**ТЕМА 6: ПЛАТЁЖНЫЕ СИСТЕМЫ. КЛЮЧЕВЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ ПС**

## 6.1. Общие положения

**Платежная система –** это совокупность банковских и финансовых институтов, платежных инструментов, банковских правил и процедур, а также межбанковских систем перевода денежных средств, обеспечивающих обращение денежных средств внутри страны и взаимодействие с зарубежными платежными системами.

**Платежные инструменты, используемые при безналичных расчетах в Республике Беларусь:**

- платежные поручения
- платежные требования
- чеки
- требования-поручения
- аккредитивы
- банковские пластиковые карточки

**Что входит в понятие «платёжная система»?**

Проектные решения платежных систем в различных странах мира различаются в значительной степени. Определяющими элементами платежной системы является «совокупность инструментов, банковских процедур и, как правило, межбанковские системы переводов средств, обеспечивающие обращение денежных средств». В центре внимания находится система перевода средств, то есть ядро платежной системы. Это, как правило, связано с соглашением между определенной группой участников системы и системным оператором, в котором определяются правила и процедуры, касающиеся перевода средств между участниками. Участники могут быть прямыми или косвенными. Банк международных расчетов (далее БМР) признается, что главным назначением платежных систем является обслуживание экономики, но их специфическое предназначение означает, что они не связаны непосредственно с правами и обязанностями каких-либо иных сторон, кроме системных операторов, участников систем и центральных банков. Так, например, при обсуждении правовой основы окончательности расчета, в центре внимания находится расчет между участниками систем.

Платежные системы находятся в сердце финансового сектора. Вместе с быстрыми технологическими переменами на национальном и международном уровнях, а также конкуренцией в этой области, государственная политика должна постоянно уделять внимание поддержке безопасности и эффективности платежных систем обоих уровней.

## 6.2. Определение системно значимых платежных систем

Важнейшим шагом в применении Ключевых принципов является разграничение платежных систем, являющихся системно значимыми, от иных. В стране может быть несколько платежных систем, которые являются важными для пользователей и для непрерывной и эффективной работы экономики в целом. Отличительной чертой системно значимой платежной системы является то, что она способна вызывать или передавать потрясения (шоки) в собственной или даже международной финансовой системе. Большинство стран имеют по крайней мере одну такую систему.

Главным фактором при оценке потенциальной возможности платежной системы вызвать или спровоцировать системные сбои является сумма обрабатываемых системой платежей в совокупном или индивидуальном выражении, по отношению к ресурсам участников системы и в контексте всей финансовой системы в целом.

Еще одним фактором при определении системной значимости системы является характер обрабатываемых платежей. Система, предназначенная для расчетов по иным платежным системам (например, если в ней обрабатываются платежи чистых сумм для расчетов по многосторонней неттинговой расчетной системе) или система для обработки платежей для расчета по транзакциям финансового рынка (например, транзакций на денежных рынках или рынках валют, или по переводам денег для операций на рынке ценных бумаг) обычно рассматривается как системно значимая платежная система.

Считается, что система является системно значимой, если к ней применимо хотя бы одно из следующих условий:

- она является единственной платежной системой в стране или главной системой с учетом совокупной величины платежей;
- в ней обрабатываются в основном крупные платежи;
- она используется для расчета транзакций финансового рынка или для расчета иных платежных систем.

Ключевые принципы предназначены для внедрения во всех странах в разумные временные сроки, независимо от того, является ли их экономика развитой, переходной или развивающейся. Конкретное применение Ключевых принципов зависит от экономического уровня развития страны, от институциональной структуры экономики и инфраструктуры в целом. При этом Ключевые принципы могут быть полезными при первоначальной оценке платежных систем, при постоянном контроле за их безопасностью и эффективностью, а также при разработке проектов модернизации.

Ключевой принцип I – Система должна иметь хорошо проработанную правовую базу во всех соответствующих юрисдикциях

Ключевой принцип II – Правила и процедуры системы должны давать участникам четкое представление о влиянии системы на каждый из финансовых рисков, которые они несут в силу их участия в системе.

Ключевой принцип III – Система должна иметь четко определенные процедуры управления кредитными рисками и рисками ликвидности, устанавливающие ответственность оператора системы и участников, а также содержащие надлежащие стимулы для управления этими рисками и их сдерживания.

