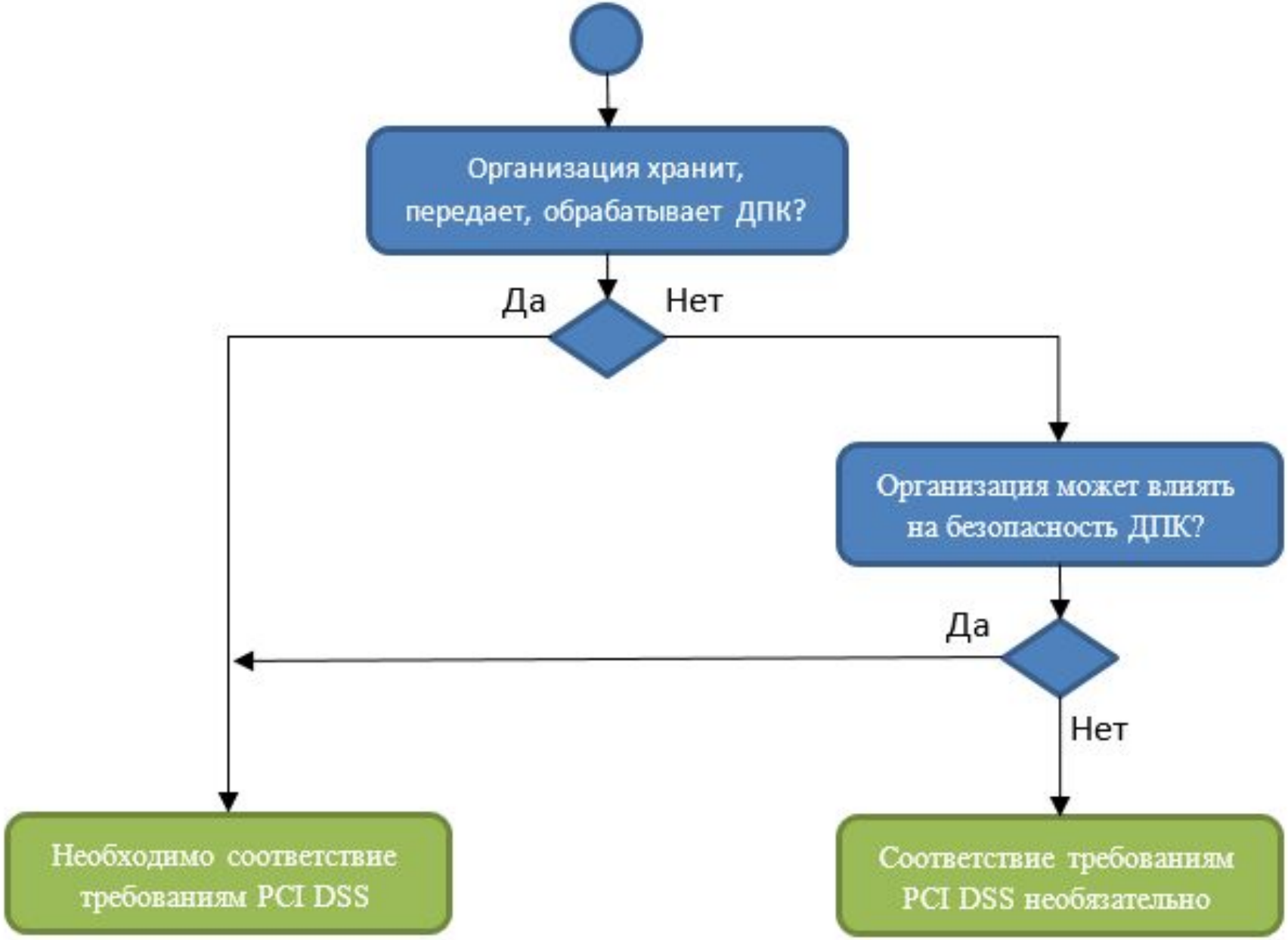
Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет
при Правительстве Российской Федерации»
(Финансовый университет)

PCI DSS

Выполнила: студентка группы ИБ3-3
Петрова Юлия

PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) — стандарт безопасности данных индустрии платежных карт. Стандарт разработан международными платежными системами Visa и MasterCard. Любая организация, планирующая принимать и обрабатывать данные банковских карт на своем сайте, должна соответствовать требованиям PCI DSS.



ДПК - данные платежных карт

Для соответствия стандарту необходимо выполнение определенных требований, вот некоторые из них:

- защита вычислительной сети,
- управление доступом к данным о держателях карт,
- конфигурация компонентов информационной инфраструктуры,
- механизмы аутентификации,
- физическая защита информационной инфраструктуры,
- защита передаваемых данных о держателях карт и так далее

В общем, стандарт требует прохождения порядка 440 проверочных процедур.

