Глоссарий терминов в области платежных систем и информационной безопасности данных

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

Настоящий глоссарий терминов в области платежных систем и информационной безопасности данных является дополнением к *Руководству по безопасным платежам*, которое является частью документа «Основные инструменты обеспечения безопасности данных для ТСП». Его цель — объяснить соответствующие термины индустрии платежных карт (PCI) и информационной безопасности данных простыми словами.

Определения терминов, отмеченных звездочкой (*) получены из *документа: «Стандарт безопасности данных индустрии платежных карт (PCI DSS) и Стандарт безопасности данных платежных приложений (PA-DSS). Глоссарий терминов, аббревиатур и сокращений»*. Последняя версия данного глоссария считается надежным источником актуальных и исчерпывающих определений PCI DSS и PA-DSS.

См. документ «Основные инструменты обеспечения безопасности данных для малых ТСП», который содержит следующие разделы:

РЕСУРС	URL
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*
Вопросы для вендоров и поставщиков	*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 актуальными методами обеспечения безопасности, связанными со способами приема платежей, чтобы реализовывать начальные меры и отслеживать их результаты.

Глоссарий

ТЕРМИН	ОПРЕДЕЛЕНИЕ
P2PE	Аббревиатура термина «Стандарт безопасности межабонентского шифрования Совета по стандартам безопасности PCI». Подробности см. на сайте www.pcisecuritystandards.org
PA-DSS*	Аббревиатура термина «Стандарт безопасности данных платежных приложений Совета по стандартам безопасности PCI». Подробности см. на сайте www.pcisecuritystandards.org
PCI DSS*	Аббревиатура термина «Стандарт безопасности данных индустрии платежных карт Совета по стандартам безопасности PCI». Подробности см. на сайте www.pcisecuritystandards.org
PCI*	Аббревиатура термина «Индустрия платежных карт» (Payment Card Industry).
PED*	Аббревиатура термина «Устройство для ввода ПИН-кода». Клавиатура, с помощью которой клиент вводит ПИН-код. Синоним «Клавиатура для ввода ПИН».
PTS*	Аббревиатура термина «Стандарт безопасности транзакций с вводом ПИН-кода Совета PCI». PTS– это перечень модульных требований к оценке терминалов точек взаимодействия (POI), в которых запрашивается ПИН. Подробности см. на сайте www.pcisecuritystandards.org.
QIR*	Аббревиатура термина «Квалифицированный интегратор или реселлер». QIR – интеграторы и реселлеры, прошедшие специальную подготовку в Совете для решения вопросов, связанных с критически важными средствами обеспечения безопасности при установке платежных систем ТСП. Подробности см. на сайте www.pcisecuritystandards.org
SRED	Аббревиатура термина «Безопасное считывание данных и обмен ими». Перечень требований PCI PTS, направленных на защиту и шифрования данных карт в платежных терминалах. Система межабонентского шифрования (P2PE), включенная в список Совета PCI, должна использовать отвечающий требованиям PTS (и внесенный в соответствующий список) платежный терминал с постоянным шифрованием данных карты согласно требованиям SRED.
Wi-Fi*	Беспроводная сеть, обеспечивающая соединение компьютеров без физического подключения проводов.
Автономный терминал	Платежный терминал, который не требует подключения к какому-либо другому устройству в среде ТСП и не выполняет иных функций. Единственным требованием для обеспечения его работы является подключение к процессинговой системе через Интернет или телефонную линию. Если терминал требует подключения к компьютеризированному электронному кассовому аппарату или является многофункциональным (например, мобильное устройство), его нельзя классифицировать как автономный.
Авторизация*	В контексте проведения транзакций с платежной картой авторизация выполняется, когда ТСП получает одобрение транзакции, после того как эквайер согласовывает транзакцию с эмитентом/процессинговой компанией.
Авторизованный вендор, предоставляющий услуги сканирования (ASV)*	Компания, которой Совет PCI SSC предоставил право проведения внешнего сканирования на наличие уязвимостей в конфигурации системы.
Антивирусное ПО*	Программа или программное обеспечение для обнаружения, удаления и защиты от различных форм вредоносного ПО, таких как вирусы, черви, трояны, шпионское и рекламное ПО, руткиты. Синоним: «программа для защиты от вредоносного ПО».

