

УДК 336.717.1:519.866

А.А. Стрижак

## Системный анализ и исследование структуры и источников рисков в платежных системах

С позиций системного анализа рассмотрены платежные системы, функционирующие на базе платежных карт: их структура, составные элементы и функциональное назначение. Классифицированы и структурированы риски, которым подвержены участники платежной системы. Формализованы риски каждого структурного элемента платежной системы с учетом методологии «источник-сценарий-последствия».

From the standpoint of a system analysis the payment system, operating on the basis of payment cards, are considered: their structure, the constituent elements and functionality. The risks of the participants of the payment system are classified and structured. The risks of each structural element of the payment system are formalized with the account of the «source-script-consequences» methodology.

З позицій системного аналізу розглянуто платіжні системи, що функціонують на базі платіжних карт: їх структура, складові елементи та функціональне призначення. Класифіковано й структуровано ризики, на які наражаються учасники платіжної системи. Формалізовано ризики кожного структурного елемента платіжної системи з урахуванням методології «джерело-шлях-наслідки».

**Введение.** Современные мировые тенденции экономического развития характеризуются активным использованием и распространением платежных систем (ПС), функционирующих на базе платежных карт (ПК). ПС объединяют большое количество финансовых учреждений, банков, торгово-сервисных организаций, держателей ПК по всему миру, обеспечивая важную функцию жизнедеятельности общества – быстрое и надежное осуществление платежей между разными участниками. Кроме того, ПС обеспечивают ряд дополнительных функций и сервисов: поддержка систем лояльности (скидки, бонусы), систем медицинского страхования, учет предоставления льгот различным категориям населения и так далее, количество которых растет с возникновением новых потребностей общества и появлением новых технических средств, устройств и инженерно-технических решений.

Соответственно ПС – не застывшая структура с зафиксированными элементами и неизменными правилами функционирования. Она постоянно развивается и изменяется: увеличивается количество ее участников – банков, клиентов, появляются новые технологии хранения, передачи и контроля данных, вводится в эксплуатацию новое оборудование, возникают

новые функции и методы обслуживания клиентов, происходят процессы интеграции ПС разных стран [1, 2]. Это неизменно приводит к усложнению взаимосвязей между участниками ПС, росту количества и сложности операций, увеличению влияния внешней среды, появлению новых подсистем и моделей взаимодействия. Следовательно возникают разнотипные источники опасности и риски (финансовые, технологические, операционные, системные, риск мошенничества с ПК), цена которых достаточно высокая.

Такие особенности ее работы ставят новые для Украины актуальные задачи исследования ПС, обеспечения безопасности ее функционирования и эффективного развития, выявления критических моментов в ее работе, рисков и методов управления ими. Исследование и анализ этих проблем – важная научно-прикладная задача, требующая основательного и системного изучения для обеспечения качества обслуживания клиентов ПС.

### Формализация взаимодействия структурных элементов ПС

Для анализа источников рисков в ПС, их классификации, определения эффективных методов управления ими, выявления критических моментов в работе системы необходимо ис-

следование ПС и ее составных элементов с позиций системного анализа, построения схем и моделей функционирования ПС в целом и каждого элемента в частности.

Современная ПС, построенная на базе ПК, представляет собой сложную иерархическую территориально-распределенную информационно-аналитическую систему, обеспечивающую выполнение финансовых операций (транзакций) с помощью ПК [1, 3–4]. Основное назначение ПС – обеспечение выполнения в безналичной форме расчетов между поставщиком услуги/товара (продавцом) и потребителем услуги/товара (покупателем), который предоставил к оплате ПК, и обеспечение получения наличных средств держателем ПК в специальных устройствах – банкоматах и в операционных кассах, оказывающих такие услуги.

ПС состоит из большого количества разнотипных участников: финансовых учреждений (банков и компаний, которые обслуживаются этими банками); процессинговых центров, платежной организации, держателей ПК.

**Платежная организация** (ПО) является центральным административным органом, обеспечивающим организацию работы и общее руководство ПС как в плане текущей деятельности, так и развития системы [1]. Обозначим  $O_0$  – ПО ПС.

**Банки-участники ПС** осуществляют обслуживание клиентов – держателей ПК (*эмитенты*) и предоставляют услуги перевода денежных средств торгово-сервисным предприятиям за предоставленные последними товары и услуги, оплаченные с помощью ПК (*экваеры*), а также отвечают за проводку межбанковских расчетов в ПС [1, 3, 5]. Обозначим  $B = \{b_i, i = 1, 2, \dots, i_B\}$  – множество банков-участников ПС;  $b_i$  –  $i$ -й банк-участник ПС; банки-эмитенты  $b_i^I \in B$ , банки-экваеры  $b_i^A \in B$ , банки-эмитенты-экваеры  $b_i^S \in B$ .

