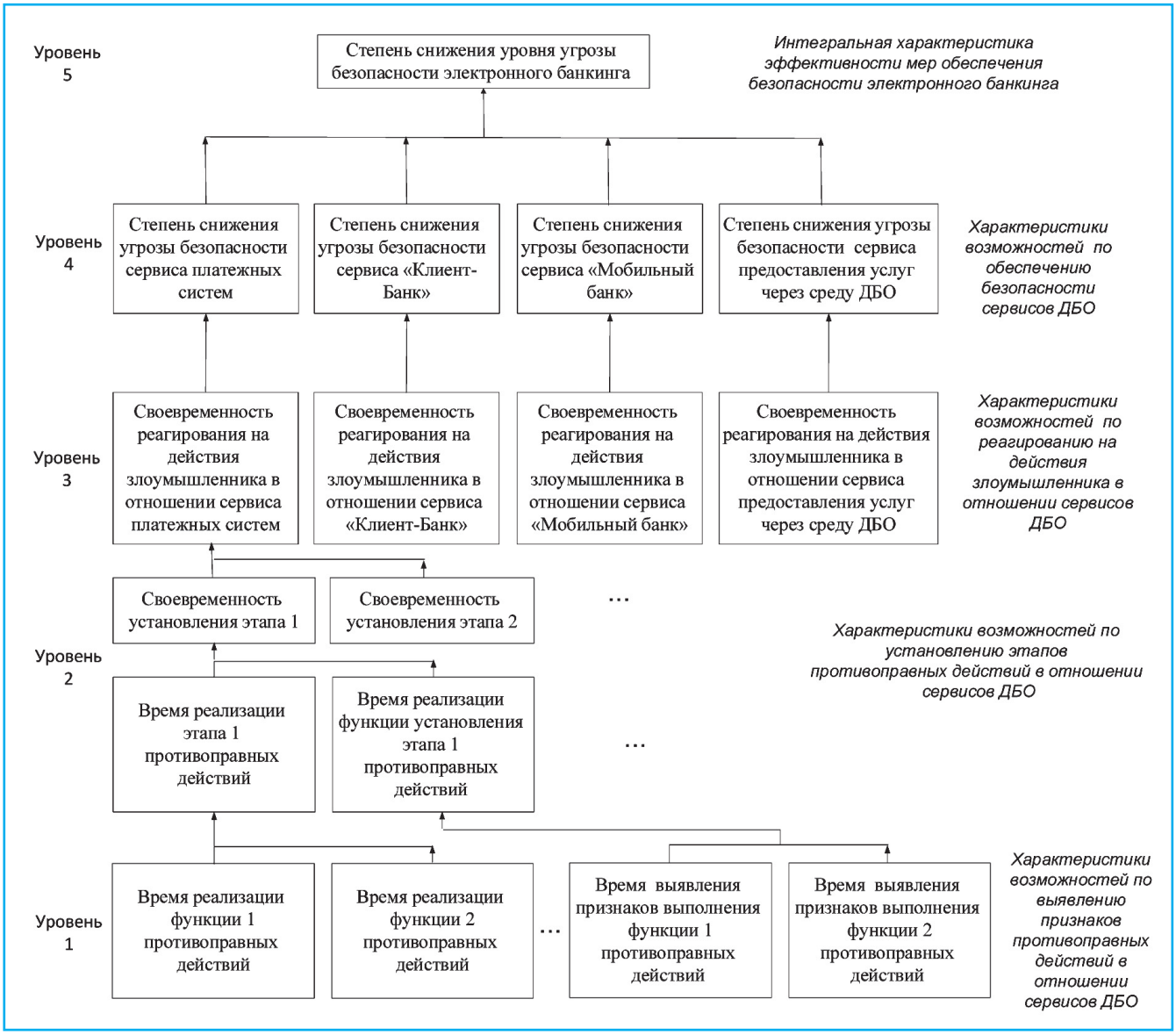

Рис. 1. Система характеристик мер обеспечения безопасности электронного банкинга

установления этапов противоправных действий в отношении сервисов ДБО, то при его обосновании определено соответствующее условие [9]:

$$\tau_{(\text{уст})ij} \le \overline{\tau}_{(\text{э})ij} - \overline{\tau}_{(\text{р})ij}, \tag{3}$$

где $\tau_{(\text{уст})ij}$ – время установления j-го (j = 1, 2) этапа противоправных действий в отношении i-го (i = 1, 2, 3, 4) сервиса ДБО; $\overline{\tau}_{(\text{р})ij}$ – математическое ожидание времени реагирования на противоправные действия в отношении i-го сервиса ДБО при реализации нарушителем j-го этапа; $\overline{\tau}_{(\text{э})ij}$ – математическое ожидание времени реализации нарушителем j-го этапа противоправных действий в отношении i-го сервиса ДБО.

