Вопросы к вендорам

ОСНОВНЫЕ ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ ДЛЯ МАЛЫХ ТСП

ПРОДУКТ РАБОЧЕЙ ГРУППЫ ПО РАБОТЕ С МАЛЫМИ ТСП ИНДУСТРИИ ПЛАТЕЖНЫХ КАРТ

ВЕРСИЯ 2.0 | АВГУСТ 2018 Г.

PCI Security Standards Council®

Введение

Перечень вопросов, которые можно задать вендорам, является дополнением к ***руководству по безопасным платежам, содержащемуся в*** документе «Основные инструменты обеспечения безопасности данных для малых ТСП». Возможность консультации с вендорами и поставщиками услуг и получение ответов на интересующие вопросы

позволяет вам лучше понимать способы защиты этими организациями данных карт ваших клиентов.

См. ***«Руководство по безопасным платежам», а*** также документ «Основные инструменты обеспечения безопасности данных для малых ТСП»:

РЕСУРС	URL-адрес
Руководство по безопасным платежам	*https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf*
Традиционные платежные системы	*https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf*
Глоссарий терминов по платежам и информационной безопасности	*https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf*
Инструмент оценки	*http://www.pcisecuritystandards.org/merchants/ds.org/merchants/* Этот инструмент предназначен исключительно для информационных целей ТСП. Его можно использовать на первых этапах работы для ознакомления с методами обеспечения безопасности, связанных со способами приема платежей, чтобы реализовывать начальные меры и отслеживать их результаты.

Вендоры и поставщики услуг: специфика деятельности

Малые предприятия/ТСП могут заключать договора с рядом вендоров и поставщиков услуг, поэтому они должны понимать тип вендоров, с которыми они работают, и быть уверенными в том, что вендор принял надлежащие меры для защиты данных карты.

В таблице на стр. 2 описаны наиболее распространенные типы вендоров и поставщиков услуг, а также услуги, на которые могут рассчитывать ТСП при сотрудничестве с каждым из них.

В таблице, начинающейся на стр. 3, содержатся вопросы, которые ТСП могут задавать своим вендорам и поставщикам, чтобы лучше понимать их роль в защите данных платежных карт.

Вендоры и поставщики услуг

В таблице ниже описаны наиболее распространенные типы вендоров платежных систем и поставщиков услуг, их функции, стандарты PCI и программы, относящиеся к этим функциям. Список вопросов для каждого типа вендоров или поставщиков услуг см. в Приложении.

Тип вендора/поставщика услуг	Направление деятельности	Стандарт или программа PCI	Что проверить или уточнить
Вендор платежного приложения	Продают и осуществляют поддержку приложений для хранения, обработки и/или передачи данных держателей карт.	Стандарт безопасности данных платежных приложений (PA-DSS)	Приложение присутствует в *списке PCI PA-DSS с проверенными платежными приложениями.*
Вендоры платежных терминалов, вендоры платежных решений	Продают и обеспечивают поддержку устройств или решений (например, платежные терминалы или решения для шифрования данных), используемых для приема платежей по картам.	Безопасность транзакций с использованием ПИН-кода (PTS) Межабонентское шифрование PCI	Платежный терминал присутствует в *списке соответствующих требованиям PCI устройств PTS* Решение для шифрования присутствует в списке *списке решений PCI P2PE*
Процессинговые компании, поставщики платежных услуг в области электронной коммерции, платежные шлюзы, контакт-центры	Хранят, обрабатывают и/или передают данные держателей карт от вашего имени.	Стандарт безопасности данных PCI (PCI DSS)	Уточните наличие свидетельства о соответствии стандарту PCI DSS, а также выясните, распространяется ли выполненная оценка на услугу, которую вы используете. Поставщик услуг присутствует в одном из этих списков: *Список одобренных MasterCard поставщиков услуг* *Международный реестр поставщиков услуг Visa* *Зарегистрированные в Visa агенты ТСП в Европе*
Поставщики услуг хостинга в области электронной коммерции	Размещают и управляют вашим сервером/сайтом электронной коммерции, разрабатывают и обслуживают ваш сайт. Поставщик этого типа может предоставлять только услуги хостинга или, в качестве дополнительной функции, выполнять процессинг платежей.		
Поставщики программного обеспечения как услуги, поставщики услуг облачного хостинга	Разрабатывают, размещают и/или управляют вашим облачным веб- или платежным приложением (например, онлайн-приложением для покупки билетов или бронирования).		
Поставщики услуг, которые могут помочь вам выполнить требования PCI DSS	Управляют/обеспечивают функционирование систем или служб от вашего имени (например, центры сбора и обработки данных, центры колокации и ИТ-службы, например службы по управлению брандмауэром, установке обновлений или антивирусные службы).		
Интеграторы/реселлеры	Устанавливают платежные системы ТСП.	Сертифицированные интеграторы и реселлеры (QIR)	Уточните, является ли вендор сертифицированным PCI интегратором или реселлером (QIR). Вендор присутствует в *списке QIR PCI*.