**Процессинговый центр** (ПЦ) – компания, выполняющая по доверенности банков различные операции обработки транзакционных данных (маршрутизацию, авторизацию [1, 5]) и их

хранение. Обозначим  $C = \{c_k, k = 1, 2, \dots, k_C\}$  – множество ПЦ ПС;  $c_k$  –  $k$ -й ПЦ.

**Расчетно-клиринговый центр** (РКЦ) – учреждение, которое обрабатывает (клирингует) предоставленные ПЦ данные о выполненных в ПС транзакциях и направляет их после этого соответствующим эмитентам и экваерам для окончательных расчетов по ним [1]. Как правило, каждый ПЦ  $c_k$  имеет в своей структуре подразделение, выполняющее функции РКЦ.

**Расчетный банк** (РБ) – банк, уполномоченный ПО соответствующей ПС, который открывает корреспондентские счета банкам-участникам ПС и выполняет взаиморасчеты между ними в соответствии с условиями, указанными в договорах. Обозначим  $B_0 = \{b_0\}$  – РБ ПС.

**Торгово-сервисные предприятия** (ТСП) – это предприятия торговли или услуг, которые в соответствии с подписанным соглашением с обслуживающим банком берут на себя обязательство принимать ПК данной ПС в качестве средств расчета за предложенные ими товары/услуги [1]. Обозначим  $V = \{v_m, m = 1, 2, \dots, m_V\}$  – множество ТСП;  $v_m$  –  $m$ -е ТСП. Такие предприятия оборудуются специальными устройствами – торговыми терминалами. Обозначим  $W = \{w_n, n = 1, 2, \dots, n_W\}$  – множество торговых терминалов, зарегистрированных в ПС;  $w_n$  –  $n$ -й торговый терминал ПС.

**Пункты выдачи наличных** (ПВН) – структурные подразделения экваеров (касса банка, банкоматы), осуществляющих выдачу наличных по ПК. Обозначим  $A = \{a_r, r = 1, 2, \dots, r_A\}$  – множество терминалов выдачи наличных, зарегистрированных в ПС;  $a_r$  –  $r$ -й терминал.

**Держатели ПК** – это физические лица, клиенты банка-эмитента, которые на основании заключенных договоров получили ПК и могут их использовать для инициирования перевода средств из соответствующего счета в банке или осуществлять другие операции с их использованием. Обозначим  $Z = \{z_l, l = 1, 2, \dots, l_Z\}$  – множество клиентов – держателей ПК ПС;  $z_l$  –  $l$ -й клиент ПС.

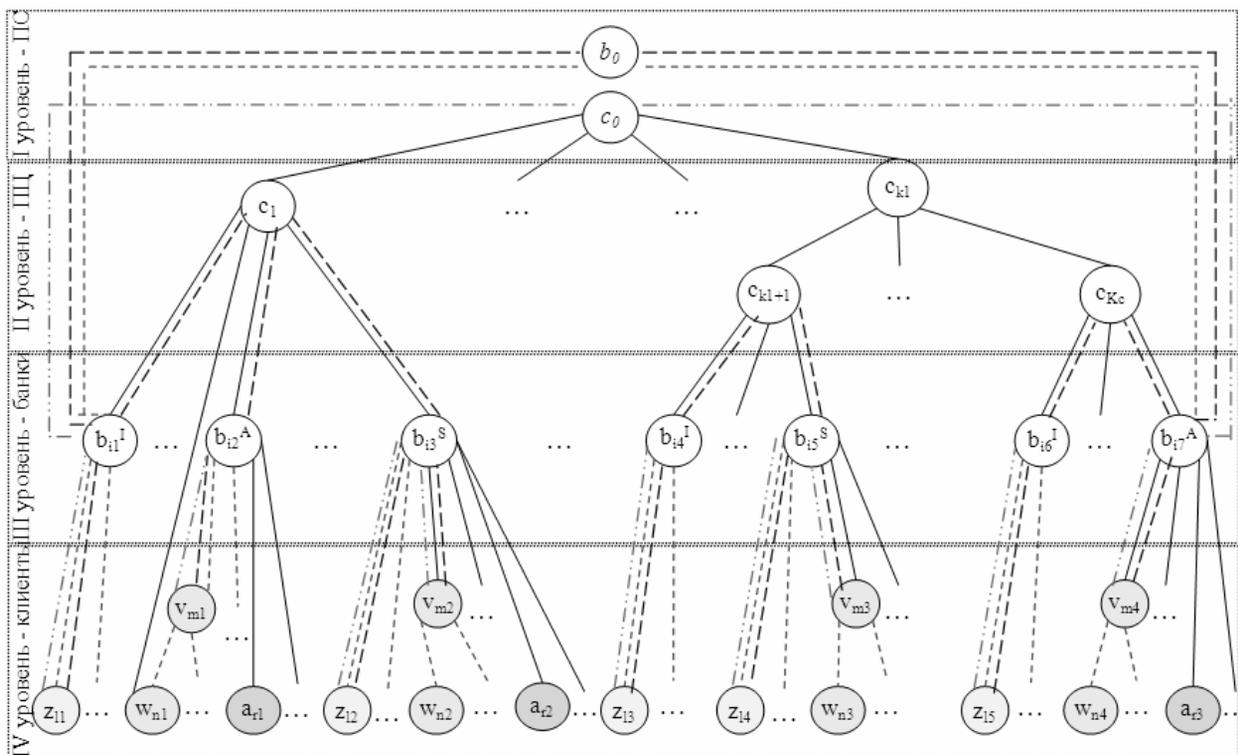
Обозначим множество всех элементов ПС  $\Omega$ , которое состоит из разных классов элементов  $\Omega = (B, C, Z, V, W, A)$ . В множестве  $\Omega$  номера всех элементов ПС уникальны в пределах своего класса.