Ключевой принцип IV – Система должна обеспечивать быстрый окончательный расчет в день валютирования, предпочтительно в течение дня или, как минимум, на конец дня.

Ключевой принцип V – Система, в которой осуществляется многосторонний неттинг, должна быть, как минимум, в состоянии обеспечить своевременное завершение ежедневных расчетов в случае неспособности участника произвести расчет по самому крупному расчетному обязательству.

Ключевой принцип VI – Средства, используемые для расчета, должны быть предпочтительно в форме требований к центральному банку; если используются иные средства, они должны иметь незначительный или нулевой кредитный риск или риск ликвидности.

Ключевой принцип VII – Система должна обеспечивать высокую степень безопасности и операционной надежности, а также должна иметь запасные процедуры для нештатных ситуаций, позволяющих своевременно завершить обработку данных за день.

Ключевой принцип VIII – Система должна предлагать такие средства для проведения платежей, которые являются практичными для пользователей и эффективными для экономики.

Ключевой принцип IX – Система должна иметь объективные и публично объявленные критерии для участия, обеспечивающие справедливый и открытый доступ.

Ключевой принцип X – Процедуры управления (руководства) системой должны быть эффективными, подотчетными и прозрачными.

Для обеспечения точности и целостности транзакций, система должна использовать целесообразные с экономической точки зрения стандарты безопасности. Стандарты, относящиеся к использованию информации, должны анализироваться на их соответствие имеющейся на данный момент технологии. Для завершения дневного цикла обработки, система должна поддерживать высокую степень операционной гибкости. Это вопрос не только наличия надежной технологии и резервирования всего программно-технического и сетевого комплекса. Кроме этого, необходимо иметь в наличии эффективные производственные процедуры и хорошо обученный и компетентный персонал, который умеет надежно и эффективно эксплуатировать систему и обеспечивать исполнение всех процедур. Степень надежности зависит также от наличия альтернативных механизмов проведения платежей в чрезвычайных ситуациях.

**Критерии оценки**

В системе должны быть решены следующие вопросы.

Разработчики и операторы платежных систем должны рассмотреть следующие вопросы в отношении безопасности и операционной надежности системы:

**Общие вопросы**

a) Система должна отвечать принципам безопасности и уровням качества операционных услуг, согласованным между системным оператором и участниками, а также соответствующим правовым нормам, системным правилам, процедурам управления риском, производственным требованиям и международным, национальным или отраслевым стандартам.

b) Безопасность системы и операционная надежность зависят как от центральной системы, так и от системных компонентов участников; участники также несут ответственность за безопасность и операционную надежность. Система должна осуществлять официальный контроль над соблюдением соответствующего уровня качества услуг.

c) Принципы безопасности и уровни качества операционных услуг со временем должны изменяться в соответствии с развитием рынка и технологий; система должна проектироваться и работать в соответствии с этими изменениями.

d) Система требует адекватного числа хорошо обученных, компетентных и надежных сотрудников для безотказной и эффективной эксплуатации системы в нормальных и чрезвычайных ситуациях.

**Безопасность**

e) Задачи и политика безопасности должны определяться во время проектирования системы и периодически пересматриваться. Они должны подходить системе, учитывать ее конкретную архитектуру и форму собственности.

f) Безопасность системы должна соответствовать экономически разумным стандартам, например, стандартам конфиденциальности, целостности, аутентификации, безотказности, операционной надежности, доступности и подконтрольности. Характеристики безопасности должны регулярно тестироваться.

g) Система должна регулярно подвергаться анализу на предмет рисков безопасности. Системный оператор должен постоянно следить за технологическим прогрессом и проводить анализ рисков безопасности системы на самом современном уровне.

**Операционная надежность**

h) Угрозы операционной надежности возникают не только при сбое центральной системы и компонентов участников, но также и при выходе из строя обслуживающей инфраструктуры и в случае природных катастроф.

i) В системе должны присутствовать всеобъемлющие, строгие и хорошо документированные операционные и технические процедуры.

j) Изменения в системе должны быть хорошо документированы, санкционированы, подконтрольны, протестированы и подвергнуты контролю качества.

k) Система должна быть спроектирована с достаточным запасом мощности, которая должна контролироваться и наращиваться в предвидении изменений производственных объемов.