Аналитическая модель своевременности реализации функций установления этапов противоправных действий в отношении сервисов ДБО, представляет собой вероятность выполнения условия (3) [9]:

$$P\left(\tau_{(\text{уст})} \le \overline{\tau}_{(\text{э})} - \overline{\tau}_{(\text{р})}\right) \approx \frac{1}{z_1} \cdot \left[\frac{\overline{\tau}_{(\text{э})} - \overline{\tau}_{(\text{р})}}{4 \cdot z_1 \cdot \sigma} \cdot \left[1 + \text{erf}\left(\frac{\overline{\tau}_{(\text{уст})}}{\sigma\sqrt{2}} \right) \right] + \frac{1}{4 \cdot z_2} \exp\left(\frac{\overline{\tau}^2_{(\text{уст})}}{2\sigma^2} \right) - \frac{1}{8} \cdot \left| 1 + \text{erf}\left(\frac{\overline{\tau}^2_{(\text{уст})}}{2\sigma^2} \right) \right| \right], \tag{4}$$

где s – среднеквадратическое отклонение случайной величины $\tau_{(\text{уст})}$; erf(*) – функция ошибок.

Приведенные в условии (7) нормировочные коэффициенты z_1, z_2 для усеченного нормального распределения определяются в соответствии с выражениями:

