AMERICAN EXPRESS

Операционная политика в отношении защиты информации (DSOP)

Пиктограммы изменений

Важные обновления перечислены в Сводной таблице изменений, а также показаны в *DSOP* с помощью пиктограммы изменений. Пиктограмма изменений рядом с заголовком раздела или подраздела указывает на исправленный, добавленный или удаленный текст из раздела или подраздела. Изменения в *DSOP* обозначаются пиктограммой изменений, как показано здесь.

Сводная таблица изменений

Важные обновления перечислены в следующей таблице, а также показаны в *DSOP* с помощью пиктограммы изменений.

Раздел/подраздел	Описание изменения
Пиктограммы изменений	Добавлен язык Пиктограммы изменений.
Сводная таблица изменений	Добавлена Сводная таблица изменений.
Раздел 1, «Компрометация Данных о держателе карты»	Добавлена Программа компрометации данных о держателе карты.
Раздел 3, «Обязательства по урегулированию случаев нарушения конфиденциальности информации»	Увеличен срок уведомления о случаях нарушения конфиденциальности информации с 24 до 72 часов.
Раздел 5, «Важная периодическая валидация ваших систем»	Обновлена таблица штрафов за Непрохождение валидации. Увеличение комиссионного сбора Организации торговли (услуг) уровней 3 и 4, если Валидационная документация не будет получена к установленному сроку.

Являясь лидером в области защиты прав потребителей, компания American Express уже долгое время соблюдает принятые на себя обязательства по защите Данных о держателе карты и Конфиденциальной аутентификационной информации.

Украденная информация может нанести ущерб потребителям, Организациям торговли (услуг), Поставщикам услуг и эмитентам карт. Даже единичный случай утечки информации может серьезно испортить репутацию компании и ухудшить ее способность эффективно вести свою деятельность. Ответ на данную угрозу заключается во введении операционных политик безопасности, которые могут помочь укрепить доверие потребителей и репутацию компании, а также повысить рентабельность.

American Express знает, что наши Организации торговли (услуг) и Поставщики услуг (совместно именуемые вы) разделяют нашу обеспокоенность, и призывает **вас** в рамках ваших обязательств соблюдать положения о защите информации, предусмотренные вашими договорными отношениями по принятию [в случае Организаций торговли (услуг)] или обработке (в случае Поставщиков услуг) Карт American Express® (каждые из которых именуются **Соглашение**), и данную Операционную политику в отношении защиты информации, которую мы можем периодически дополнять. Данные требования распространяются на все ваше оборудование, системы и сети (и их компоненты), в которых хранятся, обрабатываются или передаются ключи шифрования, Данные о держателе карты или Конфиденциальная аутентификационная информация (или и то и другое).

Термины, написанные с прописной буквы, определения которых отсутствуют в данном документе, обладают значением, присвоенным им в глоссарии в конце данной политики.

Раздел 1 Компрометация Данных о держателе карты

Вы и ваши Затрагиваемые стороны должны оценивать и устранять пробелы в безопасности данных в вашей среде Данных о держателе карты (CDE) после получения уведомления от American Express о потенциальной компрометации Данных о держателе карты. Примеры компрометации Данных о держателе карты включают среди прочего следующее.

- **Обычная точка покупки (CPP):** Держатели карт American Express сообщают о мошеннических Операциях на своих карточных счетах, которые были идентифицированы и определены как совершенные в результате покупок в ваших Учреждениях.
- **Найдены данные карты:** Карта American Express и Данные о держателе карты, доступные в Интернете, связаны с Операциями в ваших Учреждениях.
- **Подозрение на вредоносное ПО:** American Express подозревает, что вы используете программное обеспечение, зараженное вредоносным кодом или уязвимое для него.

Ваши Данные о держателе карты нарушают обязательства.

- Вы должны незамедлительно проверить ваш CDE на предмет пробелов в безопасности данных и исправить все обнаруженные проблемы.
  - Вы должны поручить стороннему (-им) поставщику (-ам) провести тщательное расследование вашего CDE, если он передан на аутсорсинг.
- После получения уведомления от American Express вы должны предоставить сводку предпринятых или запланированных действий по проверке, оценке и (или) исправлению ошибок.
- Вы должны предоставить обновленные документы проверки PCI DSS в соответствии с разделом 5, «Важная периодическая валидация ваших систем», действие 3, «Заполнение Валидационной документации, которую необходимо отправить в American Express», ниже.
- Если применимо, вы должны привлечь квалифицированного Судебного следователя PCI для проверки вашего CDE, если вы или ваш (-и) сторонний (-е) поставщик (-и) не можете решить проблему компрометации Данных о держателе карты в течение разумного периода времени, определенного American Express.

American Express имеет право взимать комиссию за несоблюдение, приостанавливать платежи и (или) расторгать Соглашение, если вы не выполняете данные обязательства.

Комиссия за несоблюдение обязательств в связи с компрометацией Данных о держателе карты

Описание	Организация торговли (услуг) или Поставщик услуг уровня 1	Организация торговли (услуг) или Поставщик услуг уровня 2	Организация торговли (услуг) уровня 3 или 4
Комиссия за несоблюдение обязательств взимается, если обязательства в связи с компрометацией Данных о держателе карты не выполняются в течение 45 дней с даты уведомления.	25 000 долл. США	5000 долл. США	1000 долл. США
Комиссия за несоблюдение обязательств взимается, если обязательства в связи с компрометацией Данных о держателе карты не выполняются в течение 90 дней с даты уведомления.	35 000 долл. США	10 000 долл. США	2500 долл. США
Комиссия за несоблюдение обязательств взимается, если обязательства в связи с компрометацией Данных о держателе карты не выполняются в течение 120 дней с даты уведомления. **ПРИМЕЧАНИЕ.** *Плата за несоблюдение требований может по-прежнему взиматься ежемесячно до тех пор, пока обязательства не будут выполнены или* Компрометация Данных о держателе карты *не будет разрешена.*	45 000 долл. США	15 000 долл. США	5000 долл. США

Если ваши обязательства в связи с компрометацией Данных о держателе карты не будут выполнены в течение 120 дней с даты уведомления, American Express имеет право взимать комиссию за несоблюдение обязательств в совокупности, приостановить платежи и (или) расторгнуть Соглашение.

Раздел 2 Стандарты Защиты ключей шифрования, Данных о держателе карты и Конфиденциальной аутентификационной информации

Вы и ваши Затрагиваемые стороны должны:

- хранить Данные о держателе карты только с целью осуществления Операций по Картам American Express в соответствии с требованиями Соглашения;
- выполнять условия текущей версии Стандарта безопасности данных индустрии платежных карт и других Требований Совета по стандартам безопасности индустрии платежных карт, применимых к обработке, хранению или передаче Данных о держателе карты или Конфиденциальной аутентификационной информации не позднее даты вступления в силу данной версии применимого требования;
- при установке новых или замене существующих Устройств для ввода ПИН-кода или Платежных приложений (или и того и другого) использовать только те устройства и приложения, которые были утверждены индустрией платежных карт.

