Стандарт безопасности данных индустрии платежных карт (PCI DSS) и Стандарт безопасности данных платежных приложений (PA-DSS)

Глоссарий. Основные определения, аббревиатуры и сокращения.

Версия 3.0

Январь 2014 г.

Термин	Определение
AAA	Аббревиатура — аутентификация, авторизация и учет (authentication, authorization, and accounting). Набор протоколов для: — аутентификации пользователя на основе его верифицируемых идентификационных данных; — авторизации пользователя на основе его прав; — учета потребления пользователем сетевых ресурсов.
Контроль доступа (Access Control)	Механизмы, с использованием которых доступ к данным или к ресурсам для обработки данных ограничивается только авторизованным кругом лиц или приложений.
Данные платежных карт (Account Data)	Данные платежных карт включают данные о держателе карты и (или) критичные аутентификационные данные. См. *«Данные о держателе карты» (Cardholder Data)* и *«Критичные аутентификационные данные» (Sensitive Authentication Data)*
Номер карты (Account Number)	См.*PAN (Primary Account Number).*
Эквайрер (Acquirer)	Синонимы: «банк торгово-сервисного предприятия» (merchant bank), «банк-эквайрер» (acquiring bank), «финансовая организация – эквайрер» (acquiring financial institution). Организация, которая устанавливает и поддерживает договорные отношения с торгово-сервисными предприятиями по приему платежных карт.
Рекламное ПО (Adware)	Тип вредоносного ПО, которое, будучи установленным, заставляет компьютер автоматически отображать или загружать рекламные объявления.
AES	Аббревиатура для Advanced Encryption Standard («улучшенный стандарт шифрования»). Название алгоритма блочного шифрования, используемого в симметричной криптографии, утвержденного институтом NIST (Национальным институтом стандартов и технологий), США в ноябре 2001 года. Этот алгоритм был принят как стандарт U.S. FIPS PUB 197 (или FIPS 197). См. *«Стойкая криптография» (Strong Cryptography).*
ANSI	Аббревиатура – American National Standards Institute («Американский национальный институт стандартов»). Частная некоммерческая организация, которая управляет и координирует в США деятельность добровольной системы стандартизации и оценки соответствия требованиям.
Антивирус (Anti-Virus)	Программа или программное обеспечение для обнаружения, удаления и защиты от различных форм вредоносного ПО, таких как вирусы, черви, трояны, шпионское и рекламное ПО, руткиты.
Свидетельство о соответствии (AOC, attestation of compliance)	Свидетельство о соответствии — это форма документа для ТСП и поставщиков услуг, предназначенная для подтверждения результатов оценки соответствия требованиям PCI DSS, описанных в Опросном листе для самооценки или в Отчете о соответствии.

Термин	Определение
Свидетельство о проверке (AOV, attestation of validation)	Свидетельство о проверке — это форма документа для аудиторов PA-QSA, предназначенная для подтверждения результатов проверки на соответствие требованиям PA-DSS, описанных в Отчете о проверке на соответствие стандарту PA-DSS.
Приложение (Application)	Любые приобретенные или заказные программы или пакеты программ, включая внутренние и внешние приложения (например, веб-приложения).
ASV	Аббревиатура — Approved Scanning Vendor («авторизованный поставщик услуг сканирования»). Компания, которой Совет PCI SSC предоставил право проведения внешнего сканирования на наличие уязвимостей.
Журнал аудита (Audit Log)	Синоним: «журнал регистрации событий». Перечень записей действий в системе в хронологическом порядке. Журнал предоставляет возможность независимого и верифицируемого анализа записей, достаточного для восстановления, изучения и анализа последовательности смены сред, состояний и действий, которые имеют отношение или ведут к операции, процедуре или событию в транзакции от начала ее выполнения и до завершения.
Журнал регистрации событий (Audit Trail)	См. *«Журнал аудита» (Audit Log).*
Аутентификация (Authentication)	Процесс проверки подлинности в отношении человека, устройства или процесса. Аутентификация обычно выполняется посредством использования одного или нескольких аутентификационных факторов, таких как: ▪ обладание информацией (например, паролем или парольной фразой); ▪ обладание предметом (например, аппаратным токеном или смарт-картой); ▪ обладание параметрами (например, биометрическими).
Учетные данные для аутентификации (Authentication Credentials)	Сочетание идентификатора пользователя или учетной записи и одного или нескольких аутентификационных факторов, которые используются для проверки подлинности в отношении человека, устройства или процесса.
Авторизация (Authorization)	В контексте контроля доступа авторизация означает предоставление прав доступа или иных прав пользователю, программе или процессу. Авторизация определяет, что пользователь или программа может делать после успешной аутентификации. В контексте проведения транзакций с платежной картой авторизация выполняется, когда ТСП получает одобрение транзакции, после того как эквайрер согласовывает транзакцию с эмитентом и (или) процессинговым центром.
Резервная копия (Backup)	Копия данных, создаваемая с целью архивирования или защиты от повреждения или потери.
Привычные бизнес-процессы (BAU,	business as usual) Привычные бизнес-процессы — это обычные повседневные рабочие операции организации.