Глоссарий

ТЕРМИН	ОПРЕДЕЛЕНИЕ
Аутентификация*	Процесс проверки личности человека или идентификации устройства или процесса, которые пытаются получить доступ к компьютеру. Для подтверждения личности пользователя используются один или несколько факторов: • пароль или парольная фраза (информация, известная пользователю); • токен, смарт-карта или уникальный цифровой сертификат пользователя (что-то, чем владеет пользователь); • биометрический идентификатор, например, цифровой отпечаток пальца (уникальный признак пользователя).
Банк ТСП*	Банк или финансовое учреждение, которое обрабатывает платежи по кредитным и/или дебетовым картам от имени ТСП. Синонимы: «эквайер», «банк-эквайер», «процессинговая система», «процессинговая компания». Также см. раздел «Процессинговая система».
Банковский идентификационный номер (BIN)	Первые шесть (или более) цифр номера платежной карты, которые указывают на эмитента карты.
Безопасный считыватель карт (SCR)	Соответствующее требованиям PTS устройство, которое подключается к мобильному телефону или планшету для безопасного приема платежных карт. SCR, отвечающие критериям PCI PTS, защищают и шифруют данные карты посредством SRED. Также см. SRED.
Беспроводной платежный терминал	Платежный терминал, который для подключения у Интернету использует любую беспроводную технологию.
Брандмауэр*	Устройство и/или программа, защищающие сетевые ресурсы от несанкционированного доступа. Брандмауэр разрешает или ограничивает передачу данных между сетями с различными уровнями безопасности, руководствуясь набором правил и других критериев.
Вендор	Субъект бизнеса, который поставляет ТСП продукт или предоставляет услугу, необходимую для осуществления коммерческой деятельности. В случае предоставления услуг вендор может классифицироваться как поставщик услуг и запросить доступ к физическим местоположениям или компьютерным системам в среде ТСП, что может повлиять на безопасность данных карты. Также см. *«Поставщик услуг».*
Вендор платежного приложения	Вендор, который продает приложения, используемые для хранения, процессинга и/или передачи данных карты во время платежных транзакций.
Вендор платежной системы	Вендор, который продает, лицензирует или поставляет комплексное платежное решение для ТСП. Данное решение включает оборудование и программное обеспечение, необходимое для обработки платежей в торговой точке, и предоставляет способ подключения к процессинговой системе.
Виртуальная частная сеть (VPN)*	Программное обеспечение, которое создает безопасный частный канал для обмена данными и телефонных звонков через Интернет.
Виртуальный платежный терминал*	Система доступа через браузер к эквайеру, процессинговой системе или сайту стороннего поставщика услуг для авторизации транзакций по платежным картам. В отличие от физических терминалов, виртуальные платежные терминалы не считывают данные непосредственно с платежной карты. ТСП вручную вводит данные платежной карты через браузер с защищенным подключением. Поскольку транзакции по платежным картам инициируются вручную, виртуальные платежные терминалы обычно используются вместо физических терминалов в средах ТСП с низкими объемами транзакций.