**Непрерывность производственного процесса**

l) Системный оператор обязан осуществлять официальное планирование непрерывности производственного процесса. При разработке мероприятий для аварийных обстоятельств, следует учитывать принципы простоты и практичности.

m) Мероприятия по обеспечению непрерывности производственного процесса должны быть документированы и регулярно тестироваться. Они должны включать процедуры управления кризисными ситуациями и процедуры оповещения.

Мероприятия по обеспечению непрерывности производственного процесса могут включать в себя:

- перенос обработки платежей в другую платежную систему,
- создание второго центра обработки данных,
- введение режима «обслуживания на минимальном уровне».

Кроме этого, следует произвести оценку следующих аспектов:

**Операционная надежность**

n) Должны быть внедрены внутренние принципы и процедуры контроля, включая меры безопасности, предназначенные для ограничения операционного риска.

o) Все аспекты вычислительной системы должны быть документированы и обновлены. Следует иметь процедуру проведения аудита независимым специалистом по безопасности и возможность отслеживать обработку отдельной транзакции с начала до конца процесса.

p) Внутренний аудит должен проверять меры контроля операционного риска на регулярной основе.

q) Должен периодически проводиться внешнего аудит систем информационных технологий.

**Непрерывность производственного процесса**

r) В случае выхода из строя основного вычислительного комплекса, следует иметь в наличии резервные средства.

s) В случае необходимости перехода на резервную систему следует иметь специальные процедуры сохранения всех данных по транзакциям. Резервная система должна находиться на достаточном расстоянии от места расположения главного центра обработки данных и использовать другие телекоммуникации и линии электропитания.

t) В случае выхода из строя основных систем, следует иметь планы действий в чрезвычайных ситуациях (включая план действий при природных катастрофах и план восстановительных мероприятий).

u) Отчеты о мониторинге производительности системы и о показателях качества должны составляться не реже раза в квартал. Системный оператор должен иметь план моделирования производительности важнейших систем, которые должны периодически тестироваться под пиковой нагрузкой.

v) Старший персонал, включая лиц, не несущих ответственность за соответствующие операции, должен регулярно изучать вопросы безопасности и высказывать свое мнение.

w) Система должна использовать отказоустойчивое или дублирующее оборудование и телекоммуникационные средства.

x) Документация процедур системы должна быть ясной и периодически обновляемой; она должна быть в наличии как на основном, так и резервном центрах. Следует иметь процедуры для копирования данных и ПО при их изменении. Следует также иметь процедуры обмена физическими данными на бумаге или дисках в ситуациях выхода из строя основных телекоммуникаций.

**Пояснения и замечания**

a) Полезной информацией для оценки операционной надежности системы является следующая:

- Сколько раз за прошлый год система давала сбои?
- Сколько времени потребовалось на восстановление обработки?
- Какими были масштабы потерь данных (транзакции и контролируемые служебные данные) и каким образом они были восстановлены?

b) Для оценки соответствия КП VII, эксперт должен провести беседы в центральном банке со специалистами департамента ИТ, аудиторами ИТ, специалистами платежных систем, органами надзора и системным оператором. Если центральный банк не является оператором и не производил оценку системы, такие беседы следует провести с частным оператором, его специалистами ИТ и аудиторами ИТ. Кроме этого, следует поговорить с произвольно выбранными участниками, особенно с их служащими, ответственными за вопросы ИТ.

c) Для управления безопасностью, операционными рисками и непрерывностью производственного процесса существуют разные способы, и приведенные выше критерии являются примерами таких механизмов. Для соответствия КП не обязательно соответствовать всем критериям оценки. Эксперт должен проанализировать, достаточны ли средства, используемые системой для управления этими рисками, или необходимо предпринять дополнительные меры.

d) Взаимосвязь с другими Ключевыми принципами: Выбор принципов политики, используемых для решения вопросов безопасности и операционной надежности, должен производиться с учетом таких аспектов, как практичность и эффективность, рассматриваемых в КП VIII.

Системно значимая платежная система должна проектироваться и эксплуатироваться с высокой степенью безопасности и операционной надежности, что соответствует, учитывая ее особенность, ее назначению и требованиям пользователей. Специфические факторы могут значительно различаться в системах. Более того, технологический процесс в мире развивается очень быстро, меняя как характер требований пользователей, так и возможности их выполнения. В связи с этим в данном разделе говорится только в общем смысле о тех факторах, которые следует рассмотреть. Системно важная платежная система как правило, но не обязательно, является технически сложной, и именно этот случай рассматривается в данном

разделе. Однако многие из этих учитываемых факторов распространяются и на иные аналогичные системные проектные решения.