Вы должны защищать все записи об Операциях с использованием карты, а также записи об Операциях по возврату средств, сохраняемые по настоящему Соглашению, в соответствии с настоящими положениями о защите информации; вы должны использовать данные записи только с целью выполнения своих обязательств по настоящему Соглашению и защищать эти записи надлежащим образом. Вы несете финансовую и иную ответственность перед American Express за соблюдение вашими Затрагиваемыми сторонами настоящих положений о защите информации (за исключением демонстрации соблюдения вашими Затрагиваемыми сторонами настоящей политики в соответствии с разделом 5, «Важная периодическая валидация ваших систем»).

Раздел 3 Обязательства по урегулированию случаев нарушения конфиденциальности информации

Вы должны незамедлительно уведомить об инциденте American Express, но в любом случае не позднее 72 (семидесяти двух) часов с момента обнаружения Случая нарушения конфиденциальности информации.

Чтобы уведомить American Express, просим вас связаться с Программой по реагированию на инциденты на предприятии (Enterprise Incident Response Programme, *EIRP*) American Express по номеру телефона +1 (602) 537-3021 («+» означает префикс прямого набора международного номера IDD, к которому применяется международный тариф) или по электронной почте EIRP@aexp.com. Вы должны назначить контактное лицо по данному Случаю нарушения конфиденциальности информации. Кроме того, вы обязаны сделать следующее.

- Вы обязаны проводить тщательное расследование каждого Случая нарушения конфиденциальности информации.
- В случае инцидентов, в которые вовлечено более 10 000 уникальных номеров Карт, в течение пяти дней после обнаружения инцидента вы обязаны привлечь к расследованию Специального следователя индустрии платежных карт.
- Неотредактированный отчет по результатам расследования должен быть представлен компании American Express в течение 10 рабочих дней с момента его составления.
- Вы должны незамедлительно представить American Express все Взломанные номера карт. Компания American Express оставляет за собой право проводить собственный внутренний анализ для определения номеров Карт, вовлеченных в Случай нарушения конфиденциальности информации.

Отчеты по результатам расследования должны заполняться в соответствии с актуальным Шаблоном заключительного отчета о расследовании случаев нарушения конфиденциальности информации, принятым для индустрии платежных карт. Отчет Специального следователя индустрии платежных карт должен содержать экспертные заключения, отчеты о соблюдении требований и другие сведения, связанные со Случаем нарушения конфиденциальности информации; определять причину произошедшего; подтверждать соблюдение или несоблюдение требований Стандарта безопасности данных индустрии платежных карт на момент инцидента; подтверждать вашу способность предотвращать такие случаи в будущем, (1) представив план по устранению всех недостатков в отношении Стандарта безопасности данных индустрии платежных карт и (2) участвуя в программе соответствия American Express (как описано ниже). По требованию компании American Express вы обязаны представить подтверждение устранения недостатков от Квалифицированного аудитора систем безопасности.

Невзирая на предыдущие параграфы настоящего раздела 3, «Обязательства по урегулированию случаев нарушения конфиденциальности информации»:

- American Express может по своему усмотрению потребовать от вас привлечь Специального следователя индустрии платежных карт для проведения расследования Случая нарушения конфиденциальности информации, в который вовлечено менее 10 000 уникальных номеров Карт (любое такое расследование должно соответствовать требованиям, изложенным выше в разделе 3, «Обязательства по урегулированию случаев нарушения конфиденциальности информации», и должно быть завершено в сроки, установленные American Express);
- при необходимости American Express может самостоятельно привлечь Специального следователя индустрии платежных карт для проведения расследования Случая нарушения конфиденциальности информации, а также обязать вас оплатить стоимость его услуг.

Вы должны сотрудничать с American Express по вопросам устранения любых проблем, возникших в результате Случая нарушения конфиденциальности информации, в том числе консультироваться с American Express касательно ваших контактов с Держателями карт, которых затронул данный Случай нарушения конфиденциальности информации, и предоставлять (в частности, получать отказ от претензий в случае предоставления) American Express любую необходимую информацию, подтверждающую вашу способность предотвращать возникновение Случаев нарушения конфиденциальности информации в будущем, в порядке, предусмотренном Соглашением.

Невзирая на любое обязательство о конфиденциальности по Соглашению, которое говорит об обратном, American Express обладает правом разглашать информацию о любом Случае нарушения конфиденциальности информации Держателям карт American Express, эмитентам и иным участникам платежной системы American Express, а также широкой публике, как того требует применимое законодательство, судебное, административное или регулятивное распоряжение, указ, судебная повестка, запрос или иной процесс с целью уменьшения риска мошенничества или причинения иного вреда, либо совершить иные действия в той мере, насколько это необходимо для того, чтобы платежная система American Express могла функционировать.

Раздел 4 Обязательства по выплате компенсации за случаи нарушения конфиденциальности информации

Ваши обязательства по выплате компенсации в пользу компании American Express в соответствии с Соглашением о случаях нарушения конфиденциальности информации будут определены в данном разделе 4, «Обязательства по выплате компенсации за случаи нарушения конфиденциальности информации», и не будут затрагивать какие-либо другие права и средства правовой защиты American Express. В дополнение к вашим обязательствам по выплате компенсации (если таковые имеются) с вас может взиматься плата за несоблюдение требований в связи со Случаем нарушения конфиденциальности информации, как описано ниже в настоящем разделе 4, «Обязательства по выплате компенсации за случаи нарушения конфиденциальности информации».

За Случаи нарушения конфиденциальности информации, в которые вовлечено:

- более 10 000 номеров Карт American Express с чем-либо из нижеперечисленного:
  - Конфиденциальной аутентификационной информацией или
  - датой окончания срока действия,

  вы обязаны выплатить American Express компенсацию из расчета 5 долларов США за каждый номер счета.

Однако American Express не будет требовать от вас компенсации за Случаи нарушения конфиденциальности информации, в которые вовлечено:

- менее 10 000 номеров Карт American Express или
- более 10 000 номеров Карт American Express, если вы выполнили следующие условия.
  - Вы уведомили компанию American Express о Случае нарушения конфиденциальности информации в порядке, изложенном в настоящем разделе 4, «Обязательства по выплате компенсации за случаи нарушения конфиденциальности информации».
  - На момент возникновения Случая нарушения конфиденциальности данных вы соблюдали Стандарты безопасности данных индустрии платежных карт (согласно результатам расследования случая Специальным следователем индустрии платежных карт).
  - Случай нарушения конфиденциальности информации произошел не по причине вашего ненадлежащего поведения (или ваших Затрагиваемых сторон).