Вопросы

В приведенной ниже таблице содержится ряд вопросов, которые ТСП могут задавать своим вендорам/поставщикам услуг, чтобы выяснить о реализации надлежащих мер контроля для защиты данных карты.

Примечание. Если вендор или поставщик услуг отвечает отрицательно на вопросы из этой таблицы, вам следует серьезно задуматься о поиске другого поставщика.

Какие вопросы задать	Анализ ответов вендоров: целесообразные действия и дополнительная информация для ТСП
Решение или продукт вендора безопасны?	
1. Насколько безопасным является сбор и передача данных платежных карт при использовании продукта или решения вендора? Если продукт или услуга внесены в список PCI SSC или платежных систем, это означает, что продукт/услуга прошли проверку на соответствие стандарту безопасности PCI. Включение в эти списки свидетельствует о том, что вендор или поставщик услуг приняли дополнительные меры для обеспечения безопасности их продуктов или услуг.	**Для решений или продуктов, предполагающих использование платежных терминалов или приложений:** • Проверьте наличие одобрения PCI PTS для платежного терминала в: *списке устройств PTS, соответствующих требованиям PCI* И/ИЛИ • Выясните, проверено ли платежное приложение на соответствие стандарту PCI PA-DSS в: *списке платежных приложений, соответствующих стандарту PCI PA-DSS* ИЛИ • Проверьте, проверено ли решение для шифрования на соответствие требованиям PCI P2PE в: *списке проверенных решений PCI P2PE* **Для платежных транзакций без присутствия карты (включая электронную коммерцию, заказы по почте/телефону):** • Проверьте, проверен ли поставщик услуг на соответствие требованиям PCI DSS, здесь: *Список одобренных MasterCard поставщиков услуг* *Международный реестр поставщиков услуг Visa* *Зарегистрированные в Visa агенты ТСП в Европе* ИЛИ • Выясните, проверено ли платежное приложение на соответствие стандарту PCI PA-DSS в: *списке платежных приложений, соответствующих стандарту PCI PA-DSS*