В основе функционирования ПС лежат договорные (нормативно-правовые акты, договоры), технологические (каналы связи, сеть терминального и сервисного оборудования передачи данных), информационные (обмен транзакционными и другими информационными сообщениями) и финансовые (переводы денежных средств) взаимодействия участников в ПС, обеспечивающие проведение операций с ПК и дальнейшие расчеты по ним [4, 6–7].

Соответственно в общем виде формальную модель структуры ПС можно представить упорядоченным графом  $G(\Omega)$  (рис. 1), с множеством вершин  $\Omega$ , которые составляют участники ПС  $e_i \in \Omega$ , и ребрами  $(e_i, e_j)$ , отображающими

основные взаимодействия участников в ПС [4, 8].

Поскольку ПС является иерархической структурой, выделим уровни иерархии  $\alpha$ ,  $\alpha \in \{I, II, III, IV\}$ . Уровень I – это уровень конечных потребителей услуг ПС: держатели ПК  $Z$ , ТСП  $V$  и ПВН  $A$ . Уровень II состоит из банков-участников ПС  $B$ , предоставляющих услуги конечным пользователям относительно перевода денежных средств в соответствии с выполненными операциями с помощью ПК. Уровень III объединяет множество ПЦ  $C$ , оказывающих технологические услуги для осуществления транзакций. Последний уровень иерархии IV состоит из основных регулирующих, управляющих и координирующих органов ПС: ГПЦ, ГРКЦ, РБ, ПО ПС. Обозначим  $e_i^\alpha$   $i$ -й элемент, который находится на уровне  $\alpha$ ,  $\alpha \in \{I, II, III, IV\}$ ;  $e_i^\alpha \in \Omega$ .



- организационные взаимосвязи (договорные взаимоотношения по обслуживанию и т.п.);
- технологические взаимосвязи (линии связи, маршрутизация запросов, авторизация и т.п.);
- информационные взаимосвязи (расчетно-клиринговые ведомости, выписка по счету);
- финансовые взаимосвязи (перевод средств, оплата счетов, взаиморасчеты, зачисления средств и т.п.).

Рис. 1. Иерархическая структура ПС

Различные схемы взаимодействия структурных элементов ПС, отображенные на рис. 1, и соответствующие им организационно-технологические, информационные и финансовые модели детально рассмотрены в [4]. В частности, финансовая модель ПС представляется через функции финансовых потоков между структурными элементами ПС и имеет вид:

$$\varphi^F(z_i; b_j) = \sum_{t_{z_i}^{ar} \in T_{on-us}^A} \left( s(t_{z_i}^{ar}) + r_{b_j}^{SA}(t_{z_i}^{ar}) \right) + \sum_{t_{z_i}^{ar} \in T_{not-on-us}^A} \left( s(t_{z_i}^{ar}) + r_{b_j}^{IA}(t_{z_i}^{ar}) \right) + \sum_{t_{z_i}^{wn} \in T_{on-us}^P \cup T_{not-on-us}^P} s(t_{z_i}^{wn}), \quad (1)$$

$$\varphi^F(b_j; b_l) = \sum_{t_{z_l}^{ar} \in T_{not-on-us}^A} \left( s(t_{z_l}^{ar}) + r_{b_l}^{AA}(t_{z_l}^{ar}) \right) + \sum_{t_{z_l}^{wn} \in T_{not-on-us}^P} \left( s(t_{z_l}^{wn}) - r_{b_j}^{IP}(t_{z_l}^{wn}) \right), \quad (2)$$