Невзирая на вышеизложенные параграфы настоящего раздела 4, «Обязательства по выплате компенсации за случаи нарушения конфиденциальности информации», в отношении любого Случая нарушения конфиденциальности информации, независимо от количества номеров Карт American Express, вы обязаны выплатить American Express компенсацию за несоблюдение требований и произошедший Случай нарушения конфиденциальности информации, не превышающую 100 000 долларов США за каждый отдельный случай (по усмотрению American Express), в случае невыполнения вами каких-либо обязательств, изложенных в разделе 3, «Обязательства по урегулированию случаев нарушения конфиденциальности информации». Во избежание сомнений общий размер компенсации за несоблюдение требований, установленный для любого отдельного Случая нарушения конфиденциальности информации, не должен превышать 100 000 долларов США.

Компания American Express исключит из своих расчетов любой номер счета Карты American Express, который был включен в предыдущее требование о возмещении ущерба в Случае нарушения конфиденциальности информации, предъявленное в течение двенадцати (12) месяцев до Даты уведомления. Все расчеты, сделанные American Express по этой методологии, являются окончательными.

American Express может выставить вам счет на полную сумму ваших обязательств по выплате компенсации в отношении Случаев нарушения конфиденциальности информации или вычесть эту сумму из причитающихся вам платежей American Express (или соответственно списать сумму с вашего банковского счета) в соответствии с Соглашением.

Обязательства Организации торговли (услуг) по выплате компенсации за Случаи нарушения конфиденциальности информации по настоящему Соглашению не должны рассматриваться как случайные, косвенные, спекулятивные, непрямые, специальные, штрафные или показательные убытки при условии, что такие обязательства не включают убытки, связанные с упущенной выгодой или доходом, утратой репутации или потерей деловых возможностей.

По собственному усмотрению American Express может сократить сумму обязательства по выплате компенсации для Организаций торговли (услуг) исключительно в отношении Случаев нарушения конфиденциальности информации, соответствующих каждому из следующих критериев:

- на момент возникновения и в течение всего Промежутка времени, в котором происходило нарушение конфиденциальности информации, использовались применимые Технологии снижения рисков;
- было проведено тщательное расследование в соответствии с программой Специальных следователей индустрии платежных карт (если иное не согласовано ранее в письменной форме);
- в отчете по результатам расследования четко указывается, что для обработки, хранения и (или) передачи данных во время инцидента использовались Технологии снижения рисков;
- вы не храните (и не хранили в течение всего Промежутка времени, в котором происходило нарушение конфиденциальности информации) Конфиденциальную аутентификационную информацию или другие Данные о держателе карты в читаемом формате.

Если сокращение суммы обязательства по выплате компенсации возможно (за исключением любых подлежащих уплате сборов за несоблюдение требований), оно будет определяться следующим образом.

Сокращение суммы обязательства по выплате компенсации	Необходимые требования
Стандартное сокращение: 50 %	> 75 % общего числа Операций обработано на Устройствах, позволяющих считывать чипы [1], ИЛИ
	в > 75 % торговых точек Организаций торговли (услуг) используется Технология снижения рисков [2].
Повышенное сокращение: 75–100 %	> 75 % общего числа Операций обработано на Устройствах, позволяющих считывать чипы [1], И в > 75 % торговых точек Организаций торговли (услуг) используется другая Технология снижения рисков [2].

[1] Определяется внутренним анализом American Express.

[2] Определяется согласно результатам расследования Специального следователя индустрии платежных карт.

- Повышенное сокращение (75–100 %) будет определяться на основе меньшего процента Операций с использованием Устройств, позволяющих считывать чипы, И торговых точек Организаций торговли (услуг), использующих другую Технологию снижения рисков. Приведенные далее примеры иллюстрируют расчет сокращения суммы обязательства по выплате компенсации.
- Чтобы считалось, что вы используете Технологию снижения рисков, вы должны продемонстрировать эффективное использование этой технологии в соответствии с ее схемой и назначением. Например, внедрение Устройств, позволяющих считывать чипы, и последующая обработка Карт с чипом с использованием магнитной полосы или с помощью введения пароля НЕ является эффективным использованием этой технологии.
- Процент торговых точек, использующих Технологию снижения рисков, определяется в ходе расследования Специального следователя индустрии платежных карт.
- Сокращение суммы обязательства по выплате компенсации не распространяется на компенсации за несоблюдение требований, подлежащие уплате в связи с произошедшим Случаем нарушения конфиденциальности информации.

Повышенное сокращение суммы обязательства по выплате компенсации

Пример	Используемые Технологии снижения рисков	Компенсации	Сокращение
1	80 % Операций обработано на Устройствах, позволяющих считывать чипы. 0 % торговых точек используют другую Технологию снижения рисков.	Нет	50 %: стандартное сокращение (использование Технологии снижения рисков менее чем в 75 % случаев не дает права на повышенное сокращение)[1].
2	80 % Операций обработано на Устройствах, позволяющих считывать чипы. 77 % торговых точек используют другую Технологию снижения рисков.	Да	77 %: повышенное сокращение (на основании того, что в 77 % случаев используется Технология снижения рисков).
3	93 % Операций обработано на Устройствах, позволяющих считывать чипы. 100 % торговых точек используют другую Технологию снижения рисков.	Да	93 %: повышенное сокращение (на основании того, что 93 % Операций обработано на Устройствах, позволяющих считывать чипы).
4	40 % Операций обработано на Устройствах, позволяющих считывать чипы. 90 % торговых точек используют другую Технологию снижения рисков.	Нет	50 %: стандартное сокращение (наличие менее 75 % Операций, обработанных на Устройствах, позволяющих считывать чипы, не дает права на повышенное сокращение).

[1] Случай нарушения конфиденциальности информации, связанный с 10 000 Карт American Express, из расчета по 5 долларов США за каждый номер счета (10 000 x 5 = 50 000 долларов США), может подпадать под сокращение на 50 %, что уменьшает сумму обязательств по выплате компенсации с 50 000 до 25 000 долларов США, не учитывая компенсации за несоблюдение требований.

Раздел 5 Важная периодическая валидация ваших систем

Вы обязаны предпринять следующие действия для проведения ежегодной и квартальной валидации состояния вашего (и ваших Получателей франшизы) оборудования, систем и (или) сетей (и их компонентов), посредством которых производится обработка, передача и хранение Данных о держателе карты или Конфиденциальной аутентификационной информации, в соответствии со Стандартом безопасности данных индустрии платежных карт в установленном ниже порядке.

Предусмотрено четыре действия для проведения валидации.

Действие 1. Участие в программе соответствия American Express, предусмотренной настоящей политикой.

Действие 2. Определение вашего Уровня и Требований к валидации.

Действие 3. Заполнение Валидационной документации, которую необходимо отправить в American Express.

Действие 4. Отправка Валидационной документации в American Express в течение установленного срока.