▪Политические решения должны базироваться на рассмотрении вопросов безопасности и операционной надежности, а также практической целесообразности и эффективности, рассматриваемые в Ключевом принципе VIII. Этот выбор является как правило предметом консультаций между системным оператором и участниками, результат которых выливается в соглашение о принципах и уровнях услуг. Такое соглашение достигается как правило на высшем уровне руководства. Это делается для того, чтобы лица, разрабатывающие принципы и уровни услуг, были теми же лицами, кто несет ответственность за поддержку соответствующего равновесия между расходами на внедрение принципов и уровней услуг и выгодами, получаемыми от надежности системы и бесперебойного предоставления услуг. При проектировании системы и ее эксплуатации следует также проанализировать любые правовые ограничения, системные правила, процедуры управления риском и соответствующие операционные требования, имеющие отношение к безопасности и операционной надежности.

▪Операционная надежность системы зависит от операционной надежности всех ее компонентов (включая оборудование, ПО, телекоммуникационную сеть, энергоснабжение, служащих). Разработчики и операторы платежной системы обязаны заниматься вопросами безопасности и операционной надежности компонентов центральной системы, но также и компонентов систем участников (включая, если требуется, косвенных участников). Такое вмешательство может выходить за пределы первоначального интерфейса с системой и включать операции участников, которые могут оказать отрицательное воздействие на работу платежной системы. Вот почему участники системы несут ответственность за безопасность и операционную надежность всей платежной системы в целом, что должно быть отражено во всех соответствующих правилах и контрактах.

▪Оператор платежной системы должен контролировать и определять, отвечает ли система принципам безопасности и операционным уровням услуг. Это должен быть постоянный и всеобъемлющий процесс с привлечением внутренних и/или внешних аудиторов. Сюда же входит мониторинг безопасности и операционной надежности участников, например, рабочая готовность их компонентов в течение обычных рабочих часов. Если участники создают излишний риск платежной системы или иных участников, системный оператор обязан, например, поставить в известность старших руководителей участника или, в особо серьезных случаях, предупредить системный надзор.

▪Система должна иметь соответствующее количество хорошо обученных, компетентных и надежных служащих. Они должны быть способны надежно и эффективно управлять системой и обеспечивать выполнение процедур операционного управления и управления риском в нормальных и чрезвычайных ситуациях. Некоторые служащие должны действовать как операционные администраторы и администраторы безопасности и иметь соответствующий уровень знаний, опыта и полномочий для выполнения своих задач. Обучение персонала должно включать углубленное понимание системы и ее назначения, чтобы операционные решения принимались на фоне имеющихся знаний. Персонал, ответственный за техническую

поддержку всех компонентов системы, должен быть на рабочем месте по мере надобности (включая вне рабочих часов) для исправления ошибок и решения проблем.

▪Политика безопасности платежной системы и уровни операционных услуг со временем меняются в ответ на изменения на рынке платежных услуг (таких, как рост спроса и новые участники или клиенты), а также в ответ на технологические изменения, которые дают возможность осуществлять более надежную, быструю, эффективную или более эффективную с точки зрения цены обработку. Это проходит менее болезненно, если проектная разработка и эксплуатация системы обладают достаточной гибкостью, чтобы приспособиться к имеющимся изменениям.