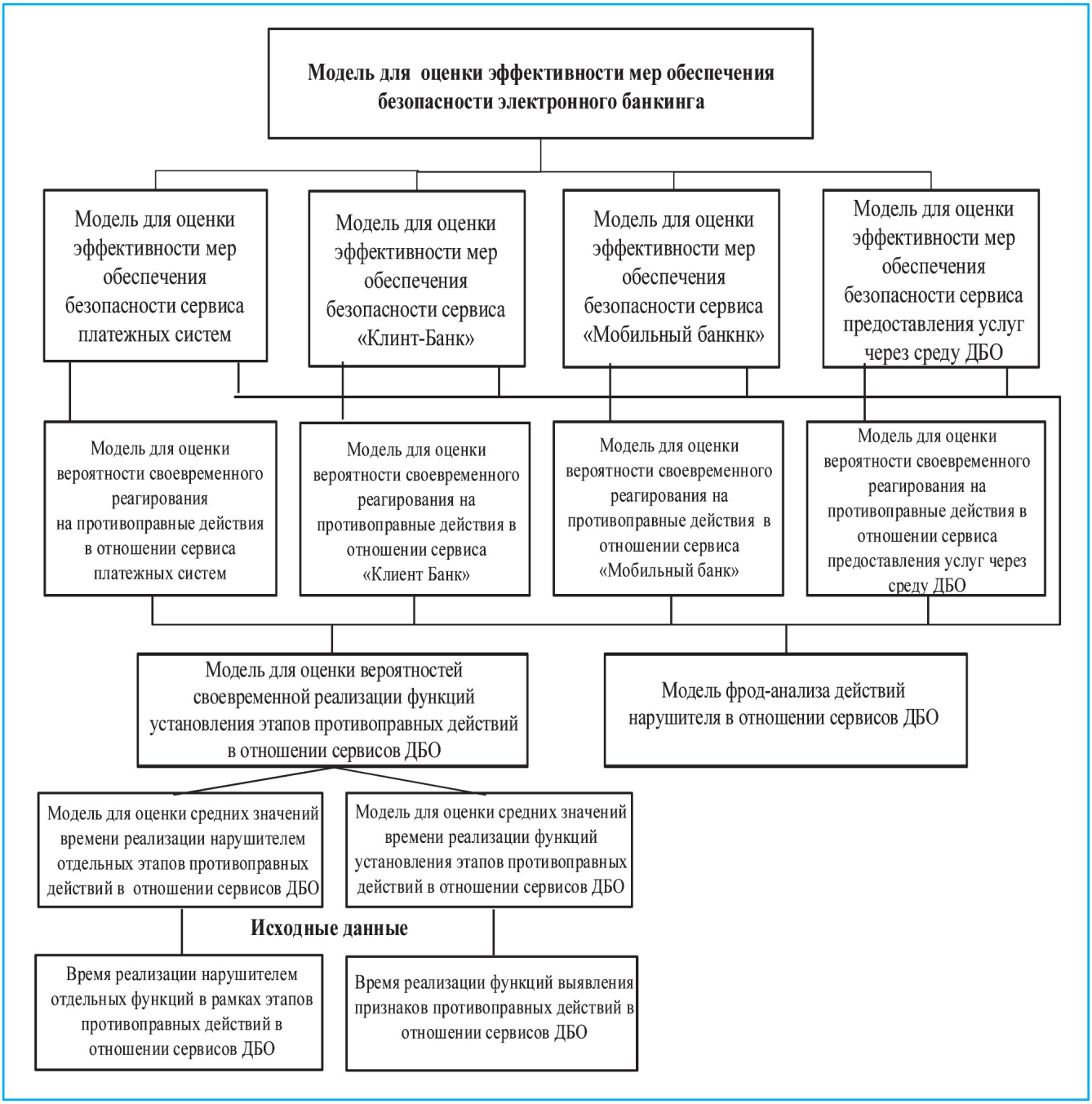

Рис. 2. Система математических моделей оценки характеристик мер обеспечения безопасности электронного банкинга

$$z_1 = \frac{1}{2}\cdot\left[1-\mathrm{erf}\left(\frac{\overline{\tau}_{(\text{уст})}+\overline{\tau}_{(\text{э})}-\overline{\tau}_{(\text{р})}}{\sigma\cdot\sqrt{2}}\right)\right],$$

$$z_2 = \frac{1}{2}\cdot\left[1+\mathrm{erf}\left(\frac{\overline{\tau}_{(\text{уст})}}{\sigma\cdot\sqrt{2}}\right)\right].$$

Характеристики третьего уровня системы характеристик мер обеспечения безопасности электронного банкинга оцениваются множеством моделей для оценки вероятностей $P_i^{(3)}$ своевременного реагирования на угрозы, вызванные противоправными действиями в отношении сервисов ДБО:

$$P_1^{(3)} = 1-\left(1-P_{11}^{(2)}\cdot P_{21}^{(2)}\right)\cdot\left(1-P_{11}^{(2)}\cdot P_{25}^{(2)}\right), \quad (5)$$

$$P_2^{(3)} = P_{12}^{(2)}\cdot P_{22}^{(2)}, \quad (6)$$

$$P_3^{(3)} = P_{13}^{(2)}\cdot P_{23}^{(2)}, \quad (7)$$

$$P_4^{(3)} = P_{14}^{(2)}\cdot P_{24}^{(2)}. \quad (8)$$

Приведенные выше модели позволяют определить показатели E_i (i = 1, 2, 3, 4) эффективности мер обеспечения безопасности каждого из четырех типов сервисов ДБО как характеристики полезности такого рода мер для соответствующих технологий электронного банкинга.

С этой целью введем ряд ограничений на используемый вариант интерпретации модели противоправных действий в сфере электронного банкинга:

1) подобного рода противоправные действия являются способом реализации угроз безопасности электронного банкинга;

2) источником угроз является злоумышленник;

3) для такого рода источника характерно однократное (за исследуемый период) воздействие на среду ДБО;

4) однократное воздействие на среду ДБО осуществляется также из соображений скрытности;

5) нарушение безопасности электронного банкинга связано с проведением соответствующих противоправных действий, связанных со следующими операциями:

- получением конфиденциальной информации клиентов банка;
- модификацией, либо уничтожением этой информации;
- блокированием информационного обеспечения среды ДБО при определенных обстоятельствах.

При этом целевую мотивацию имеют противоправные действия по модификации, либо уничтожению информации клиентов банка.

Воспользовавшись данным вариантом интерпретации модели противоправных действий в сфере электронного банкинга в качестве предпосылки для формального представления такого рода действий в виде потока угроз нарушения безопасности информации в отношении i-го (i = 1, 2, 3, 4) сервиса ДБО на временном интервале $[t_1, t_2]$ исследования, определим такого рода угрозы как поток событий, характеризующийся стационарностью, ординарностью и отсутствием последействия [10].