$$\varphi^F(b_i; v_m) = \sum_{t_{z_i}^{wn} \in T_{on-us}^P \cup T_{not-on-us}^P} \left( s(t_{z_i}^{wn}) - r_{b_i}^{AP}(t_{z_i}^{wn}) \right), \quad (3)$$

$$\varphi^F(b_i; c_k) = \sum_{t_{z_i}^{ar} \in T_{on-us}^A \cup T_{not-on-us}^A} r_{c_k}^{CS}(t_{z_i}^{ar}) + \sum_{t_{z_i}^{ar} \in T_{not-on-us}^A} r_{c_k}^{CA}(t_{z_i}^{ar}) + \sum_{t_{z_i}^{wn} \in T_{not-on-us}^P} r_{c_k}^{CP}(t_{z_i}^{wn}), \quad (4)$$

где  $s(t_{z_i}^{\bullet})$  – сумма транзакции  $t_{z_i}^{\bullet}$  ( $t_{z_i}^{\bullet} = t_{z_i}^{ar}$  или  $t_{z_i}^{\bullet} = t_{z_i}^{wn}$ );  $r(t_{z_i}^{\bullet})$  – сумма комиссии по транзакции  $t_{z_i}^{\bullet}$ .

Данные модели позволяют ставить и решать задачи анализа рисков, возникающих в процессе функционирования ПС, оценки убытков от их реализации. Если для каждого из элементов  $e_j^{\alpha} \in \Omega$  определить, классифицировать и оценить возможные риски, которым он подвергается в процессе своей внутренней деятельности, и риски, возникающие в процессе технологического, организационного и финансового взаимодействия с его описателем вершины  $e_i^{\alpha+1} \in \Omega$ , оценить вероятности реализации данных рисков и возможные потери от них, то можно получить комплексную модель оценки и управления рисками в ПС в целом.

## Классификация и структуризация рисков в платежной системе

Риск в ПС выражается вероятностью нежелательных последствий в виде финансовых потерь, потери прибыли и возникновения убытков вследствие нарушения нормального процесса прохождения платежей, неплатежей по выданным кредитам, резких прыжков курса валюты (и как следствие, возникновения не санкционированных кредитов), потери или подделки транзакционных данных, отказа терминального оборудования и т.п. Причем это может вызвать негативные последствия не только для одного элемента ПС, а для всей ПС в целом. Среди основных причин, из-за которых участники ПС подвергаются рискам потерь, можно отметить: ошибки, чрезвычайные события (нарушение энергоснабжения, связи, стихийные бедствия), мошенничество, банкротство поставщиков платежных услуг, неопределенность относительно окончательного выполнения платежных обязательств [2].

Существует довольно много определений риска [2, 9–10]. Согласно [11] будем применять понятие риск как совокупность специфических нежелательных событий, имеющих место в определенный период времени или при определенных условиях и возникающих вследствие реализации определенных опасностей, связанных с организационной, технологической или финансовой деятельностью ПС в целом и каждого ее участника в частности. Опасность – это физическая ситуация с потенциальными повреждениями для коммуникационных сетей и оборудования, которое технологически обеспечивает функционирование ПС (процессинг, авторизация транзакций), повреждениями или незаконным вмешательством в работу общего и специализированного программного обеспечения (ПО) и баз данных (БД), используемых в ПС (системы биллинга, системы перевода средств, системы авторизации, операционные системы банкоматов и т.п.), потенциальными прямыми финансовыми потерями вследствие неплатежеспособности одного или нескольких участников ПС и комбинациями указанных случаев. Опасность, как правило, определяется как ис-

точный вред или убытка, в то время как определение риска включает вероятность того, что вред или убыток действительно будут причинены.

Исчерпывающего перечня и однозначной классификации всех видов рисков ПС в литературе не существует. Проблемой анализа и классификации рисков в ПС занимались разные исследователи [1, 2, 12], однако большинство из них изучали и акцентировали внимание на разных аспектах деятельности ПС, не применяя системный подход. Поэтому комплексной классификации и единого системного подхода к исследованию и управлению рисками в ПС до сих пор не проведено.

На рис. 2 предложена обобщенная структура рисков, возникающих в ПС.

Под **физическим риском** понимают риски потерь, связанных с физической потерей ресурсов в ПС: потеря оборудования, информации; потеря пластика или персонализированных ПК, несанкционированный доступ к содержимому банкоматов, в операционные системы терминалов, линии связи, в процессинговые и криптографические системы; нарушение целостности БД и систем информационной безопасности [1].