Вопросы

Какие вопросы задать	Анализ ответов вендоров: целесообразные действия и дополнительная информация для ТСП
Решение или продукт вендора безопасны?	
2. Сохраняется ли информация о платежных картах в моих системах (например, в установленных в моих магазинах, веб-приложении или на площадке электронной коммерции) при использовании продукта/решения вендора. Если да, то каким образом защищаются данные?	Продукты или решения, которые токенизируют или шифруют информацию о платежных картах, предоставляют ТСП возможности для защиты данных карты. Дополнительную информацию о шифровании и токенизации см. в *Руководстве по безопасным платежам*.
3. Защищает ли продукт/решение вендора данные платежных карт во время передачи с надежным шифрованием?	Шифрование преобразует информацию в формат, непригодный для использования. Она может считываться только держателями специального цифрового ключа. Такая защита данных платежной карты снижает вероятность кражи и мошенничества. **Для платежных терминалов и интегрированных платежных терминалов:** • По возможности выбирайте из *списка решений проверенных решений PCI P2PE* продукт или решение, в котором данные карты шифруются. Использование решения P2PE, внесенного в список PCI, означает, что данные платежной карты будут защищаться при их получении, а также при прохождении через вашу сеть к процессинговой системе. **Для платежных приложений:** • Уточните у своего поставщика, реселлера или интегратора, прошло ли платежное приложение *проверку PCI PA-DSS.* **Для размещенных площадок электронной коммерции, веб- или платежных приложений:** • Узнайте у поставщика услуг, использует ли он безопасную версию протокола Transport Layer Security (TLS) для защиты передачи данных платежных карт.
4. Требуется ли интеграция решения/ продукта поставщика с другими моими системами, например, с моими платежными терминалами, системами учета дебиторской задолженности или другими системами, которые содержат данные держателей карт?	Автономный или изолированный платежный терминал защитить гораздо проще, чем более сложную платежную платформу, к которой может быть подключено много систем. **Если решение требует интеграции с другими системами в вашей среде, задумайтесь над следующими вопросами:** • Станут ли условия процессинга более простыми? • Какую выгоду это даст вашему бизнесу? Нужно ли вам данное решение? • Примите во внимание, что оно увеличит риски и сложность вашего бизнеса, сделав среду данных держателей карт более крупной и сложной для защиты. Возможно, вы захотите обратиться к другому вендору или воспользоваться другим продуктом, если в вашем бизнесе нет большой потребности для использования более сложного решения с подключениям к другим вашим системам.

Вопросы

Какие вопросы задать	Анализ ответов вендоров: целесообразные действия и дополнительная информация для ТСП
Оказывает ли вендор содействие в безопасной установке и настройке продукта или решения?	
5. Если вендор устанавливает платежное приложение или систему в вашей среде, следует получить ответ на такие вопросы: • Является ли вендор интегратором или реселлером, сертифицированным PCI? • Если вендор не устанавливает платежное приложение или систему, следует ли устанавливать их самостоятельно?	QIR — интеграторы и реселлеры, прошедшие специальную подготовку в Совете для решения вопросов, связанных с критически важными средствами обеспечения безопасности при установке платежных систем ТСП. QIR работают над снижением рисков ТСП и устранением наиболее распространенных причин утечки данных о платежах, уделяя особое внимание критически важным средствам обеспечения безопасности. Проверьте, включен ли вендор в: *список QIR, соответствующих требованиям PCI.*
6. Независимо от того, является ли вендор сертифицированным интегратором или реселлером, если он устанавливает платежное приложение или систему, задайте такие вопросы: • Предоставляет ли вендор поддержку во время установки и гарантирует ли он ее защиту? • Предоставляет ли вендор руководство по внедрению, которое поможет выполнить безопасную настройку приложения?	Неправильная установка может сделать систему уязвимой к компрометации. Вендор должен либо самостоятельно установить приложение или систему, обеспечив ее безопасность, либо помочь вам в установке, предоставив рекомендации по внедрению. Внедрение должно включать, как минимум, способы изменения паролей по умолчанию и их замену на более надежные, способы управления исправлениями и обновлениями, а также описание способов использования вендором программного обеспечения для удаленного доступа к вашему бизнесу (и описание ваших действий в таком программном обеспечении). Более подробная информация о всех трех указанных областях отражена в вопросах 7–9 ниже.