Действие 1. Участие в программе соответствия American Express, предусмотренной настоящей политикой

Организации торговли (услуг) уровней 1 и 2, а также все Поставщики услуг, как описано далее, должны участвовать в Программе соответствия American Express, предусмотренной настоящей политикой, предоставляя свое полное имя (наименование), адрес электронной почты, номер телефона и фактический почтовый адрес человека, который является контактным лицом по вопросам данных. Вы обязаны предоставить эту информацию в SecureTrust, подразделение компании Trustwave (https://portal.securetrust.com), которая управляет Программой от имени компании American Express, одним из способов, указанных в действии 4, «Отправка Валидационной документации в American Express», ниже. При необходимости вы обязаны уведомить SecureTrust в случае изменения такой информации, предоставив обновленную информацию. Если вы не предоставите такую контактную информацию, это не затронет наши права на начисление штрафа за непрохождение валидации, как указано в таблице штрафов за непрохождение валидации.

Компания American Express по собственному усмотрению может потребовать от определенных Организаций торговли (услуг) уровней 3 и 4 принять участие в Программе соответствия American Express, предусмотренной настоящей Политикой, направив им письменное уведомление. Указанная Организация торговли (услуг) должна зарегистрироваться в Программе не позднее 90 дней с момента получения уведомления.

Действие 2. Определение вашего уровня и требований к валидации

Существует четыре уровня для Организаций торговли (услуг) и два уровня для Поставщиков услуг, которые определяются исходя из количества Операций с использованием Карт American Express. Для Организаций торговли (услуг) это количество, представленное их предприятиями, которые могут достигать максимального уровня American Express для таких организаций *. Вы попадете под критерии одного из уровней, указанных в таблицах для Организаций торговли (услуг) и Поставщиков услуг ниже. Платежи, инициированные покупателем, не включаются в количество Операций с Картами American Express для определения уровня Организации торговли (услуг) и требований к валидации.

* В случае с Компаниями, предоставляющими право франшизы, также должно учитываться количество Операций Получателей франшизы. Компании, предоставляющие право франшизы, которые обязывают Получателей своей франшизы использовать определенную Систему торговой точки или обращаться к определенному Поставщику услуг, также должны предоставлять Валидационную документацию на соответствующих Получателей франшизы.

Требования к Организации торговли (услуг)

Для Организаций торговли (услуг) (не Поставщиков услуг) существует четыре классификации их уровней и требований к валидации. После определения уровня Организации торговли (услуг) из приведенного далее списка см. таблицу классификации Организаций торговли (услуг) для определения требований к Валидационной документации.

- **Организация торговли (услуг) уровня 1** — организация, достигшая 2,5 миллиона Операций с использованием Карт American Express или более в год, или какая-либо Организация торговли (услуг), которую компания American Express по собственному усмотрению приравнивает к уровню 1.
- **Организация торговли (услуг) уровня 2** — организация, достигшая от 50 000 до 2,5 миллиона Операций с использованием Карт American Express в год.
- **Организация торговли (услуг) уровня 3** — организация, достигшая от 10 000 до 50 000 Операций с использованием Карт American Express в год.
- **Организация торговли (услуг) уровня 4** — организация, достигшая менее 10 000 Операций с использованием Карт American Express в год.

Таблица классификации Организаций торговли (услуг)

	Валидационная документация		
Уровень организации/ количество Операций с использованием карт American Express в год	Внутренний экспертный отчет о соответствии	Анкета самооценки И Ежеквартальная проверка сети	Аттестация соответствующих критериям Организаций торговли (услуг) по программе STEP
Уровень 1/ 2,5 миллиона или более	Обязательно	Неприменимо.	Необязательно (заменяет отчет о соответствии).
Уровень 2/ от 50 000 до 2,5 миллиона	Необязательно	Анкета самооценки обязательна (за исключением случаев подачи внутреннего экспертного отчета). С определенными типами Анкет самооценки проверка обязательна.	Необязательно (заменяет Анкету самооценки и проверку сети или отчет о соответствии).
Уровень 3/ от 10 000 до 50 000	Необязательно	Анкета самооценки необязательна (обязательна в случае запроса от American Express). С определенными типами Анкет самооценки проверка обязательна.	Необязательно (заменяет Анкету самооценки и проверку сети или отчет о соответствии).
Уровень 4/ менее 10 000	Необязательно	Анкета самооценки необязательна (обязательна в случае запроса от American Express). С определенными типами Анкет самооценки проверка обязательна.	Необязательно (заменяет Анкету самооценки и проверку сети или отчет о соответствии).

* Во избежание двусмысленного толкования Организации торговли (услуг) уровней 3 и 4 не обязаны предоставлять Валидационную документацию, за исключением случаев, когда этого требует компания American Express. Тем не менее на них распространяются все другие положения об ответственности, предусмотренные настоящей Операционной политикой в отношении защиты информации.

American Express может проверить точность и соответствие предоставленной по запросу валидационной документации индустрии платежных карт, в частности посредством привлечения за свой счет Квалифицированного аудитора систем безопасности или Специального следователя индустрии платежных карт, выбранного компанией American Express.

Программа улучшения технологий безопасности (Security Technology Enhancement Programme, STEP)

Организации торговли (услуг), соответствующие стандартам безопасности данных индустрии платежных карт, по усмотрению компании American Express могут участвовать в ее программе STEP в случае, если они внедряют в своих средах обработки Карт определенные дополнительные технологии безопасности. Программа STEP применяется только в том случае, если Организация торговли (услуг) не была вовлечена в Случаи нарушения конфиденциальности информации в течение предыдущих 12 месяцев и если 75 % всех Операций с использованием Карт выполняются с применением следующих технологий.

- **EMV** — на активном Устройстве, позволяющем считывать чип, имеющем действующее одобрение и сертификацию EMVCo (www.emvco.com) и способном обрабатывать Операции с Картами с чипом, совместимыми с AEIPS. [Организации торговли (услуг) из США также должны иметь возможность бесконтактной обработки Операций.]
- **Межабонентское шифрование (P2PE)** — связь с операционным центром Организации торговли (услуг) с использованием системы межабонентского шифрования, одобренной Советом по стандартам безопасности индустрии платежных карт или Квалифицированным аудитором систем безопасности.

Для Организаций торговли (услуг), имеющих право на участие в Программе улучшения технологий безопасности, требования к Валидационной документации индустрии платежных карт были снижены, что более подробно описано в действии 3, «Заполнение Валидационной документации, которую необходимо отправить в American Express», ниже.

Требования к Поставщику услуг

Для Поставщиков услуг [не Организаций торговли (услуг)] существует две классификации их уровней и требований к валидации. После присвоения Поставщику услуг уровня из перечисленного ниже списка см. таблицу классификации Поставщиков услуг для определения требований к Валидационной документации.

Поставщик услуг уровня 1 — поставщик, достигший 2,5 миллиона Операций с использованием Карт American Express или более в год, или какой-либо Поставщик услуг, которого компания American Express приравнивает к уровню 1.

Поставщик услуг уровня 2 — поставщик, достигший менее 2,5 миллиона Операций с использованием Карт American Express в год, или какой-либо Поставщик услуг, которого компания American Express не приравнивает к уровню 1.

Поставщики услуг не имеют права на участие в программе STEP.