С физическим риском тесно связаны **техногенные риски** – выход из строя составляющих прикладной системы и систем связи (аппарат-

ных средств, ПО, каналов связи), что может нарушить инфраструктуру ПС, вследствие стихийных бедствий или намеренных действий, нарушающих безопасность операций [1, 2].

**Операционный риск** – риск полного или частичного отказа программно-аппаратного комплекса поддержки финансовых транзакций и потери БД по уже выполненным транзакциям [2]. Также к операционным рискам в [1] относят все риски непосредственно связанные с ведением текущих операций в ПС: неправильная обработка платежных документов, ошибочное или умышленное необоснованное увеличение лимитов, и, как следствие, риски возникновения несанкционированных овердрафтов, несанкционированного использования ПК, ошибочной загрузки и параметризации банкоматов.

**Юридические риски** – это риски, возникающие в ПС вследствие несовершенной правовой базы, особенностей правового режима [2].

**Риск мошенничества с ПК** – финансово-технологическая разновидность риска ПС, который приводит к финансовым потерям участников ПС вследствие преступных действий с ПК как от имени держателя ПК, так и от чужого имени с целью получения выгоды (денег, товаров, услуг) [1]. Финансовое мошенничество с использованием ПК осуществляется различными способами и построено на несанкционированном списании средств со счетов клиентов банка – держателей ПК [1,3].

Наиболее распространенные виды мошенничества постоянно изменяются вместе с совершенствованием защиты ПК и появляющимися новыми возможностями для мошенничества. Наиболее распространенными категориями мошенничества считаются следующие:

– операции с потерянными или незаконно полученными ПК, являющимися наиболее распространенным видом преступления с ПК (49% всех убытков от мошенничества) [1, 13];

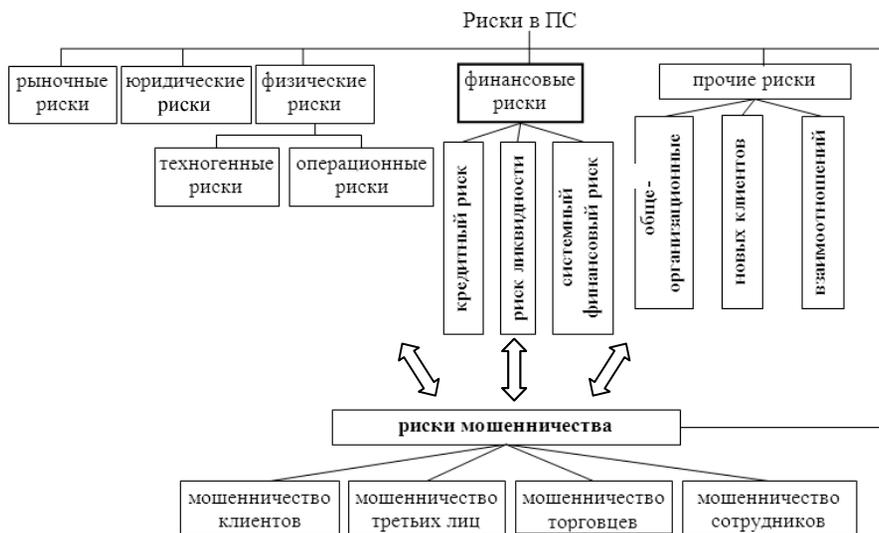


Рис. 2. Классификация рисков в ПС

– операции с поддельными ПК, среди которых выделяют полную подделку ПК, частичную подделку (модификация данных на настоящей ПК) и «белый пластик» (поддельные ПК без внешних реквизитов) [1, 13–14];

– многократная оплата товаров и услуг на суммы, не превышающие лимит авторизации («*Floor limit*»), а следовательно не требующие авторизации и проверки остатка на счете [1, 13];

– мошенничество с почтовыми/телефонными заказами (МОТО) и пр.

К другим видам мошенничества относят разные комбинации рассмотренных ранее способов или новые появляющиеся еще не изученные виды мошенничества.

Заметим, что некоторые исследователи [2] риски мошенничества в ПС, подделки финансовых документов, кражи также относят к группе юридических рисков. Однако считаем, что целесообразно их выделить, поскольку риск мошенничества, хотя и тесно связан с юридическими и операционными рисками, но все же имеет собственные, отличные от последних, источники возникновения и пути развития.

**Финансовые риски** – это риски прямых финансовых потерь, которые возникают вследствие финансовой деятельности участников платежей и обусловлены наличием некоторой неопределенности относительно окончательного выполнения финансовых обязательств участниками ПС при проведении расчетов за осуществленные операции с ПК [1, 2, 12]. Данный вид риска наиболее очевидный, к тому же он легко поддается численной оценке. Среди основных финансовых рисков ПС выделяют: кредитный риск и риск ликвидности [2].