Вопросы

Какие вопросы задать	Анализ ответов вендоров: целесообразные действия и дополнительная информация для ТСП
Оказывает ли вендор содействие в безопасной установке и настройке продукта или решения?	
7. Предоставляет ли вендор поддержку во время установки и настройки продукта/решения для содействия в изменении предоставленных им паролей по умолчанию? • Помогает ли вендор устанавливать надежные пароли?	Слабые пароли и пароли по умолчанию, предоставленные вендорами, являются одной из трех основных причин утечки данных ТСП (две другие рассматриваются в вопросах 8 и 9 ниже). Пароли по умолчанию, предоставляемые вендором, являются паролями, которые поставляются с продуктом/решением, например исходный пароль для новой системы/приложения, сайта электронной коммерции ТСП или приложения для бронирования гостиничных номеров. Зачастую они очень простые и хорошо известны хакерам (например, пароли «admin», «password» или название поставщика или продукта). При первой установке или настройке продукта пароли необходимо менять на более надежные. Если задать простой пароль (например, «12345»), хакер с легкостью сможет получить доступ к вашим платежным системам. Если вендор не меняет пароли по умолчанию при установке или настройке приложения/системы, он должен предоставить вам руководство по внедрению, в котором объясняются способы их изменения и выбора надежных.
Предоставляет ли вендор поддержку и обслуживание с использованием безопасных методов?	
8. Чтобы разобраться с исправлениями системы безопасности и обновлениями продукта/решения, задайте вендору следующие вопросы: • Какая поддержка и руководства обеспечивается вендором для моего бизнеса в процессе установки исправлений/обновлений? • Исправления и обновления предоставляются и устанавливаются автоматически? • Нужно ли самостоятельно искать и устанавливать исправления/обновления? • Какими способами пользуется вендор для уведомления о появлении новых исправлений/обновлений и их автоматической установке? • Для размещенных на хосте сайтов электронной коммерции, веб- и платежных приложений: берет ли вендор ответственность за исправление/обновление предоставляемого решения?	Приложения и системы, на которые не были установлены исправления, составляют одну из трех основных причин утечки данных ТСП (две другие рассматриваются в вопросах 7 и 9). В системах, на которых не установлены исправления, часто содержатся уязвимости, используемые хакерами для получения доступа к данным платежной карты. Поставщик должен обеспечивать текущее обслуживание и поддержку своих приложений и систем с помощью обновлений и исправлений (patch-файлов) для устранения уязвимостей программного обеспечения. Например, вендор должен при необходимости присылать вам исправления, уведомлять об их появлении и давать инструкции по установке. Для обеспечения безопасности вашего бизнеса в ваших интересах выбирать вендоров/поставщиков, которые полностью поддерживают свои продукты/решения и либо берут на себя ответственность за их установку, либо помогают вам с установкой исправлений и обновлений.

Вопросы

Какие вопросы задать	Анализ ответов вендоров: целесообразные действия и дополнительная информация для ТСП
Предоставляет ли вендор поддержку и обслуживание с использованием безопасных методов?	
9. Требуется ли вендору удаленный доступ к моему платежному приложению или системе для поддержки его продукта/решения? • Необходимо ли предоставлять вендору постоянный удаленный доступ? • Какие шаги предпринимаются вендором для защиты удаленного доступа? • Использует ли вендор один и тот же или разные пароли для своих клиентов?	Постоянно включенный удаленный доступ — одна из трех основных причин утечки данных ТСП (две другие указаны в вопросах 7 и 8 выше). Удаленный доступ открывает путь к сети ТСП извне, поэтому хакер может без проблем использовать его для взлома вашей системы (или системы, размещенной на хосте) и получения доступа к данным держателей карт. Он может предполагать удаленный доступ к сети ТСП, используемый вендором для поддержки платежного терминала/приложения или для поддержки сторонней среды/веб-приложения ТСП, размещенного на хосте. Для максимальной безопасности убедитесь, что вендоры помогают вам следующим образом: • Ограничение удаленного доступа кратковременными периодическими сеансами • Отключение удаленного доступа, когда он не используется • Многофакторная аутентификация (способ проверки личности человека, получающего доступ к системе, с использованием двух или более факторов, например: информация, которой он владеет; деятельность, которой он занимается; и то, кем он является) • Использование разных имен пользователей и паролей для каждого клиента, к которому вендор получает удаленный доступ (чтобы предотвратить использование универсальных имен пользователей и паролей, которые могут привести к компрометации данных всех клиентов)
Соответствуют ли предлагаемые вендором услуги стандарту PCI DSS?	
10. Решение/продукт запускаются из систем, принадлежащих и обслуживаемых вендором (размещенных у него)? Это означает, что ваш вендор является поставщиком услуг. **Какие вопросы задать** • Среда поставщика услуг соответствует стандарту PCI DSS? • Услуги, предлагаемые мне поставщиком услуг, включены в оценку соответствия PCI DSS	Это считается «управляемой услугой». Уточните наличие у поставщика услуг свидетельства о соответствии стандарту PCI DSS, а также выясните, распространяется ли выполненная оценка на услугу, которую вы используете. Проверьте, включен ли поставщик услуг в один из следующих списков: *Список одобренных MasterCard поставщиков услуг* *Международный реестр поставщиков услуг Visa* *Зарегистрированные в Visa агенты ТСП в Европе*
11. . В соглашение вендора со мной включены пункты, в которых указано, что вендор будет обеспечивать соответствие стандарту PCI DSS для предлагаемых услуг (или получит положительную оценку проверки на соответствие PCI DSS)?	Вендоры, предоставляющие услуги, (т. е. поставщики услуг), которые имеют свидетельство о соответствие стандарту PCI DSS или находятся на этапе его получения, захотят указать этот статус в письменное соглашение. Проверьте, включен ли поставщик услуг в один из списков, указанных в вопросе 10 выше.