Таблица классификации Поставщиков услуг

Уровень	Валидационная документация	Характер требований
1	Ежегодный отчет об оценке соответствия требованиям внутренней системы безопасности.	Обязательно
2	Ежегодная анкета самооценки D (Поставщик услуг) и Ежеквартальная проверка сети или Ежегодный отчет об оценке внутренней безопасности (по желанию).	Обязательно

Рекомендуется, чтобы Поставщики услуг также соответствовали требованиям дополнительной валидации определенных предприятий индустрии платежных карт.

Действие 3. Заполнение Валидационной документации, которую необходимо отправить в American Express

Ниже приведены документы, необходимые для Организаций торговли (услуг) и Поставщиков услуг различных уровней, перечисленных в таблице классификации Организаций торговли (услуг) и таблице классификации Поставщиков услуг выше.

Ежегодная оценка внутренней системы безопасности. Представляет собой детальную внутреннюю проверку вашего оборудования, системы и сетей (и их компонентов), посредством которых производится обработка, передача и хранение Данных о держателе карты или Конфиденциальной аутентификационной информации. Проверку должны проводить:

- Квалифицированный аудитор систем безопасности или
- вы и уполномоченный вами исполнительный директор, финансовый директор, директор по информационной безопасности или руководитель, а ее результаты должны ежегодно передаваться компании American Express в соответствующем Свидетельстве о соответствии требованиям.

Свидетельство о соответствии требованиям должно подтвердить соблюдение всех требований Стандарта безопасности данных индустрии платежных карт, и (по запросу) в него необходимо включить копии полного отчета о соответствии требованиям [для Организаций торговли (услуг) уровня 1 и Поставщиков услуг уровня 1].

Ежегодная анкета самооценки. Ежегодная самооценка представляет собой процесс, основанный на заполнении Анкеты самооценки, разработанной согласно Стандарту безопасности данных индустрии платежных карт, которая позволяет произвести самостоятельную оценку своего оборудования, системы и сетей (и их компонентов), посредством которых производится обработка, передача и хранение Данных о держателе карты или Конфиденциальной аутентификационной информации (или и того и другого). Такую оценку должны проводить вы и уполномоченный вами исполнительный директор, финансовый директор, директор по информационной безопасности или руководитель. Раздел Анкеты самооценки Свидетельства о соответствии требованиям должен ежегодного передаваться компании American Express. Этот раздел должен подтверждать соблюдение вами всех требований Стандарта безопасности данных индустрии платежных карт. По запросу в него включаются все копии Анкеты самооценки [для Организаций торговли (услуг) уровней 2, 3 и 4, а также для Поставщиков услуг уровня 2].

Ежеквартальная проверка сети. Представляет собой процесс удаленной проверки ваших подключенных к Интернету компьютеров и веб-серверов на наличие потенциальных слабых и незащищенных мест. Такую проверку должен проводить Утвержденный поставщик услуг сканирования. Вы обязаны ежеквартально подготавливать и предоставлять компании American Express Свидетельство о соответствии сканирования требованиям, подготовленное Утвержденным поставщиком услуг сканирования, либо краткое изложение результатов сканирования (по запросу также прилагаются копии полного сканирования). Свидетельство о соответствии сканирования требованиям или краткий отчет должны подтвердить соответствие результатов сканирования процедурам сканирования, предусмотренным Стандартом безопасности данных индустрии платежных карт, и отсутствие выявленных высоких рисков [для всех Организаций торговли (услуг), за исключением подающих Отчет об оценке внутренней системы безопасности и имеющих право на участие в Программе улучшения технологий безопасности, а также всех Поставщиков услуг]. Во избежание двусмысленного толкования Ежеквартальные проверки сети являются обязательными, если они требуются в соответствии с Анкетой самооценки.

Валидационная документация к ежегодной оценке по Программе улучшения технологий безопасности. Ежегодная квалификационная оценка по Программе улучшения технологий безопасности (далее — «Оценка STEP») доступна только для тех Организаций торговли (услуг), которые соответствуют критериям, перечисленным в действии 2, «Определение вашего уровня и требований к валидации», выше. Оценка STEP представляет собой процесс, основанный на требованиях Стандарта безопасности данных индустрии платежных карт, который позволяет произвести самостоятельную оценку своего оборудования, систем и сетей (и их компонентов), посредством которых производится обработка, передача и хранение Данных о держателе карты или Конфиденциальной аутентификационной информации (или и того и другого). Такую оценку должны проводить вы и уполномоченный вами исполнительный директор, финансовый директор, директор по информационной безопасности или руководитель. Процесс должен завершаться ежегодной подачей формы оценки STEP в компанию American Express [только для Организаций торговли (услуг), имеющих право на участие в программе STEP]. Форма для ежегодной оценки по Программе улучшения технологий безопасности доступна для загрузки на защищенном портале SecureTrust.

Несоблюдение требований Стандарта безопасности данных индустрии платежных карт. Если вы не соблюдаете требования Стандарта безопасности данных индустрии платежных карт, вы должны подать один из указанных ниже документов.

- Свидетельство о соответствии требованиям, в том числе «Часть 4. План действий по устранению несоответствий требованиям».
- Отчет об инструменте приоритетного подхода и Свидетельство о соответствии требованиям индустрии платежных карт (Prioritised Approach Tool Summary and Attestation of Compliance, PASAOC).
- Шаблон проектного плана (доступен для загрузки на защищенном портале SecureTrust).

В каждом из перечисленных выше документов должна быть назначена дата урегулирования вопроса, которая не должна быть позже 12 месяцев с даты заполнения документа, что является условием соответствия требованиям. Вы обязаны представить соответствующий документ компании American Express одним из способов, указанных в действии 4, «Отправка Валидационной документации в American Express», ниже. Вы обязаны предоставлять компании American Express периодические обновления информации по устранению несоответствий требованиям [для Организаций торговли (услуг) уровней 1, 2, 3 и 4, а также для всех Поставщиков услуг]. Во избежание двусмысленного толкования Организации торговли (услуг), не соответствующие Стандартам безопасности данных индустрии платежных карт, не имеют права на участие в STEP. Компания American Express не будет взимать с вас

штрафы за непрохождение валидации (предусмотренные ниже) до даты урегулирования вопроса, но при этом за вами сохраняется ответственность перед American Express за исполнение всех обязательств по выплате компенсаций за Случаи нарушения конфиденциальности информации и на вас распространяются другие положения настоящей политики.

Действие 4. Отправка Валидационной документации в American Express

Все Организации торговли (услуг) и Поставщики услуг, которые должны участвовать в Программе соответствия American Express, обязаны предоставить Валидационную документацию, обозначенную как «Обязательная» в таблицах, приведенных в действии 2, «Определение вашего уровня и требований к валидации». Вы обязаны представить свою Валидационную документацию в SecureTrust одним из следующих способов.

- **Защищенный портал**. Валидационная документация может быть загружена через защищенный портал SecureTrust по адресу https://portal.securetrust.com.

