Приложение №4
к Договору об осуществлении расчетов с использованием банковских карт платежных систем

Требования по безопасности в отношении сети Wi-Fi

1. **Шифрование передачи данных Держателей:**

Для защиты конфиденциальных данных Держателей владельцев карточек при их передаче по открытым, общедоступным сетям должны быть использованы стойкие криптографические алгоритмы и протоколы, такие как «протокол защищенных сокетов» (Secure Sockets Layer — SSL) / «протокол безопасности на транспортном уровне» (Transport Layer Security — TLS) и «протокол безопасности Internet» (Internet Protocol Security — IPSEC);

Для беспроводных сетей, по которым передаются данные Держателей, передачи должны быть зашифрованы с помощью Wi-Fi технологии защищенного доступа WPA2, IPSEC VPN, или SSL / TLS;

Никогда не отправлять незащищенные PANs (основные учетные номера) по электронной почте.

2. **Беспроводные сети**

По причинам безопасности и доступности беспроводные сети рекомендуется использовать только в тех случаях, когда использование проводной локальной сети не представляется возможным. Поскольку беспроводные сети (например, WLAN) по своей природе обладают неконтролируемым распространением, эти сети должны быть специально защищены.

Любая используемая Предприятием беспроводная передача данных должна быть зашифрована. В беспроводных локальных сетях необходимо применять общие и специфические меры безопасности, в зависимости от предполагаемого использования WLAN.

Сеть Wi-Fi должна быть защищена обязательной авторизацией WPA2.

Размещение, мощность передачи и характеристики антенны точки доступа должны быть отрегулированы таким образом, чтобы покрыть только предназначенную область (например, торговый зал). Все беспроводные точки доступа / базовые станции должны быть подключены к сегментам DMZ (демилитаризованной зоны) корпоративной сети и должны быть зарегистрированы (по типу / модели, MAC-адресу, местонахождению).

При наличии возможности необходимо применять продукты инфраструктуры WLAN с централизованной конфигурацией и управлением, а не индивидуально настроенные точки доступа. Для обнаружения мошеннических (несанкционированных) точек доступа и других атак на инфраструктуру WLAN необходима работающая система управления WLAN, соответствующая требованиям. Идентификатор SSID должен быть изменен с настройки по умолчанию и должен быть настроен таким образом, чтобы в нем не содержалось каких-либо сведений об организации, например, названия компании, отдела, и т.д.

Трансляцию SSID необходимо отключить.

3. **Внутренние беспроводные локальные сети для гостевого использования (например, для мобильного доступа в Интернет):**

• Обеспечение легкого доступа для гостей, не целесообразно полагаться только на простую аутентификацию;
• Шифрование WLAN WPA2 (AES);
• Для доступа к VPN (виртуальная частная сеть) ресурсам компании должна быть использована технология в верхней части шифрования WLAN (например, IPSec);
• *Рекомендуется выполнить успешный вход и неудачный запрос аутентификации.*

4. **Внутренние беспроводные локальные сети с доступом к производственной среде:**

Доступ должен быть усилен строгой аутентификацией пользователя или устройства (например, на основании сертификата) с помощью центральной системы аутентификации (например, TACACS +, RADIUS, PKI).

Следует использовать шифрование WPA2 (защищенный доступ по Wi-Fi).

5. **Внешние беспроводные локальные сети с доступом к производственной среде:**

В связи с общественным доступом, к внутренней локальной сети применяются дополнительные требования:

должен быть использован стандарт 802.11i (продукты WPA2).