*Кредитный риск* – риск того, что участник операции, который должен выплатить средства, окажется не в состоянии выполнить расчеты по своим обязательствам в определенный срок вследствие своей полной или частичной неплатежеспособности [2].

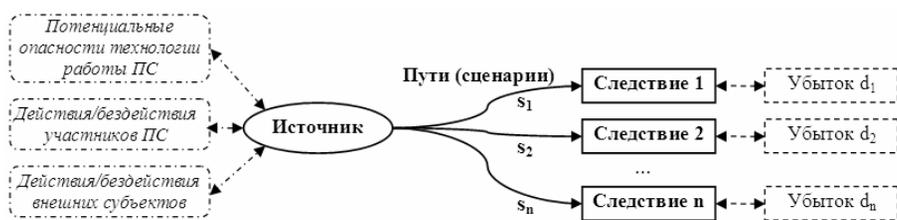


Рис. 3. Базовые элементы в проблеме риска в ПС

*Риск ликвидности* – это риск, возникающий вследствие опасности того, что участник операции или посредник, который должен выплатить средства, может столкнуться с трудностями при покрытии своей отрицательной позиции и не выполнить целиком свои обязательства в определенный срок. Риск ликвидности не означает, что посредник или участник является неплатежеспособным, он, возможно, сможет рассчитаться по своим дебиторским обязательствам позднее, в неопределенное точно время [2].

**Другие типы рисков.** К прочим рискам, присущим элементам ПС, можно отнести:

- *рыночные риски*, возникающие вследствие изменения условий на рынке карточных продуктов и возникновение которых может вызвать появление финансовых рисков;

- *общеорганизационные риски*, происходящие из организации производственных отношений между сотрудниками и подразделениями, кадровый риск, риски, связанные с ошибочной постановкой целей, неадекватного восприятия рынка и т.п. [1];

- *риски, связанные с новыми клиентами*, необходимостью принятия положительного или негативного решения относительно работы с ними: выпуск ПК, подписание эквайрингового соглашения или выдача лицензии на вступление в ПС и т.п. [1];

- *риски взаимоотношений* – неблагоприятное развитие отношений с персоналом, клиентами, партнерами, что может привести к нарушению безопасности ПС, бездеятельности, мошенничеству, и в конце концов убыткам [1].

Перечисленные риски присущи всем участникам ПС. Отдельно следует отметить риски, которым подвергается ПС в целом, присущие

как собственно ПО, так и, как следствие, прочим участникам ПС, особенно при их взаимодействии. **Системный риск ПС** – это риск, связанный с возможными ошибками в концепции построения ПС, ошибками в реализации концепции, ошибками в администрировании ПС [2]. Кроме того, следует отметить **финансовый риск системы** – риск того, что неплатежеспособность одного участника ПС может вызвать невыполнение своих обязательств другими участниками, вызывая тем самым цепную реакцию под названием «эффект домино». Системный риск может возникнуть как по финансовой причине, так и вследствие сбоев в энергоснабжении, сетях связи или отказа оборудования, недостатков ПО, а также при недостаточно налаженном или неправильном управлении рисками в рамках ПС.

Следует отметить, что риски ПС – взаимосвязаны и реализация одного из них может привести к реализации другого вида риска. В значительной мере это касается финансового риска, поскольку любые риски (операционные, техногенные, юридические и т.п.) фактически приводят к финансовым потерям участников ПС, а следовательно и к реализации, той или другой мерой, финансового риска.

С различными рисками (см. рис. 2) сталкивается как каждый элемент ПС в процессе своей собственной деятельности или в процессе взаимодействия с другими элементами ПС, так и ПС в целом. Определим, детализируем и формализуем данные риски для каждого структурного элемента ПС.

### **Анализ рисков в ПС: источники, сценарии, следствия**

Для эффективной оценки рисков в ПС и построения схем и методов их минимизации и управления в ПС целесообразно применять методологию анализа риска, включающую определение, исследование и описание трех элементов риска: источник; сценарий действий (путь развития); следствие (результат) [11], которые являются взаимосвязанными и формируют границы проблемы анализа риска (рис. 3). Действия, связанные с решением проблем анализа и оценки риска, базируются на взаимосвя-

зях элементов риска и могут рассматривать источник, путь и следствия как отдельно, так и в их комбинации.