Способы подтверждения соответствия требованиям стандарта

- Существуют различные способы подтверждения соответствия требованиям стандарта PCI DSS, которые заключаются в проведении внешнего аудита (QSA), внутреннего аудита (ISA) или проведении организацией самооценки (SAQ).
- **Внешний аудит QSA** выполняется внешней аудиторской организацией, сертифицированной Советом PCI SSC. В ходе проверки аудиторы собирают свидетельства выполнения требований стандарта и сохраняют их на период длительностью в три года.
- **Внутренний аудит ISA** выполняется внутренним, прошедшим обучение и сертифицированным по программе Совета PCI SSC, аудитором. Что касается **самооценки SAQ**, то она выполняется самостоятельно путём заполнения листа самооценки. В этом случае сбор свидетельств выполнения требований стандарта не требуется.

Типы организаций

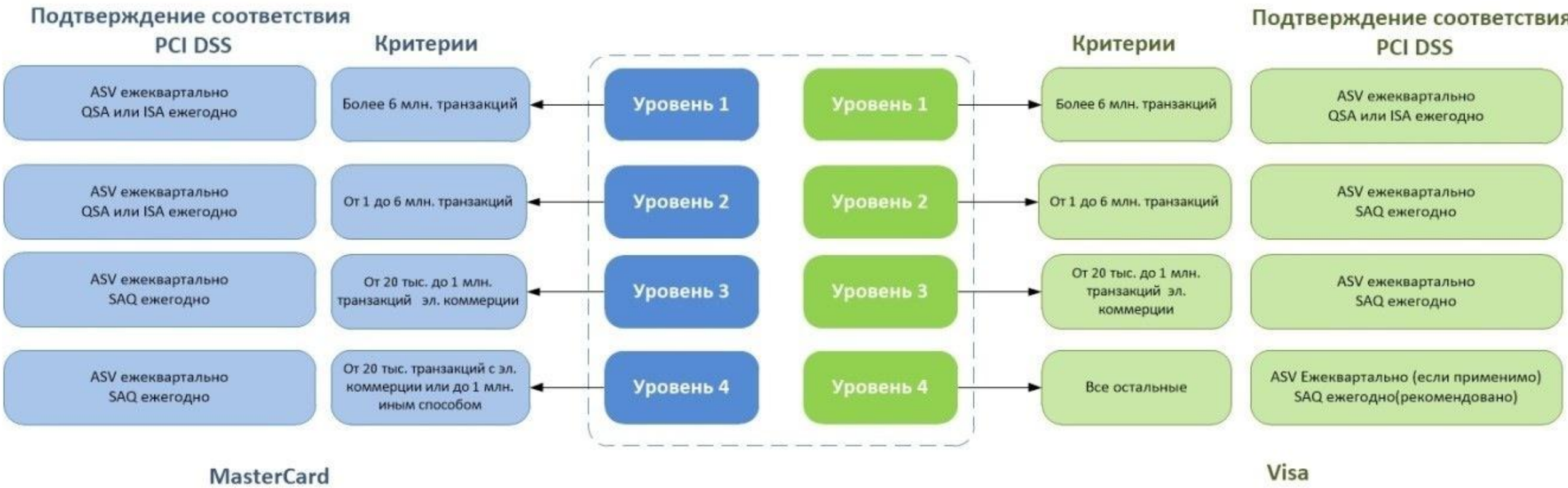
Чтобы ответить на вопрос, в какой ситуации необходимо проводить внешний аудит, а в какой – внутренний, и стоит ли это вообще делать, нужно взглянуть на тип организации и оценить количество обрабатываемых транзакций в год.

Существует классификация, согласно которой выделяют два типа организаций: торгово-сервисные предприятия и поставщики услуг.