Глоссарий

ТЕРМИН	ОПРЕДЕЛЕНИЕ
Вирус	Вредоносное ПО, которое самостоятельно копируется в иное программное обеспечение или файлы данных на «инфицированном» компьютере. После репликации вирус выполняет действия разрушительного характера, например удаляет все данные с компьютера. Иногда вирус бездействует и активируется позже, а в некоторых случаях не наносит ущерб. Вирус, который самостоятельно копируется и повторно отправляется в виде вложения электронной почты или как часть сетевого сообщения, называется «червем».
Вредоносное ПО*	Вредоносное ПО, предназначенное для проникновения в компьютерную систему с целью похищения данных или повреждения приложений и операционной системы. Такое ПО обычно проникает в сеть при выполнении обычных деловых задач, связанных с электронной почтой или поиском в Интернете. Примерами вредоносного ПО являются вирусы, черви, трояны, шпионское и рекламное ПО, руткиты.
Данные карты/данные карты клиента*	Как минимум, данные карты включают основной номер счета (PAN); дополнительно могут содержать имя держателя карты и срок действия. PAN указан на лицевой стороне карты и закодирован на магнитной полосе карты и/или во встроенном чипе. Синоним: «данные держателя карты». В разделе «Конфиденциальные аутентификационные данные» описаны другие элементы данных, которые могут быть частью платежной транзакции, но которые запрещено хранить после ее авторизации.
Журнал*	Файл, который создается автоматически и содержит записи об определенных событиях (связанных с безопасностью) в системе или сети. Данные журнала включают отметку даты/времени, описание события и уникальную информацию. Такой файл полезен для решения технических вопросов и расследования утечки данных. Синоним: «журнал регистрации событий».
Злоупотребление правами доступа	Злоупотребление правами доступа к системе. Например, неправомерный доступ системного администратора к данным карты, а также завладение привилегированными правами доступа администратора и их использование в злоумышленных целях.
Интегратор/реселлер	Интегратор/реселлер — это компания, которая помогает ТСП настроить платежную систему (включая установку, конфигурирование и поддержку). Кроме того, такие компании могут в рамках своих услуг продавать платежные устройства или приложения. Также см. раздел «Сертифицированный интегратор/реселлер (QIR)».
Интегрированный платежный терминал	Платежный терминал и электронный кассовый аппарат в одном устройстве, которое может принимать платежи, регистрировать и рассчитывать сумму транзакций и печатать квитанции.
Исправление*	Обновление к существующей версии ПО для расширения функционала и исправления ошибок (или «багов»).
Касса	См. Электронный кассовый аппарат.
Кибератака	Любые нарушения в виде взлома компьютера или системы. Разновидности кибератак варьируются от установки шпионского ПО на ПК до взлома процессинговой системы с целью кражи данных карты или попытки взломать критически важный объект инфраструктуры, такой как электросеть.
Код безопасности*	Комбинация из трех или четырех цифр на лицевой или оборотной стороне платежной карты в месте для подписи. Этот код является уникальным признаком конкретной карты и используется в рамках дополнительной проверки — как правило, во время транзакции без присутствия карты. Код дает возможность убедиться, что карта находится у ее законного держателя. Синоним: «Код безопасности карты».
Криптография	Криптография — это способ защиты данных путем их преобразования в нечитаемую для человека или компьютера форму. Криптография целесообразна только при условии, что получатель информации может преобразовать зашифрованные данные в исходное сообщение известным для него и отправителя способом. Также см. раздел «Шифрование».