  Вы можете связаться с SecureTrust по номеру телефона для вашей страны либо по электронной почте americanexpresscompliance@securetrust.com, чтобы получить консультацию об использовании данного портала.
- **Безопасный факс**. Валидационная документация может быть отправлена по факсу на номер +1 (312) 276-4019 («+» означает префикс прямого набора международного номера IDD, к которому применяется международный тариф).

  Просим указать ваше имя (наименование), торговое название, имя вашего контактного лица по вопросам защиты данных, ваш адрес и телефон, а также [только для Организаций торговли (услуг)] 10-значный номер, присвоенный вам компанией American Express.

Если у вас есть общие вопросы о Программе или указанном выше процессе, свяжитесь с SecureTrust по номеру +800 9000 1140 или +1 (312) 267-3208 либо по электронной почте americanexpresscompliance@securetrust.com.

Проверка на соответствие требованиям и валидация проводятся за ваш счет. Отправляя Валидационную документацию, вы заявляете и гарантируете компании American Express, что вы уполномочены раскрывать информацию, содержащуюся в таких документах, и предоставляете Валидационную документацию компании American Express, не нарушая права третьих лиц.

Рынки	Номер телефона SecureTrust
IDC	+888 900 0114
Австралия	+800 9000 1140
Австрия	+800 9000 1140
Аргентина	+800 9000 1140
Болгария	+312 267 3208
Великобритания	+800 9000 1140
Венгрия	+800 9000 1140
Германия	+800 9000 1140
Гонконг	+800 9000 1140
Греция	+312 267 3208
Дания	+800 9000 1140
Индия	+800 9000 1140
Ирландия	+800 9000 1140

Рынки	Номер телефона SecureTrust
Исландия	+800 9000 1140
Испания	+800 9000 1140
Италия	+800 9000 1140
Канада	1 866 659 9016
Кипр	+800 9000 1140
Латвия	+312 267 3208
Литва	+312 267 3208
Мальта	+312 267 3208
Мексика	+888 900 0114
Нидерланды	+312 267 3208
Новая Зеландия	+800 9000 1140
Норвегия	+800 9000 1140
Польша	+800 9000 1140
Португалия	+312 267 3208
Россия	+312 267 3208
Румыния	+312 267 3208
Сингапур	+800 9000 1140
Словакия	+312 267 3208
Словения	+312 267 3208
США	1 866 659 9016
Таиланд	+800 9000 1140
Тайвань	+312 267 3208
Франция	+800 9000 1140
Хорватия	+312 267 3208
Чешская Республика	+800 144 316
Швеция	+800 9000 1140
Эстония	+312 267 3208
Япония	+312 267 3208

«+» означает префикс прямого набора международного номера IDD, к которому применяется международный тариф.

Штрафы за непрохождение валидации и расторжение соглашения

Компания American Express имеет право наложить на вас штраф за непрохождение валидации и расторгнуть настоящее Соглашение в случае неисполнения вами настоящих требований или непредоставления вами обязательной Валидационной документации в установленные сроки. Компания American Express отдельно проинформирует вас о применимых сроках каждого ежегодного и квартального отчетного периода.

Отправьте документацию в American Express в установленные сроки. Компания American Express отдельно проинформирует вас о применимых сроках каждого ежегодного и квартального отчетного периода.

Таблица штрафов за непрохождение валидации

Описание *	Организация торговли (услуг) или Поставщик услуг уровня 1	Организация торговли (услуг) или Поставщик услуг уровня 2 либо Организация торговли (услуг)	Организация торговли (услуг) уровня 3 или 4
Штраф за непрохождение валидации будет начислен в случае, если Валидационная документация не получена к первому сроку подачи.	25 000 долл. США	5000 долл. США	50 долл. США
Дополнительный штраф за непрохождение валидации будет начислен в случае, если Валидационная документация не будет получена в течение 60 дней после окончания первого срока подачи.	35 000 долл. США	10 000 долл. США	100 долл. США
Дополнительный штраф за непрохождение валидации будет начислен в случае, если Валидационная документация не будет получена в течение 90 дней после окончания первого срока подачи, и каждые 30 дней после этого.	45 000 долл. США	15 000 долл. США	250 долл. США

* Штрафы за непрохождение валидации будут оцениваться в эквиваленте местной валюты.

** Неприменимо в Аргентине.

Если компания American Express не получает вашей обязательной Валидационной документации в течение 90 дней с момента истечения первого срока подачи, она вправе расторгнуть настоящее Соглашение в установленном порядке, а также взыскать с вас совокупность вышеуказанных штрафов за непрохождение валидации.

Раздел 6 Конфиденциальность

Компания American Express обязана принять обоснованные меры для защиты конфиденциальности ваших отчетов о соответствии требованиями, в том числе Валидационной документации (и обязана обеспечить осуществление таких мер со стороны своих агентов и субподрядчиков, включая SecureTrust), а также не имеет права раскрывать Валидационную документацию каким-либо третьим лицам (за исключением собственных Аффилированных лиц, агентов, представителей, Поставщиков услуг и субподрядчиков) в течение трех лет с момента ее получения. При этом такое обязательство по сохранению конфиденциальности не применяется к Валидационной документации, которая:

а) уже была известна компании American Express до ее раскрытия;

б) является или становится общедоступной без нарушения настоящего абзаца компанией American Express;

в) на законных основаниях получена компанией American Express от третьих лиц без обязательства сохранения конфиденциальности;

г) самостоятельно разработана компанией American Express;

д) должна быть раскрыта на основании постановления суда, административного ведомства или правительственного органа либо на основании закона, предписания, распоряжения, повестки в суд, запроса документов и других административно-правовых процессов либо на основании официального или неофициального запроса или расследования, проводимого правительственным органом либо ведомством (в том числе чиновником, инспектором, экспертом или правоохранительным органом).

Раздел 7 Оговорка об ограничении ответственности

КОМПАНИЯ AMERICAN EXPRESS НАСТОЯЩИМ ОТКАЗЫВАЕТСЯ ОТ ЛЮБЫХ ЗАВЕРЕНИЙ, ГАРАНТИЙ И ОБЯЗАТЕЛЬСТВ В ОТНОШЕНИИ НАСТОЯЩЕЙ ОПЕРАЦИОННОЙ ПОЛИТИКИ ОТНОСИТЕЛЬНО ЗАЩИТЫ ИНФОРМАЦИИ, СТАНДАРТА БЕЗОПАСНОСТИ ДАННЫХ ИНДУСТРИИ ПЛАТЕЖНЫХ КАРТ, СПЕЦИФИКАЦИЙ EMV, НАЗНАЧЕНИЯ И ДЕЯТЕЛЬНОСТИ КВАЛИФИЦИРОВАННЫХ АУДИТОРОВ СИСТЕМ БЕЗОПАСНОСТИ, УТВЕРЖДЕННЫХ ПОСТАВЩИКОВ УСЛУГ СКАНИРОВАНИЯ ИЛИ СПЕЦИАЛЬНЫХ СЛЕДОВАТЕЛЕЙ ИНДУСТРИИ ПЛАТЕЖНЫХ КАРТ, НЕЗАВИСИМО ОТ ТОГО, ЯВЛЯЮТСЯ ЛИ ОНИ ВЫРАЖЕННЫМИ В ПРЯМОЙ ФОРМЕ, ПОДРАЗУМЕВАЕМЫМИ, ПРЕДУСМОТРЕННЫМИ ПО ЗАКОНУ ИЛИ ИНЫМ ОБРАЗОМ, ВКЛЮЧАЯ ГАРАНТИИ ТОВАРНОГО СОСТОЯНИЯ ИЛИ ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ. ЭМИТЕНТЫ КАРТ AMERICAN EXPRESS НЕ ЯВЛЯЮТСЯ СТОРОННИМИ БЕНЕФИЦИАРАМИ СОГЛАСНО НАСТОЯЩЕЙ ПОЛИТИКЕ.