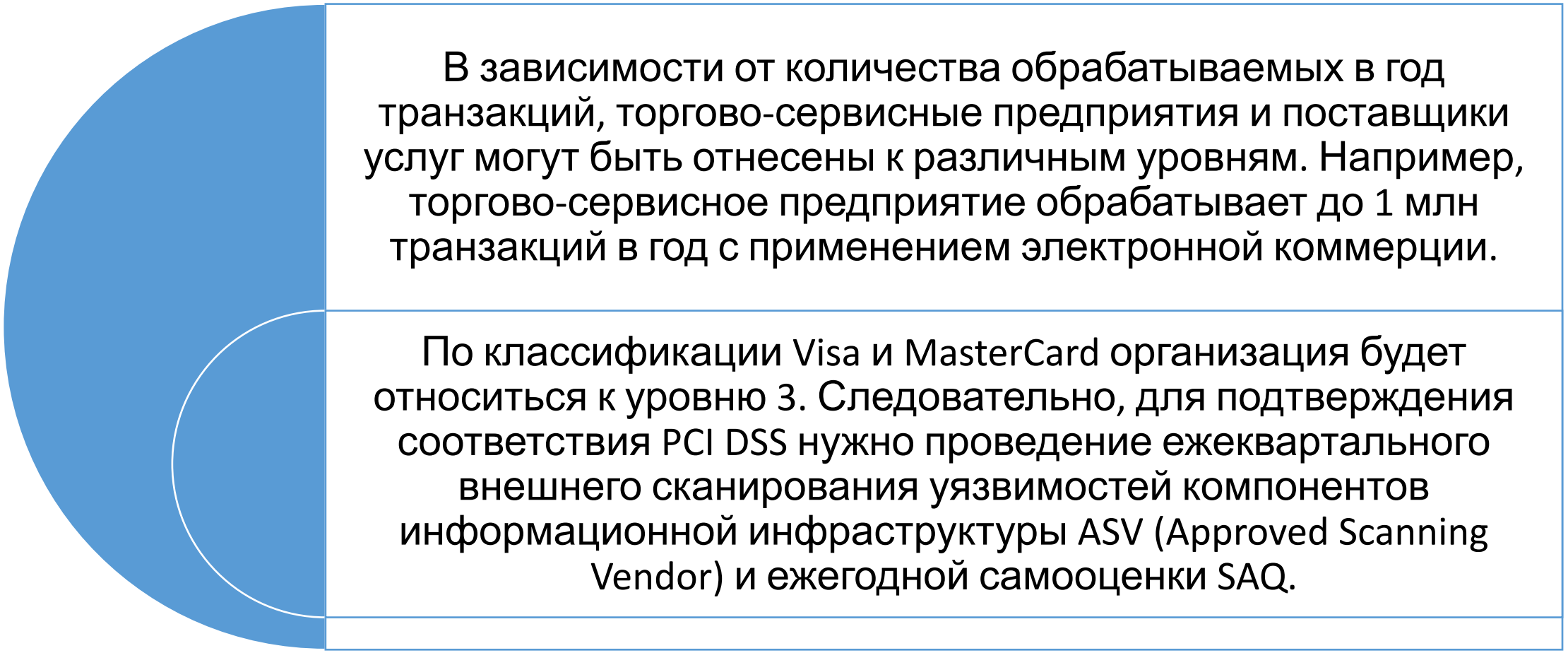
Торгово-сервисное предприятие является организацией, принимающей для оплаты товаров и услуг платежные карты (магазины, рестораны, интернет-магазины и другие).

Поставщик услуг же, в свою очередь, является организацией, оказывающей услуги в индустрии платежных карт, связанные с обработкой транзакций (это дата-центры, хостинг-провайдеры, международные платежные системы и другие).

Торгово-сервисное предприятие



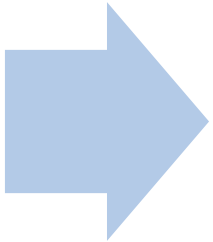
* имеется в виду транзакций в год


В зависимости от количества обрабатываемых в год транзакций, торгово-сервисные предприятия и поставщики услуг могут быть отнесены к различным уровням. Например, торгово-сервисное предприятие обрабатывает до 1 млн транзакций в год с применением электронной коммерции.
По классификации Visa и MasterCard организация будет относиться к уровню 3. Следовательно, для подтверждения соответствия PCI DSS нужно проведение ежеквартального внешнего сканирования уязвимостей компонентов информационной инфраструктуры ASV (Approved Scanning Vendor) и ежегодной самооценки SAQ.

PCI DSS-хостинг

Заключение

Как известно, аутсорсинг решает множество задач, облегчая и упрощая жизнь организациям. Если раньше многие компании разворачивали информационную инфраструктуру в собственном серверном помещении и выполняли все требования соответствия стандартам самостоятельно, то сейчас многие отдают эти задачи на откуп сертифицированным поставщикам услуг, тем самым повышая уровень защищенности среды обработки карточных данных и снижая риски финансовых потерь от возможных инцидентов информационной безопасности.



Любая организация, использующая собственный карточный процессинг, рано или поздно сталкивается с необходимостью сертификации по стандарту PCI DSS. Обращение к сертифицированным поставщикам услуг помогает существенно упростить процесс сертификации для торгово-сервисных предприятий и обеспечить защиту данных платежных карт на должном уровне

Список источников

1. Сертификация PCI DSS (ИТ-Град)

https://habr.com/company/it-grad/blog/279227/

2. PCI DSS – как и зачем получать сертификат соответствия (Pay Online)

https://geektimes.com/company/payonline/blog/130652/

Спасибо за внимание!