Глоссарий

ТЕРМИН	ОПРЕДЕЛЕНИЕ
Критичные аутентификационные данные*	Данные, связанные с обеспечением безопасности, которые используются для аутентификации держателей и/или авторизации транзакций по платежной карте и хранятся на магнитной полосе или чипе.
Малое ТСП	Малое ТСП, как правило, представляет собой независимый бизнес с одним или несколькими торговыми точками, ограниченным ИТ- бюджетом или без такового и часто без штатных ИТ-специалистов. Необходимость проверки малого ТСП на соответствие требованиям PCI определяется платежным оператором или эквайером (банком ТСП).
Маршрутизатор*	Устройство или программное обеспечение, которое соединяет две и более внутренние или внешние компьютерные сети и выполняет функцию «маршрутизации» или направления данных через сеть, а также обеспечения надлежащего потока данных между этими сетями. Маршрутизатор способствует повышению уровня безопасности, пропуская только одобренный трафик и отклоняя неодобренный.
Межплатформенное платежное ПО	Общий термин для обозначения программного обеспечения, которое объединяет два или более платежных приложения, которые не обязательно связаны друг с другом. Например, данное ПО может передавать данные карты между приложением на платежном терминале и другими системами ТСП, которые отправляют их процессинговой компании.
Многофакторна я аутентификация*	Аутентификация пользователя с использованием двух или более факторов. Эти факторы включают предметы, которыми владеет пользователь (например, смарт-карта или электронный ключ), информацию, которой он владеет (например, пароль, кодовая фраза или ПИН), и его уникальные признаки (например, отпечатки пальцев, другие биометрические данные и пр.).
Мобильное устройство	Небольшие портативные устройства, такие как смартфон или планшет, которые подключаются к беспроводному Интернету.
Незашифрованные данные	Любые данные, которые можно прочитать без предварительной расшифровки. Синонимы: «данные в формате plaintext и clear-text».
Операционная система*	Программное обеспечение, которое выполняет общее управление компьютерными операциями и их координирование. Примеры: Microsoft Windows, Apple OSX, iOS, Android, Linux и UNIX.
Опросный лист для самостоятельной оценки (SAQ)*	Анкета с перечнем требований PCI DSS, самостоятельно заполняемая организацией, которая хочет подтвердить их выполнение.
Основной номер платежной карты (PAN)*	Уникальная комбинация цифр в номере кредитной или дебетовой карты, по которой идентифицируется счет держателя карты.
Основные инструменты обеспечения безопасности данных (Data Security Essentials, DSE)	Основные инструменты обеспечения безопасности данных для малых ТСП (Data Security Essentials, DSE) – это набор образовательных ресурсов и инструмент оценки, которые помогают ТСП упростить процесс обеспечения безопасности и снизить риски. DSE предлагают альтернативный подход к использованию опросных листов для самостоятельной оценки соответствия PCI DSS для ТСП, отвечающих критериям для выполнения такой оценки по определению платежных операторов и банков-эквайеров.
Пароль по умолчанию	Простой пароль, который изначально установлен в новом программном обеспечении или на новом устройстве. Пароли по умолчанию (например, «admin», «password» или «123456») легко подобрать и найти в Интернете. Они предназначены для временного использования и не обеспечивают реальной защиты. Такой пароль необходимо заменить на более надежный после установки нового программного обеспечения или устройства.

Глоссарий

ТЕРМИН	ОПРЕДЕЛЕНИЕ
Пароль*	Слово, фраза или строка символов, предназначенные для аутентификации пользователя. Пароль в сочетании с именем пользователя используется с целью подтверждения личности пользователя для доступа к ресурсам компьютера.
ПИН*	Аббревиатура термина «Персональный идентификационный номер». Секретная комбинация цифр, известная только пользователю, по которому он идентифицируется в системе. Обычно ПИН-код используется в банкоматах для выдачи наличных или в картах с чипом EMV как альтернатива подписи. ПИН позволяет одобрить авторизацию держателя карты или предотвратить неправомерные транзакции, если карта украдена.
Платежная система	Охватывает весь процесс приема платежей по картам в розничной точке ТСП (как обычные, так и онлайн-магазины) и может включать в себя платежный терминал, электронный кассовый аппарат и другие устройства или системы, подключенные к платежному терминалу (например, Wi-Fi или ПК, используемый для учета), серверы с элементами электронной коммерции, такими как платежные страницы, и подключения к банку ТСП.
Платежное приложение, соответствующее требованиям PCI	Программное приложение, проверенное на соответствие стандарту безопасности данных платежных приложений PCI (PA-DSS) и включенное в список, опубликованный на сайте Совета PCI.
Платежное приложение*	В отношении PA-DSS: программное приложение, которое хранит, обрабатывает или передает данные держателей карт в рамках процесса авторизации или проведения платежных транзакций.
Платежный терминал	Аппаратное устройство, используемое для приема платежей по карте клиента, при котором карта проводится, вставляется или прикладывается к терминалу. Синонимы: «Терминал торговой точки (POS)», «Устройство для приема кредитных карт», «Терминал PDQ».
Платежный терминал, одобренный PCI	Платежный терминал, признанный соответствующим стандарту безопасности транзакций с использованием ПИН-кода (PTS) PCI и включенный в список, опубликованный на сайте Совета PCI.
Подтверждение соответствия стандарту PCI DSS	Предоставление доказательств, что на конкретный момент времени выполнены все предусмотренные требования PCI DSS. В зависимости от конкретных требований банка и/или платежного оператора, подтверждение может быть предоставлено путем заполнения соответствующего опросного листа для самостоятельной оценки соответствия PCI DSS или отчета о соответствии требованиям по результатам проверки на месте.
Поставщик услуг*	Субъект бизнеса, предоставляющий ТСП различные услуги. Как правило, такие субъекты хранят, обрабатывают или передают данные карт от имени сторонней организации (например, ТСП) ИЛИ являются поставщиками управляемых услуг, предоставляющие услуги межсетевого экранирования (брандмауэра), обнаружения вторжений и прочие услуги, связанные со сферой ИТ. Синоним: «вендор».
Прием мобильных платежей	Использование мобильного устройства для приема и обработки платежных транзакций. Мобильное устройство обычно дополняется приобретаемым отдельно считывателем карт.
Приложение*	Программа или пакет программ на ПК, смартфоне, планшете, внутреннем сервере или веб-сервере.
Процессинговая компания*	Организация, привлеченная ТСП для обработки транзакций по платежным картам от имени ТСП. Несмотря на то, что процессинговые компании обычно предоставляют услуги эквайринга, они не относятся к эквайерам (банкам ТСП), если это не определено платежным оператором. Синоним: «платежный шлюз» или «поставщик платежных услуг» (PSP). Также см. раздел «Банк ТСП».