▪Современные тенденции системного проектирования уделяют особое внимание безопасности и операционной надежности использования технологий «открытых систем» (часто называемых «интернет-технологиями» или «веб-технологиями»). Последние являются чрезвычайно популярными, поскольку они упрощают доступ и совместное использование данных и вычислительных ресурсов, однако их использование для системно значимых платежных систем ставит серьезные проблемы при создании соответствующей операционной целостности. Использование Интернета, в частности, поднимает особые вопросы, поскольку эта сеть не имеет четко определенного владельца или оператора, в связи с чем нет надежности (например, гарантии) качества услуг. В более общем плане, использование технологий открытых систем требует пристального внимания к возможным проникновениям или иным типам попыток нарушения защиты ресурсов со стороны киберов (например, проникновение в электронное хранилище, искажение базы данных, подделка кода или отмена услуги). При использовании таких технологий в системно значимых платежных системах большую роль должен играть план мероприятий в аварийных ситуациях. Так, например, может потребоваться, чтобы система имела возможность реагировать на событие в масштабах всей системы, включая способность быстро и систематически привлекать соответствующие технические, производственные и человеческие ресурсы, а также юридическую базу. Кроме такого планирования чрезвычайных мероприятий, система могла бы, например, разработать собственные возможности для выявления и учета попыток нарушения защиты. Кроме этого, особое внимание должно быть уделено порядку использования коммерческого ПО, имеющегося в готовом виде, для системно значимых платежных систем, поскольку эти системы требуют высокого стандарта безопасности и операционной надежности.

**Безопасность**

▪Цели и политика безопасности должны быть четко определены и документированы. Их конкретное содержание зависит от конкретной платежной системы, ее контекста и требований ее пользователей, но они должны быть достаточно строгими для оператора системы, участников, пользователей и органов надзора, чтобы обеспечивать доверие к системе. Цели и политика безопасности системно значимых платежных систем затрагивают системного оператора, участников и, возможно, клиентов с прямым доступом к системе или ее данным. Они должны устанавливаться в период проектирования системы и периодически пересматриваться, особенно, если в системе и ее компонентах происходят значительные изменения. Характеристики безопасности должны регулярно тестироваться.

▪Цели и политика безопасности зависят от архитектуры системы и типа собственности на нее. Например, высоко централизованная система (в которой центральные компоненты, сеть и даже производственные комплексы участников принадлежат или эксплуатируются единым органом) могут иметь высоко централизованные цели и политику безопасности. С другой стороны, среда с распределенной обработкой (где системные компоненты могут иметь различных операторов и владельцев) требует, чтобы процесс обработки имел общие цели и принципы безопасности, четкое распределение ответственности за их внедрение, хорошую координацию участников, что позволит обеспечить логическое объединение общего операционного управления и контроль за системой.

▪При выработке целей и политики безопасности следует учитывать экономически целесообразное соответствие стандартам, например, конфиденциальности, целостности, аутентификации, безотказности, операционной готовности и возможности аудиторского отслеживания операций. Они должны включать четкие принципы контроля как за физическим, так и логическим доступом к системе, ее оборудованию, ПО и сети для защиты системы и ее данных от несанкционированных действий как внутренних, так и внешних сторон. Вполне нормально строго ограничивать доступ к платежной системе лишь теми лицами, кто имеет правомерное разрешение на доступ, и ограничивать его теми функциями, которые имеет данное лицо.

▪Важная роль принадлежит проведению регулярного анализа риска безопасности с использованием признанных и структурированных методологий. Такой анализ должен, например, проводиться в период проектирования системы, а в последствие, когда меняется производственная среда или предлагается существенно изменить проектное решение системы; кроме этого, следует проводить периодический анализ (например, ежегодно) во время всего жизненного цикла системы. Со временем технологический прогресс может привести к росту угроз в системе, а также к появлению новых или усовершенствованию старых методов защиты и контроля. Системный оператор должен в связи с этим активно отслеживать технологические новшества, чтобы анализ риска безопасности системы всегда был на современном уровне. Типичные элементы анализа риска безопасности показаны в Комментарии 14.

Комментарий 14

Типичные элементы анализа риска безопасности

- Установить или пересмотреть цели и политику безопасности системы
- Определить функции системы, компоненты, границы и области ответственности
- Определить возможные угрозы и их масштаб (возможные воздействия и вероятность их возникновения)
- Определить существующие и потенциальные защитные средства (такие как физические устройства, ПО безопасности и организационные или операционные процедуры)
- Определить все остаточные риски и уязвимые места
- Повторять последние два шага до тех пор, пока остаточные риски и уязвимые места не будут находится на приемлемом уровне с учетом целей и политики безопасности системы

- Внедрить в систему меры безопасности, определенные в ходе проведения анализа риска.