Вопросы

Какие вопросы задать	Анализ ответов вендоров: целесообразные действия и дополнительная информация для ТСП
Будет ли вендор оказывать поддержку в случае утечки данных держателей карт?	
12. В случае утечки данных, связанной с продуктом или решением поставщика, задайте такие вопросы: • Каким образом вы отслеживаете утечку данных и какие средства предоставляете для наблюдения за подозрительной деятельностью? • В какие сроки и каким способом вы сообщаете об утечке данных? • В случае наложения на меня штрафов/пени вы предлагаете поддержку и защиту?	Вендор/поставщик услуг должен оказывать поддержку в случае утечки данных держателя карты. В случае возникновения вопросов об управляемой услуге или продукте/решении, предоставляемых вендором/поставщиком, услуг вендор/поставщик должен согласиться сотрудничать с экспертом по компьютерной экспертизе. В случае утечки данных и обнаружения того, что причиной послужили продукты и решения вендора/поставщика услуг, он должен согласиться помочь с выплатой наложенных на вас штрафов.
13. Застрахован ли вендор/поставщик услуг от утечки данных, связанных с его продуктом/решением?	Наличие страховки свидетельствует о том, что вендор/поставщик услуг предусмотрел свою ответственность и обязательства в отношении утечки данных держателей карт. Если у него есть страховка, спросите об объеме страхового покрытия и уточните, распространяется ли страховка на внедрение продукта или решения в ваши системы.
14. Содействует ли вендор/поставщик услуг в оповещении моих клиентов об утечке данных, если его продукт/решение является причиной утечки?	Вендор/поставщик услуг должен быть готов содействовать ТСП в оповещении об утечке, если его платежная система является причиной нарушения безопасности.
15. При положительном ответе на вопрос 14: в каком объеме вендор содействует в оповещении? Вендор: • Покрывает расходы? • Отправляет уведомления? • Обеспечивает кредитный мониторинг для пострадавших клиентов?	Если вендор не помогает с оповещением клиентов, вам следует разработать план по их оповещению в случае утечки данных держателей карт.

Приложение

На какие вопросы могут отвечать вендоры/поставщики услуг конкретных типов?

Тип вендора/поставщика услуг	Применимые вопросы
Вендор платежного приложения	1–15
Вендоры платежных терминалов, вендоры платежных решений	1–15
Процессинговые компании, поставщики платежных услуг в области электронной коммерции, платежные шлюзы, контакт-центры	1–15
Поставщики услуг хостинга в области электронной коммерции	1–15
Поставщики программного обеспечения как услуги, поставщики услуг облачного хостинга	1–4 и 0-15
Поставщики услуг, которые могут помочь вам выполнить требования PCI DSS	1–15
Интеграторы/реселлеры	5-9