Источником риска в ПС может быть одна из допустимых потенциальных опасностей, которым подвержены транзакции в ПС, например, недостаточно защищенный канал передачи данных, низкий уровень безопасности производства ПК, недостаточно надежный сервер обработки транзакций, отказ работы терминального оборудования (банкоматы, POS-терминалы) и т.п. В ПС риск может возникнуть и вследствие действий или бездействия субъектов, определяющих состояние рынка и условия деятельности участника на нем. Для каждого из непосредственных участников ПС – эмитенты, эквайеры, картодержатели, ТСП, ПЦ – целесообразно выделять собственные источники риска, обусловленные технологическими особенностями их работы. Кроме того, источниками риска являются и внешние субъекты: карточные мошенники. Авторы [1], учитывая отечественную практику, к генераторам риска относят государственные и регулирующие органы.

Источник риска связан с его последствиями через путь (сценарий) – цепочка событий, связанных с реализацией риска в определенных условиях, приводящих к негативным последствиям определенного участника ПС или всей ПС в целом. Риск противоправных уголовно наказуемых действий связан с осуществлением мошеннических транзакций, незаконной передачей информации третьим лицам или проникновением в БД транзакций. Вообще существует множество путей между источником и следствиями. Пути фактически являются сценариями развития опасной ситуации, построенными с разных позиций и описывающие, что и как может случиться с источником риска. Следствия реализации риска можно оценивать как потерю средств на картсчете, невозможность получить в приемлемое время средства, убытки банка вследствие незаконных или неверных платежей и т.п. Важно оценивать вероятность реализации каждого из описанных сценариев развития риска и убытки от реализации последствий данных сценариев. При ана-

лизе и разработке методов предотвращения реализации риска необходимо уделять внимание сценариям наиболее вероятным и с максимально возможными убытками.

Таким образом, если обозначить  $s_j$  –  $j$ -й сценарий,  $p_j$  – вероятность сценария  $s_j$ ,  $d_j$  – убыток от последствий реализации сценария  $s_j$ , то риск ПС можно определить качественно как множество триплетов  $R = \{(s_j, p_j, d_j)\}_{j=1,2,\dots,n}$  [11]. Каждая компонента триплета  $(s_j, p_j, d_j)$  дает ответ на один из трех вопросов о риске: «Что может случиться?» ( $s_j$ ), «Насколько это вероятно?» ( $p_j$ ), «Какие последствия, убыток?» ( $d_j$ ) и соединяет источник–путь–последствия. Такое определение риска может использоваться для анализа разных объектов и источников риска как в целом в ПС, так и для каждого ее элемента в частности.

Рассмотрим с указанной позиции финансовый кредитный риск и риск мошенничества каждого из участников ПС как два наиболее актуальных вида риска, убытки от реализации которых у участников ПС и вероятность их реализации наибольшие. Основным источником финансового риска для участников ПС является неполная компенсация денежных средств по выполненной на терминале  $a_r$  или  $w_n$  транзакции по ПК  $z_l$ . Для участников ПС могут быть следующие сценарии реализации данного риска.

- Эмитент  $b_j^I$ :  $s_1$  – отсутствие денежных средств на картсчете  $z_l$ ;  $s_2$  – оспаривание картодержателем  $z_l$  факта выполнения транзакции (обратный платеж, *chargebacks*);  $s_3$  – оспаривание картодержателем  $z_l$  факта выполнения транзакции (мошенничество картодержателя);  $s_4$  – оспаривание картодержателем  $z_l$  факта выполнения транзакции (мошенничество третьих лиц).

- Экваер  $b_i^A$ :  $s_5$  – банкротство или проблемы с ликвидностью РБ  $b_0$ ;  $s_6$  – оспаривание картодержателем  $z_l$  факта выполнения транзакции (мошенничество в ТСП  $v_m$ );  $s_7$  – ТСП  $v_m$  не в состоянии выплатить средства по обратным платежам (*chargebacks*).

- РБ  $b_0$ :  $s_8$  – банкротство или проблемы с ликвидностью банка-эмитента  $b_i^I$ .

- ТСП  $v_m$ :  $s_9$  – банкротство или проблемы с ликвидностью банка-экваера  $b_i^A$ ;  $s_{10}$  – оспаривание картодержателем  $z_l$  факта выполнения транзакции (мошенничество картодержателя);  $s_{11}$  – оспаривание картодержателем  $z_l$  факта выполнения транзакции (мошенничество третьих лиц).

- Держатель ПК  $z_l$ :  $s_{12}$  – незаконное использование ПК  $z_l$  (мошенничество третьих лиц);  $s_{13}$  – ошибочные платежные поручения на списания средств.

Обозначим  $p_q$  вероятности реализации сценариев  $s_q, q = \overline{1;13}$  соответственно.

В соответствии с моделью финансовых потоков в ПС (1)–(3), оценка финансовых рисков участников ПС приведена в таблице.

Аналогичным образом можно оценивать и прочие риски в ПС, базируясь на организационно-технологических и информационных моделях взаимодействия структурных элементов ПС.