С целью проверки наличия свойства стационарности у рассматриваемого потока событий определим:

- длину Δt временного интервала $[t_1, t_2]$ от момента начала t_1 до момента окончания t_2 исследования угроз безопасности электронного банкинга, $\Delta t = t_2 - t_1$;
- вероятность $P_{(y)i}$ проявления такого рода угрозы;
- период $T_{(y)i}$ проявления угроз безопасности i-го сервиса как длину временного интервала между двумя последовательными проявлениями такого рода угроз.

Предположение о стационарности потока угроз безопасности i-го сервиса ДБО базируется на выполнении двух основных условий:

1) его однородность во времени: вероятность $P_{(y)i}$ зависит только от длины временного интервала Δt и не зависит от его положения на временной оси, то есть для величины $P_{(y)i}$ будет справедливым условие $P_{(y)i1} > P_{(y)i2}$, если $\Delta t_1 > \Delta t_2$;

2) моменты проявления угроз имеют одинаковую среднюю плотность λ_i, которая не изменяется от времени, а зависит лишь от периода проявления $T_{(y)i}$:

$$\lambda_i = 1/ T_{(y)i}.$$

Наличие свойства ординарности потока угроз безопасности i-го сервиса ДБО обусловлено однократностью противоправных действий нарушителя.

Доказательство свойства отсутствия последействия в потоке угроз безопасности i-го сервиса ДБО основывается на том, что угрозы появляются в последовательные моменты времени, при этом распределяясь на интервале $[t_1, t_2]$ независимо друг от друга.

Характерные для проявления свойств стационарности, ординарности и отсутствия последействия условия реализации угроз безопасности сервисов ДБО позволяют определить вероятность возникновения хотя бы одной угрозы безопасности для каждого из четырех типов сервисов ДБО с учетом мер реагирования на угрозы их безопасности $P_{(ум)i}$ и при условии отсутствия такого рода мер $P_{(y)i}$:

$$P_{(ум)i} = 1 - e^{-\lambda_{(м)i} \cdot (t_2 - t_1)},$$

$$P_{(y)i} = 1 - e^{-\lambda_i \cdot (t_2 - t_1)},$$

где $\lambda_{(м)i}$ и λ_i – интенсивность проявления угроз безопасности i-го сервиса ДБО с учетом мер реагирования на угрозы его безопасности и при условии отсутствия такого рода мер, соответственно.

При этом λ_i определяется при помощи моделей фрод-анализа [11], а для определения $\lambda_{(м)i}$ используется выражение

$$\lambda_{(м)i} = \lambda_i \cdot (1 - P_i^{(3)}),$$

в котором $P_i^{(3)}$ соответствует (5)…(8).

Это позволяет в качестве характеристики E_i эффективности мер обеспечения безопасности i-го сервиса ДБО на протяжении временного интервала $[t_1, t_2]$ исследования использовать выражение:

$$E_i = P_{(y)i} - P_{(ум)i},$$

характеризующее степень снижения угрозы безопасности n-го сервиса ДБО за счет своевременного реагирования на такого рода угрозы.

Воспользовавшись свойством аддитивности параметра интенсивности потока угроз безопасности электронного банкинга, определим вероятности такого рода угроз с учетом мер реагирования на них $P_{(ум)}$ и при условии отсутствия мер реагирования $P_{(y)}$:

$$P_{(ум)} = 1 - e^{-\lambda_{(м)} \cdot (t_2 - t_1)},$$

$$P_{(y)} = 1 - e^{-\lambda \cdot (t_2 - t_1)},$$

где $\lambda_{(м)}$ – интенсивность проявления угроз безопасности для всех четырех сервисов ДБО с учетом мер реагирования на такого рода угрозы на протяжении временного интервала $[t_1, t_2]$:

$$\lambda_{(м)} = \lambda_{(м)1} + \lambda_{(м)2} + \lambda_{(м)3} + \lambda_{(м)4},$$

λ – интенсивность проявления угроз безопасности для всех четырех сервисов ДБО при условии отсутствия мер реагирования на такого рода угрозы на протяжении временного интервала $[t_1, t_2]$:

$$\lambda = \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4.$$

Это позволяет в качестве показателя Э эффективности мер обеспечения безопасности электронного банкинга на протяжении временного интервала $[t_1, t_2]$ исследования использовать выражение:

$$Э = P_{(y)} - P_{(ум)}.$$

Разработанный аппарат системологической оценки характеристик эффективности мер обеспечения безопасности электронного банкинга может быть использован в качестве инструмента адекватной оценки возможностей механизмов обеспечения защищенности информационной среды ДБО и, как следствие, в качестве инструмента формирования обоснованных решений относительно направлений совершенствования защиты информации сервисов ДБО.