Полезные веб-сайты

Безопасность данных компании American Express: www.americanexpress.com/datasecurity

Компания PCI Security Standards Council, LLC: www.pcisecuritystandards.org

Глоссарий

Только в целях настоящей Операционной политики в отношении защиты информации (DSOP) используются следующие определения, которые имеют преимущественную силу в случае противоречия с терминами, содержащимися в *Внутренний устав Организаций торговли (услуг)*.

Анкета самооценки — инструмент самооценки, созданный компанией PCI Security Standards Council, LLC с целью оценки и проверки соблюдения требований Стандарта безопасности данных индустрии платежных карт.

Валидационная документация — Свидетельство о соответствии требованиям, предоставленное в связи с Ежегодной внутренней проверкой систем безопасности, или Анкета самооценки, Свидетельство о соответствии сканирования требованиям и краткие изложения результатов, переданных относительно Квартальных проверок Сети или Ежегодной аттестации EMV.

Взломанный номер карты — номер карточного счета American Express, связанный со Случаем нарушения конфиденциальности информации.

Данные о держателе карты — имеет значение, установленное текущим Глоссарием Стандарта безопасности данных индустрии платежных карт.

Дата уведомления — дата, когда American Express предоставляет эмитентам окончательное уведомление о Случае нарушения конфиденциальности информации. Эта дата зависит от получения компанией American Express заключительного отчета о расследовании или результатов внутреннего анализа и определяется по усмотрению American Express.

Держатель карты — любое лицо или организация, (1) которые заключили соглашение об открытии карточного счета с эмитентом, или (2) чье имя или название обозначено на Карте.

Затрагиваемые стороны — кто-либо из ваших работников, агентов, представителей, субподрядчиков, Поставщиков услуг, поставщиков оборудования или все, какие-либо или все Операционные центры, системы или решения для обработки платежей для вашей торговой точки, а также Организации торговли (услуг) в компании American Express и другие стороны, которым вы можете передать доступ к Информации о держателе карты в соответствии с настоящим Соглашением.

Информация о держателе карты — информация о Держателе карты American Express и об Операциях, совершаемых с использованием карты, включая имена, адреса, номера карточного счета и идентификационные номера карты.

Карта American Express (или **Карта)** — любая карта, устройство доступа к счету или платежное средство, имеющие наименование, логотип, торговую марку, знаки обслуживания, торговое наименование или другую фирменную разработку или указание компании American Express или ее аффилированных лиц и выпущенные эмитентом, или номер карточного счета.

Карта с чипом — карта с чипом, которая в качестве подтверждения личности Держателя карты может запросить введение ПИН-кода либо информации, содержащейся на чипе (иногда в наших материалах называется «смарт-карта», «карта EMV» или «микропроцессорная карта»).

Квалифицированный аудитор систем безопасности — юридическое лицо, аттестованное компанией PCI Security Standards Council, LLC для проведения проверки соблюдения требований Стандарта безопасности данных индустрии платежных карт.

Ключ шифрования (ключ шифрования American Express) — все ключи, используемые при обработке, создании, загрузке и (или) защите данных счетов. Это включает, помимо прочего, следующее.

- Ключи шифрования других ключей: первичные ключи зон (Zone Master Key, ZMK) и PIN-ключи зон (Zone Pin Key, ZPK).
- Ключи, используемые в защищенных криптографических устройствах: ключи верхнего уровня (Local Master Key, LMK).
- Ключи кодов безопасности карт (Card Security Code Key, CSCK).
- PIN-ключи: базовые ключи деривации (Base Derivation Key, BDK), ключ шифрования PIN (PIN Encryption Key, PEK) и PIN-ключи зон.

Компания, предоставляющая право франшизы — организация, которая предоставляет право физическим или юридическим лицам (Получателям франшизы) распространять товары и (или) услуги и осуществлять деятельность под торговым знаком своей организации. Она оказывает Получателю франшизы содействие в ведении деятельности или влияет на методы его работы, а также требует оплаты соответствующих взносов.

Конфиденциальная аутентификационная информация — имеет значение, установленное действующим Глоссарием Стандарта безопасности данных индустрии платежных карт.

Межабонентское шифрование (P2PE) — решение, которое осуществляет криптографическую защиту данных счета от точки, где Организация торговли (услуг) принимает платежную карту, до безопасной точки дешифрования.

Номер карты — уникальный идентификационный номер, который Эмитент присваивает Карте при ее выпуске.

Операционный центр — поставщик услуг для Организации торговли (услуг), который обеспечивает проведение авторизации и передачи данных, обрабатываемых сетью компании American Express.

Операция — Операция с использованием карты или Операция по возврату средств, совершаемая с использованием карты.

Операция по возврату средств — означает, что вы возвращаете Держателям карт определенную сумму за покупки или платежи, совершенные с помощью Карты.

Операция EMV — операция с микропроцессорной картой (иногда называемой «карта с интегральной микросхемой», «карта с чипом», «смарт-карта» или «карта EMV»), проводимая на терминале с поддержкой считывания карт с интегральными микросхемами торговой точки с действующим и текущим утверждением типа EMV. Утверждения типа EMV доступны по адресу www.emvco.com.

Операция с использованием карты — платеж или покупка, оплаченная с помощью Карты.

Организация торговли (услуг) — организация и все ее аффилированные лица, которые принимают Карты American Express в соответствии с Соглашением с компанией American Express или ее аффилированными лицами.

Организация торговли (услуг) уровня 1 — организация, достигшая 2,5 миллиона Операций с использованием Карт American Express или более в год, или какая-либо Организация торговли (услуг), которую компания American Express приравнивает к уровню 1.

Организация торговли (услуг) уровня 2 — организация, достигшая от 50 000 до 2,5 миллиона Операций с использованием Карт American Express в год.

Организация торговли (услуг) уровня 3 — организация, достигшая от 10 000 до 50 000 Операций с использованием Карт American Express в год.

Организация торговли (услуг) уровня 4 — организация, достигшая менее 10 000 Операций с использованием Карт American Express в год.

PCI DSS доступен по адресу www.pcisecuritystandards.org.

Платеж, инициированный покупателем — платежная Операция, доступная через файл платежных инструкций, оформленный BIP.