**Операционная надежность**

▪Стандарты операционной надежности, необходимые для платежной системы, должны быть определены формально и документированы системным оператором и участниками как “соглашение об уровне услуг”. Уровни услуг могут отличаться, например, в зависимости от быстроты расчета системы. В системе с расчетом в реальном времени на валовой основе уровни услуг могут определять максимальный период незапланированного «простоя», в то время как в системе с расчетом в конце дня они будут относиться к периоду расчета. Уровень требуемой операционной надежности также может зависеть от наличия альтернативного механизма проведения платежей (такого, например, как иная платежная система) в случае серьезного сбоя системы или ее участников.

▪Операционная надежность платежной системы связана не столько с компонентами центральной системы и участников, а с операционной надежностью инфраструктуры, от услуг которой она зависит, например, телекоммуникаций, энергоснабжения и транспорта (предоставляемых частным или государственным сектором). Угрозы прерывания услуг могут возникнуть не только из-за сбоя этих отдельных компонентов и услуг, но также и в связи с внешними событиями, например, происшествиями, затрагивающими всю отрасль, событиями общего плана, например, пожар, землетрясение или наводнение. Большое внимание в период проектирования системы следует уделить устранению ситуации, при которой выход из строя любого конкретного компонента системы приводит к выходу из строя всей системы («одна аварийная точка»). Все компоненты и угрозы должны быть учтены в мероприятиях по обеспечению непрерывности производственного процесса

▪Системный оператор обязан разработать и внедрить в практику всеобъемлющие, строгие и хорошо документированные операционные и технические процедуры. Сюда должны войти процедуры по регистрации, отчетности и анализу всех операционных происшествий. После каждого значительного нарушения работы платежной системы оператор и, если требуется, участники должны предпринять «посмертное» расследование для выявления причин, а также провести модернизацию, требующуюся для нормальной работы или для обеспечения непрерывного производственного процесса.

▪Любое значительное изменение системы и ее компонентов, включая компоненты, принадлежащие ее участникам, должны быть хорошо документированы, санкционированы, контролируемы, протестированы и подвергнуты процедурам приемки на качество соответствующими сторонами. Разработка и тестирование всех изменений должны проводиться без влияния на работу системы; этого можно достичь, используя для разработки иную систему, которая как можно точнее повторяет производственную и имеет те же уровни безопасности и контроля, что и производственная система. Если возможно, внедрение изменений должно проводиться так, чтобы внесенные изменения можно было при необходимости отменить, вернув систему в первоначальное состояние.

▪Проектное решение системы должно обеспечивать наличие достаточной мощности для обработки предполагаемого объема платежей с требуемой скоростью,

особенно в пиковое время и дни. Системный оператор должен регулярно контролировать и тестировать имеющуюся на данный момент мощность системы и ее производительность и тщательно планировать изменения объемов или производственную конфигурацию, чтобы поддерживать необходимые уровни пропускной способности и скорости прохождения платежей.

▪Для платежной системы критичными считаются операционная надежность телекоммуникационных средств. Резервные или альтернативные телекоммуникационные средства и маршрутизация (например, использование коммутируемых телекоммуникационных линий как альтернативы выделенным линиям) могут сыграть здесь свою положительную роль. В большинстве случаев платежная система зависит от одного или более поставщиков телекоммуникационных услуг, а также от надежности государственной телекоммуникационной инфраструктуры. По возможности оператор платежной системы должен в контрактах с телекоммуникационными компаниями определить требуемые уровни услуг и запасные маршруты, разработать аварийные планы.

**Непрерывность производственного процесса**

▪Целью мероприятий по обеспечению непрерывности производственной деятельности является стремление обеспечить предоставление согласованных уровней услуг даже в ситуации, когда выходят из строя один или более компонентов системы. Оператор платежной системы, а если требуется, то и участники и провайдеры услуг инфраструктуры, должны предпринять совместные действия по созданию плана мероприятий по обеспечению непрерывности обслуживания в самых разнообразных возможных сценариях. Эти сценарии должны включать выход из строя центральных компонентов, компонентов участников и используемой инфраструктуры. Следует рассмотреть как внутренние, так и внешние угрозы, а также последствия каждого сбоя. Затем следует разработать мероприятия для предупреждения, смягчения и/или реагирования на каждый тип аварии. (Некоторые примеры мероприятий по обеспечению непрерывности производственного процесса приведены в Комментарии 15). Простота и практичность – ключевые моменты при проектировании резервных систем и процедур действий во внештатных ситуациях. Они должны активизироваться во время нештатных ситуаций и несмотря на обучение и тестирование, естественно, менее знакомы персоналу, который сталкивается лишь с повседневными операционными процедурами.