Глоссарий

ТЕРМИН	ОПРЕДЕЛЕНИЕ
Раскрытие данных в связи со служебной необходимостью	Принцип, согласно которому для служебных целей может быть предоставлен доступ к системе и данным.
Регулярный платеж	Метод оплаты, при котором ТСП регулярно выставляют своим клиентам счет с определенной периодичностью (например, ежемесячная оплата подписки или членства). Безопасный способ для проведения таких транзакций со стороны эквайера/процессинговой системы – токенизация данных карты, что обеспечивает их защиту и снимает эту обязанность с ТСП.
Реселлер/интегратор*	Организация, которая продает и/или интегрирует платежные приложения, но не разрабатывает их.
Решение для межабонентского шифрования, включенное в список PCI	Инструмент шифрования, проверенный на соответствие стандарту межабонентского шифрования (P2PE) и включенный в список, опубликованный на сайте Совета PCI.
Сертифицированный аудитор безопасности (QSA)*	Компания, утвержденная Советом по стандартам безопасности PCI (PCI Security Standards Council) для проверки соблюдения организацией требований PCI DSS.
Сеть*	Два или более компьютера, объединенных проводным или беспроводным способом.
Сканирование уязвимостей	Программный инструмент, который обнаруживает и классифицирует потенциальные слабые места (уязвимости) на компьютере или в сети. Ежеквартальное внешнее сканирование уязвимостей в соответствии с требованием 1 .2.2 PCI DSS должно проводиться одобренным вендором, предоставляющим услуги сканирования. Иное сканирование уязвимостей (например, внутреннее сканирование и сканирование, выполняемое после изменений в сети) может проводиться квалифицированным персоналом ИТ-отдела организации или поставщиком услуг по обеспечению безопасности (например, одобренным вендором, предоставляющим услуги сканирования). *Также см. «Одобренный вендор, предоставляющий услуги сканирования (ASV)».*
Скимминг	Хищение данных карты непосредственно с платежной карты клиента или из платежной инфраструктуры в месте нахождения ТСП, например, с помощью несанкционированного переносного считывателя карт или посредством внесения модификаций в платежный терминал ТСП. Скимминг осуществляется в мошеннических целях, является серьезной угрозой и способен нанести ущерб программной среде ТСП.
Скиммингговое устройство	Физическое устройство, обычно прикрепляемое к считывателю карт, предназначенное для незаконного считывания и/или хранения информации с платежной карты. Синоним: «скиммер карты».
Соответствие стандарту PCI DSS	Выполнение всех предусмотренных требований действующего стандарта PCI DSS на постоянной основе в рамках обычной деловой активности. Соответствие требованиям стандарта оценивается и подтверждается по результатам проверки в конкретный момент времени; однако каждое ТСП обязано постоянно соблюдать требования для обеспечения безопасности данных. У банков или платежных операторов, обслуживающих ТСП, имеют могут быть свои требования к официальной ежегодной проверке на соответствие стандарту PCI DSS.
Строгая аутентификация	Используется для проверки личности пользователя или идентификатора устройства с целью обеспечения безопасности подконтрольной системы. Термин «строгая аутентификация» часто подразумевает многофакторную аутентификацию (MFA).