Платежное приложение — термин имеет значение, указанное в действующем на данный момент Глоссарии Стандарта безопасности данных платежных приложений индустрии платежных карт, который доступен по адресу www.pcisecuritystandards.org.

Получатель франшизы — независимая и управляемая третья сторона (включая получателя франшизы, лицензиата или отделение), кроме Аффилированного лица, которая имеет лицензию от Компании, предоставляющей право франшизы, на управление франшизой и которая заключила письменное соглашение с Компанией, предоставляющей право франшизы, в соответствии с которым она постоянно отображает внешнюю идентификацию себя со Знаками Компании, предоставляющей право франшизы, или позиционирует себя для общественности как член группы Компаний, предоставляющих право франшизы.

Поставщики услуг — уполномоченные операционные центры, привлеченные операционные центры, операционные центры межсетевого обмена данными и другие поставщики Организации торговли (услуг) оборудования, программного обеспечения, систем или иных платежных продуктов или услуг, используемых в торговой точке.

Поставщик услуг уровня 1 — поставщик, достигший 2,5 миллиона Операций с использованием Карт American Express или более в год, или какой-либо Поставщик услуг, которого компания American Express приравнивает к уровню 1.

Поставщик услуг уровня 2 — поставщик, достигший менее 2,5 миллиона Операций с использованием Карт American Express в год, или какой-либо Поставщик услуг, которого компания American Express не приравнивает к уровню 1.

Программа улучшения технологий безопасности (Security Technology Enhancement Programme, STEP) — программа компании American Express, в рамках которой Организациям торговли (услуг) предлагается внедрять технологии, повышающие безопасность данных. Чтобы иметь право на участие в программе STEP, в Организации торговли (услуг) не должны происходить Случаи нарушения конфиденциальности информации в течение 12 месяцев до подачи Ежегодной оценки по программе улучшения технологий безопасности, а также не менее 75 % всех их Операций должны проводиться с использованием Межабонентского шифрования или в виде Операций в реальном режиме с использованием Устройств, позволяющих считывать чипы, с поддержкой EMV.

Промежуток времени, в котором происходило нарушение конфиденциальности информации — период, который начинается с даты нарушения конфиденциальности, если она известна, или за 365 дней до Даты уведомления, если фактическая дата нарушения конфиденциальности неизвестна. Промежуток времени, в котором происходило нарушение конфиденциальности информации, заканчивается через 30 дней после Даты уведомления.

Свидетельство о соответствии сканирования требованиям — заявление о соблюдении вами требований Стандарта безопасности данных индустрии платежных карт, основанное на сканировании сети, в форме, установленной компанией Payment Card Industry Security Standards Council, LLC.

Свидетельство о соответствии требованиям — заявление о соблюдении требований Стандарта безопасности данных индустрии платежных карт в форме, установленной компанией Payment Card Industry Security Standards Council, LLC.

Система торговой точки — система или оборудование обработки информации, включая терминал, персональный компьютер, электронный кассовый аппарат, бесконтактный считыватель, платежное устройство или процесс, используемый Организацией торговли для получения авторизации, сбора данных об Операции или и того и другого.

Случай нарушения конфиденциальности информации — инцидент, связанный с раскрытием или предполагаемым раскрытием ключей шифрования American Express либо хотя бы одного номера карточного счета American Express и имеющий один из следующих признаков или несколько.

- Несанкционированный доступ или использование Ключей шифрования, Данных о держателе карты или Конфиденциальной аутентификационной информации (или их комбинации), которые хранятся, обрабатываются или передаются с помощью вашего оборудования, систем и (или) сетей (или их компонентов) либо использование которых вы разрешаете.
- Использование таких Ключей шифрования, Данных о держателе карты или Конфиденциальной аутентификационной информации (или их комбинации) не в соответствии с Соглашением.
- Подозрение или подтверждение потери, кражи либо незаконного присвоения с помощью любых средств, материалов, записей или информации, содержащих такие Ключи шифрования, Данные о держателе карты или Конфиденциальную аутентификационную информацию (или их комбинации).

Специальный следователь индустрии платежных карт — юридическое лицо, которое было одобрено компанией Payment Card Industry Security Standards Council, LLC для проведения расследования нарушения конфиденциальности или рассекречивания Данных платежных карт.

Спецификации EMV — спецификации, выпущенные EMVCo, LLC, которые доступны по адресу www.emvco.com.

Стандарт безопасности данных индустрии платежных карт — Стандарт безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard, PCI DSS), который доступен по адресу www.pcisecuritystandards.org.

Технология снижения рисков — технологические решения, которые повышают безопасность Данных о держателе карты American Express и Конфиденциальной аутентификационной информации, как это определено компанией American Express. Чтобы считалось, что вы используете Технологию снижения рисков, вы должны продемонстрировать эффективное использование этой технологии в соответствии с ее схемой и назначением. Например: EMV, Межабонентское шифрование и токенизация.

Требования индустрии платежных карт к безопасности ПИН-кодов доступны по адресу www.pcisecuritystandards.org.

Требования компании Совет по стандартам безопасности индустрии платежных карт (Payment Card Industry Security Standards Council, PCI SSC) — набор стандартов и требований, связанных с безопасностью и защитой данных платежных карт, включая Стандарт безопасности данных индустрии платежных карт и Стандарт безопасности данных платежных приложений, которые можно найти по адресу www.pcisecuritystandards.org.

Устройство для ввода ПИН-кода — имеет значение, установленное для Точки взаимодействия, указанное в действующей на данный момент версии Глоссария терминов Стандарта безопасности Операций, совершаемых с использованием Карт и введением ПИН-кода, и Модульных требованиях безопасности, которые можно найти на сайте www.pcisecuritystandards.org.

Устройство, позволяющее считывать чип — устройство в торговой точке, имеющее действующее одобрение и сертификацию EMVCo (www.emvco.com) и способное обрабатывать Операции с Картами с чипом, совместимыми с AEIPS.

Утверждение индустрией платежных карт — означает, что Устройство для ввода ПИН-кода либо Платежное приложение (или и то и другое) на момент внедрения находится в списке утвержденных компаний и поставщиков, который ведется компанией PCI Security Standards Council, LLC и доступен по адресу www.pcisecuritystandards.org.

Утвержденное решение по межабонентскому шифрованию (P2PE) — соответствующее решение, включенное в список проверенных решений Совета по стандартам безопасности или проверенное Квалифицированным аудитором систем безопасности Совета по стандартам безопасности индустрии платежных карт.

Утвержденный поставщик услуг сканирования — лицо, которое было утверждено компанией Payment Card Industry Security Standards Council, LLC для проведения оценки соблюдения Стандарта безопасности данных индустрии платежных карт.

Чип — интегрированный микрочип, установленный на Карте и содержащий информацию о Держателе карты и его счете.

Эмитент — любое Юридическое лицо (включая American Express и ее Аффилированных лиц), получившее лицензию American Express или Аффилированного лица American Express на выпуск Карт и участие в бизнесе по выпуску Карт.