Список литературы

1. Лямин Л.В., Пухов А.В. *Дистанционное банковское обслуживание*. М.: КноРус: ЦИПСиР, 2010. 328 с.
2. Скрыль С.В., Шелупанов А.А. *Основы системного анализа в защите информации*: учебное пособие для студентов высших учебных заведений. М.: Машиностроение, 2008. 138 с.
3. Сычев А.М., Ревенков П.В., Дудка А.Б. *Безопасность электронного банкинга*: монография. М.: Интеллектуальная литература, 2017. 318 с.
4. Вихорев С.В., Сычев А.М. *Диалоги о безопасности информации, или введение в основы построения систем обеспечения безопасности информации*: монография. М.: Медиа Группа «Авангард», 2015. 640 с.
5. Сычев А.М., Афонин И.А., Скрыль К.С., Баркалов Ю.М. Классификационные основания для синтеза системы характеристик эффективности мер реагирования на угрозы безопасности электронного банкинга // *Промышленные АСУ и контроллеры*. М.: «Научтехлитиздат». 2017, № 7. С. 44–52.
6. Скрыль С.В., Сычев А.М., Астрахов А.В., Ушакова А.А., Борукаева А.О. Функциональное моделирование в приложениях практики анализа противоправных действий в отношении сервиса «Клиент-Банк» // *Промышленные АСУ и контроллеры*. М.: «Научтехлитиздат». 2018, № 12. С. 50–63.
7. Скрыль С.В., Тямкин А.В., Литвинов Д.В. *Исследование механизмов противодействия компьютерным преступлениям: организационно-правовые и криминалистические аспекты*: монография. Воронеж: Воронежский институт МВД России, 2009. 218 с.
8. Корн Г., Корн Т. *Справочник по математике* (для научных работников и инженеров). М.: Наука, 1974. 832 с.
9. Скрыль С.В., Сычев А.М., Мещерякова Т.В., Голубков Д.А., Арутюнова В.И. Оценка защищенности информации от вирусных атак: существующий и перспективный методический аппарат // *Промышленные АСУ и контроллеры*. 2018, № 9. С. 54–61.
10. Вентцель Е.С. *Исследование операций: задачи, принципы, методология*. 2-е изд., стер. М.: Наука. 1988. 208 с.
11. Сычев А.М., Скрыль К.С., Вайц Е.В., Шатилов П.А., Борукаева А.О. Модели антифрода в практике обеспечения безопасности электронного банкинга // *Промышленные АСУ и контроллеры*. М: «Научтехлитиздат». 2019, № 1. С. 47–53.

References

1. Lyamin L.V., Pukhov A.V. *Distantsionnoe bankovskoe obsluzhivanie* [Remote banking service]. M.: KnoRus: TsIPSiR [Moscow: KnoRus: Center for Research of Payment Systems and Settlements]. 2010. 328 p.
2. Skryl' S.V., Shelupanov A.A. *Osnovy sistemnogo analiza v zashchite informatsii*: uchebnoe posobie dlya studentov vysshikh uchebnykh zavedeniy [Fundamentals of system analysis in information protection: a textbook for students of higher educational institutions]. M.: Mashinostroenie [Moscow: Publishing house «Engineering»]. 2008. 138 p.
3. Sychev A.M., Revenkov P.V., Dudka A.B. *Bezopasnost elektronnogo bankinga*: monografiya [Security of e-banking: monograph]. M.: Intellektualnaya literature [Moscow: Publishing house «Intellectual literature»]. 2017. 318 p.
4. Vikhorev S.V., Sychev A.M. *Dialogi o bezopasnosti informatsii, ili vvedenie v osnovy postroeniya sistem obespecheniya bezopasnosti informatsii*: monografiya [Dialogues on information security, or an introduction to the basics of building information security systems: monograph]. M: Media Gruppa «Avangard» [Moscow: Media Group «Avangard»]. 2015. 640 p.
5. Sychev A.M., Afonin I.A., Skryl' K.S., Barkalov Yu.M. Klassifikatsionnye osnovaniya dlya sinteza sistemy kharakteristik effektivnosti mer reagirovaniya na ugrozy bezopasnosti elektronnogo bankinga [Classification Bases for Synthesis of System of Characteristics of Efficiency of Measures of Response to Threats of Safety of Electronic Banking]. *Promyshlennye ASU i kontrollery* [Industrial Automatic Control Systems and Controllers]. M.: «Nauchtekhlitizdat». 2017, no. 7, pp. 44–52.