**Заключение.** Системный анализ принципов функционирования ПС и ее структуры позволил формализовать понятие ПС и разработать организационно-технологические, информационные и финансовые модели взаимодействия ее структурных элементов. На основе данных

Участник ПС	Величина риска	Стоимость потерь
Эмитент $b_j^I$	$p(b_j^I) = p_1 \cdot p_2 \cdot p_3 \cdot p_4$	$d(b_j^I) = \Phi^F(z_l; b_j) \cdot (p_1 \cdot p_2 \cdot p_3 \cdot p_4)$
Экваер $b_i^A$	$p(b_i^A) = p_5 \cdot p_6 \cdot p_7$	$d(b_i^A) = \Phi^F(b_j; b_i) \cdot (p_5 \cdot p_6 \cdot p_7)$
ТСП $v_m$	$p(b_i^A) = p_9 \cdot p_{10} \cdot p_{11}$	$d(v_m) = \Phi^F(b_i; v_m) \cdot (p_9 \cdot p_{10} \cdot p_{11})$
Держатель ПК $z_l$	$p(b_i^A) = p_{12} \cdot p_{13}$	$d(z_l) = \Phi^F(z_l; b_j) \cdot (p_{12} \cdot p_{13})$

формальных моделей поставлена задача выявления и классификации рисков, которым подвержены участники ПС, проведен анализ их особенностей, источников возникновения и основных характеристик, оценены последствия их реализации для различных структурных элементов ПС. При этом особое внимание уделено финансовым рискам и рискам мошенничества с ПК как наиболее актуальным рискам в ПС. Предложенный подход исследования и описания рисков в ПС с учетом методологии «источник–сценарий–последствия» может быть положен в основу построения комплексной модели управления рисками в ПС, разработки и внедрения эффективных мер риск-менеджмента для уменьшения потерь от данных рисков, разработки подходов и методов обеспечения безопасности ПС.

1. *Пластиковые карты* / Л.В. Быстров, А.С. Воронин, А.Ю. Гамольский и др. – М.: БДЦ-пресс, 2005. – 624 с.
2. *Платіжні системи* / А.А. Ющенко, А.С. Савченко, С.Л. Цокол та ін. – К.: Либідь, 1998. – 416с.
3. *Рубинштейн Т.Б., Мирошкина О.В.* Пластиковые карты. – М.: Гелиос АРВ, 2005. – 416 с.
4. *Заславський В.А., Стрижак Г.О.* Моделі аналізу та оптимізації функціонування платіжної системи // Abstracts of the Intern. Conf. «Problems of decision making under uncertainties» (May 12–17, 2008, Kiev–Rivne, Ukraine). – Rivne. – 2008. – P. 110–114.

5. *Гризов А.И.* Новые платежные технологии. Информ.-справ. из-е. – М.: ООО «Рекон Интернешнл», 2007. – 468 с.
6. *Кистанов А.М.* Оценка надежности систем безналичных расчетов на пластиковых картах // Вестн. СамГТУ. Сер. Технические науки. – 2000. – № 8. – С. 63–78
7. *Вавилов А.В., Ильин И.И.* Пластиковые карты: принципы построения платежных систем. – М.: Европиум-пресс, 1999. – 128 с.
8. *Оре О.* Теория графов. – М.: Наука, 1980. – 336 с.
9. *Вітлінський В.В.* Кредитний ризик комерційного банку. – К.: Т-во «Знання», 2000. – 251 с.
10. *Коваленко Н.* Моделирование рисков в банковском деле // Финансовые риски. – 1997. – № 3. – С. 91–94.
11. *Заславський В.А.* Мониторинг и анализ рисков в платежных системах. Соціальні ризики. / Під. ред.: Ю.І. Сасенко, Ю.О. Привалов. – К.: ПЦ «Фоліант», 2004. – Т. 2. – С. 224–270.
12. *Савченко А.С.* Аналіз ризиків в системах масових електронних платежів // Вісн. Укр. акад. банк. справи. – 1999. – № 1(6). – С. 70–75.
13. *Managing risk in the 21th century. Strategies for Issuing&Acceptance.* – Visa Int., Oct., 2000. – 156 p.
14. *Способы совершения преступлений с использованием банковских платежных карт* / М.С. Вергузаев, Я.Ю. Кондратьев, С.Е. Пугачев и др. // Информ. технол. та захист інформ.: Зб. наук. праць. – Запоріжжя: Юридичний ін-т МВС України, 1999. – 3. – № 1. – С. 50–67.

Поступила .25.07.2010  
 Тел. для справок: (044) 494-4390, 550-9238 (Киев)  
 E-mail: st-anna@ukr.net  
 © А.А. Стрижак, 2010