▪Все аспекты мероприятий по обеспечению непрерывности производственного процесса должны быть четко и полно документированы. Сотрудники оператора платежной системы и участников должны получить надлежащее обучение и тренировку в их применении. Все элементы должны регулярно тестироваться с привлечением участников системы и иных сторон, кто будет привлечен к таким мероприятиям.

▪Процедуры по быстрому формированию разносторонней группы для разрешения кризисных ситуаций являются важным элементом таких мероприятий, включая, если требуется, процедуры консультаций с участниками, органами надзора и иными заинтересованными сторонами. Мероприятия могли бы включать, например, процедуры по оперативному и регулярному информированию участников, их клиентов, иные финансовые службы, органы надзора и средства массовой информации об инцидентах и их влиянии на платежные услуги.

▪Если мероприятия по обеспечению непрерывности производственного процесса включают переключение на обработку критически важных платежей в иную платежную систему, эта возможность должны быть оговорена, согласована и протестирована заранее с оператором этой системы, чтобы предупредить негативное влияние, которое может оказать поступление этих платежей на производительность резервной платежной системы.

▪Зачастую мероприятия по обеспечению непрерывности производственного процесса включают в себя создание запасного процессингового центра. Проектное решение такого центра должно учитывать время, необходимое для его запуска и для начала обработки платежей на новом месте. Что касается системы платежа в реальном времени на валовой основе, резервный центр должен содержаться в режиме «горячего резерва» с постоянным поступлением данных с основного центра, чтобы обработка могла возобновиться на новом месте в течение нескольких минут. Что касается системы с расчетом в конце дня, то время возобновления ее работы может быть более поздним (скорее определяемое в часах, а не в минутах). Второй процессинговый центр, как правило, проектируется с аналогичным ПО, оборудованием и телекоммуникациями, что и основной (для упрощения контроля, сопровождения и тестирования). Впрочем, идентичное ПО, вряд ли будет надежной защитой в случае сбоя ПО на основном центре. Место нахождения второго процессингового центра зависит от характера угроз, от которых он предназначен предохранять. Типичным здесь является защита от выхода из строя одной из инфраструктурных систем (например, электроснабжения или сети телекоммуникаций), оказывающей негативные последствия на основной и резервный центры. Системный оператор должен также принять решение о том, обязаны ли участники иметь резервный процессинговый центр; такая возможность может быть обеспечена двусторонним соглашением междуучастникам об использовании их процессинговых центров; можно также предусмотреть планом аварийных мер использование центрального процессингового центра участником, имеющим серьезную аварию.

▪ Мероприятия по обеспечению непрерывности производственного процесса платежной системы могут включать возможность использования при серьезном сбое «минимального уровня услуг» для обработки небольшого количества критичных платежей (например, относящихся к расчетам для другой платежной и расчетной системы, рыночной ликвидности или монетарной политике). Этот минимальный уровень услуг, может быть, достигнут, например, посредством ручной обработки документов на бумажном носителе, отправку аутентифицированных факсимильных сообщений или использование системы на базе ПЭВМ с применением физических носителей для передачи данных.

Комментарий 15

Примеры мероприятий для обеспечения непрерывности производственного процесса

- Использование отказоустойчивого или дублирующего оборудования.
- Регулярное профилактическое обслуживание всех вычислительных и телекоммуникационных комплексов.
- Наличие на месте запасных частей для оборудования и телекоммуникационных компонентов.

- Производство электроэнергии на месте или применение источников непрерывного питания, а также независимая подача воды.
- Системы обнаружения огня и противопожарные системы.
- Ведение простой и постоянно обновляемой процедурной и технической документации на основном и запасном центрах.
- Процедуры по копированию текущих данных, копированию ПОпри его изменении, причем критичные его компоненты должны храниться вне основного центра.
- Процедуры обмена данными на основе физических носителей (дискеты, лента, бумага) в случае телекоммуникационных сбоев.
- Процедуры отключения некоторых системных функций или участников и запуска или остановки некоторых процессов, безотносительно их производственной последовательности.
- При введении нового компонента ПО, оборудования или телекоммуникаций, предусмотреть возможность сохранения в течение некоторого времени способности к возврату на прежнюю технологию.