Глоссарий

ТЕРМИН	ОПРЕДЕЛЕНИЕ
Токенизация	Процесс, в результате которого основной номер платежной карты (PAN) заменяется альтернативным значением, называемым токеном. Токены могут использоваться вместо исходного номера PAN для выполнения функций без присутствия карты, напр. отмена транзакции, возврат средств или регулярные платежи. Токены также улучшают защиту в случае хищения, поскольку они непригодны для использования и, следовательно, не имеют ценности для преступника.
Удаленный доступ*	Подключение к компьютерной сети извне. Удаленный доступ может осуществляться как из локальной сети компании, так и из внешней сети. Примером технологии удаленного доступа является виртуальная частная сеть (VPN). Удаленный доступ может быть как внутренним (например, подключение специалистов ИТ-поддержки), так и внешним (например, подключение поставщиков услуг, сторонних агентов, интеграторов/реселлеров).
Утечка данных	Кутечке данных относятся случаи несанкционированного раскрытия конфиденциальной информации. Это могут быть данные карты, персональная медицинская информация (PHI), идентификационные данные (PII), коммерческая тайна или интеллектуальная собственность и т. д.
Учетные данные	Информация, используемая для удостоверения личности для доступа в систему. Часто учетными данными являются имя пользователя и пароль. Учетные данные могут также включать отпечаток пальца, скан сетчатки глаза или одноразовый пароль, сгенерированный портативным аппаратным токеном. Чем больше учетных данных требуется для доступа, тем выше степень безопасности.
Уязвимость*	Недостаток или слабое место системы, которые при неправильном или неосторожном использовании могут стать причиной умышленной или неумышленной компрометации данных.
Хакер	Лицо или организация, которые пытаются обойти меры безопасности компьютерных систем для получения доступа. Обычно это делается с целью кражи данных карты.
Хостинг-провайдер*	Организация, которая предлагает ТСП и другим поставщикам различные услуги, связанные с размещением данных клиента на своих серверах. В стандартные услуги входит предоставление совместно используемого места на сервере, предоставление выделенного сервера для ТСП или веб-приложения (например, сайта с «корзиной»).
Чип	Синоним: «чип EMV». Микропроцессор (или «чип») платежной карты, используемый при процессинге транзакций в соответствии с международными спецификациями транзакций EMV.
Чип и ПИН-код	Процесс проверки карты, при котором для оплаты товаров и услуг клиент вводит свой ПИН на платежном терминале, совместимом с чипами EMV.
Чип и подпись	Процесс проверки карты, при котором для оплаты товаров и услуг клиент ставит свою подпись на платежном терминале, совместимом с чипами EMV.
Шифрование	Процесс математического преобразования данных в форму, нечитаемую для всех, кроме держателя специального цифрового ключа. Использование шифрования защищает информацию, снижая ее привлекательность для злоумышленников. Также см. раздел «Криптография».
Эквайер*	См. разделы «Банк ТСП» и «Процессинговая система».

Глоссарий

ТЕРМИН	ОПРЕДЕЛЕНИЕ
Эксперты в области компьютерной криминалистики	Эксперты в области компьютерной криминалистики (PCI Forensic Investigators, PFI) – это компании, одобренные Советом PCI, которые определяют, при каких обстоятельствах произошла утечка данных. Они проводят расследования в финансовой сфере с использованием проверенных методик и инструментов. Они также работают с правоохранительными органами и оказывают поддержку заинтересованным сторонам в любых уголовных расследованиях.
Электронный кассовый аппарат (ECR)	Устройство, которое регистрирует и рассчитывает сумму транзакции и может распечатывать квитанции, но не принимает платежи по карте клиента. Синоним: «касса».