6. Skryl' S.V., Sychev A.M., Astrakhov A.V., Ushakova A.A., Borukaeva A.O. Funktsionalnoe modelirovanie v prilozheniyakh praktiki analiza protivopravnykh deystviy v otnoshenii servisa «Klient-Bank» [Functional Modeling in the Applications of the Practice of Analysis of Anti-rights Actions with Respect to the Customer Service]. *Promyshlennye ASU i kontrollery* [Industrial Automatic Control Systems and Controllers]. M: «Nauchtekhlitizdat». 2018, no. 12, pp. 50–63.
7. Skryl' S.V., Tyamkin A.V., Litvinov D.V. *Issledovanie mekhanizmov protivodeystviya kompyuternym prestupleniyam: organizatsionno-pravovye i kriminalisticheskie aspekty*: monografiya [Research of mechanisms of counteraction to computer crimes organizational-legal and criminalistic aspects: monograph]. Voronezh: Voronezhskiy institut MVD Rossii [Voronezh: Voronezh Institute of the Russian interior Ministry]. 2009. 218 p.
8. Korn G., Korn T. *Spravochnik po matematike* (dlya nauchnykh rabotnikov i inzhenerov) [Handbook of mathematics for researchers and engineers]. M: Nauka [Moscow: Publishing house «Science»]. 1974. 832 p.
9. Skryl' S.V., Sychev A.M., Meshcheryakova T.V., Golubkov D.A., Arutyunova V.I. Otsenka zashchishchennosti informatsii ot virusnykh atak: sushchestvuyushchiy i perspektivnyy metodicheskiy apparat [Evaluation of Information Security from Virus Attacks: Existing and Promising Methodological Apparatus]. *Promyshlennye ASU i kontrollery* [Industrial Automatic Control Systems and Controllers]. 2018, no. 9, pp. 54–61.
10. Venttsel Ye.S. *Issledovanie operatsiy: zadachi, printsipy, metodologiya*. 2-e izd., ster. [Operations research: tasks, principles, methodology. 2nd ed.]. M.: Nauka [Moscow: Publishing house «Science»]. 1988. 208 p.
11. Sychev A.M., Skryl' K.S., Vayts Ye.V., Shatilov P.A., Borukaeva A.O. Modeli antifroda v praktike obespecheniya bezopasnosti elektronnogo bankinga [Anti-fraud Model in the Practice of the Security Electronic Banking]. *Promyshlennye ASU i kontrollery* [Industrial Automatic Control Systems and Controllers]. M.: «Nauchtekhlitizdat». 2019, no. 1, pp. 47–53.

Информация об авторах

Сычев Артем Михайлович, кандидат технических наук, доцент кафедры ИУ-10
E-mail: zi@bmstu.ru
Вайц Екатерина Викторовна, кандидат технических наук, доцент кафедры ИУ-10
Цой Роман Александрович, аспирант кафедры защиты информации (ИУ-10)
Ушакова Анна Андреевна, аспирант кафедры защиты информации (ИУ-10)
Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный технический университет им. Н.Э. Баумана»
105005, Российская Федерация, Москва, ул. 2-я Бауманская, 5
Скрыль Кирилл Сергеевич, кандидат юридических наук, главный специалист Управления информационной безопасности
Российское объединение инкассации (РОСИНКАС) Центрального банка Российской Федерации (Банка России)
127051, Российская Федерация, Москва, Цветной бульвар, д. 7, стр. 3

Information about the authors

Sychev Artem Mikhaylovich, Candidate of Technical Sciences, Associate Professor
E-mail: zi@bmstu.ru
Vayts Ekaterina Viktorovna, Candidate of Technical Sciences, Associate Professor
Tsoy Roman Aleksandrovich, Postgraduate Student of the Department of Information Security
Ushakova Anna Andreevna, Postgraduate Student of the Department of Information Security
Federal State Educational Institution of Higher Education «Bauman Moscow State Technical University»
105005, Russian Federation, Moscow, str. 2nd Bauman, 5
Skryl' Kirill Sergeevich, Candidate of Juridical Sciences, Chief Specialist of the Information Security Administration Russian Association of Collection (ROSINKAS) of the Central Bank of the Russian Federation (Bank of Russia)
127051, Russian Federation, Moscow, Tsvetnoy Bulvar, 7, bld. 3