Термин	Определение
Bluetooth	Протокол беспроводной связи, который использует технологию связи ближнего действия для передачи данных на короткие расстояния.
Переполнение буфера (Buffer Overflow)	Уязвимость, связанная с небезопасными методами программирования. Возникает, когда программа выходит за границы буфера и записывает данные в соседнюю область памяти. Переполнение буфера используется злоумышленниками для получения несанкционированного доступа к системам или данным.
Скиммер карт (Card Skimmer)	Физическое устройство (часто подсоединяемое к легитимному устройству, предназначенному для считывания информации с платежных карт), предназначенное для незаконного считывания и (или) сохранения информации с платежной карты.
Код или значение проверки подлинности карты (Card Verification Code or Value)	Синонимы: «код или значение подтверждения подлинности карты» (Card Validation Code or Value), «код безопасности» (Card Security Code). Обозначает следующее: (1) данные магнитной полосы или (2) напечатанные элементы обеспечения безопасности. (1) Элемент данных магнитной полосы карты, использующий безопасные процессы криптографической защиты целостности данных магнитной полосы и обеспечивающий обнаружение изменений и подделок карты. В зависимости от международной платежной системы существуют следующие коды и (или) значения проверки подлинности карты: CAV, CVC, CVV или CSC. Ниже приведены термины для каждой международной платежной системы: ▪ **CAV —** Card Authentication Value (для платежных карт JCB); ▪ **CVC —** Card Validation Code (для платежных карт MasterCard); ▪ **CVV —** Card Verification Value (для платежных карт Visa и Discover); ▪ **CSC —** Card Security Code (для платежных карт American Express). (2) Для платежных карт Discover, JCB, MasterCard и Visa второй тип значений или кодов проверки подлинности карты — это крайнее правое трехзначное число, напечатанное на полосе для подписи на оборотной стороне карты. Код проверки подлинности карт American Express — это четырехзначное неэмбоссированное число на лицевой стороне платежной карты, над ее номером PAN. Код проверки подлинности уникально связан с каждой конкретной пластиковой картой, и он связывает ее с номером PAN. Ниже приведены термины для каждой международной платежной системы: ▪ **CID —** Card Identification Number (для платежных карт American Express и Discover); ▪ **CAV2 —** Card Authentication Value 2 (для платежных карт JCB); ▪ **CVC2 —** Card Validation Code 2 (для платежных карт MasterCard); ▪ **CVV2 —** Card Verification Value 2 (для платежных карт Visa).

Термин	Определение
Держатель карты (Cardholder)	Клиент или работник, на имя которого выпущена платежная карта, или любое лицо, имеющее право пользоваться платежной картой.
Данные о держателе карты, ДДК (Cardholder Data)	ДДК включают в себя, как минимум, полный номер PAN. ДДК также могут быть представлены в виде сочетания полного номера PAN и любых данных из приведенного ниже списка: — имя держателя карты, — дата истечения срока действия карты, — сервисный код. См. *«Критичные аутентификационные данные» (Sensitive Authentication Data)*, чтобы узнать о дополнительных элементах данных, которые можно передавать или обрабатывать (но не хранить) при выполнении платежной транзакции.
Среда ДДК (CDE)	Сокращение — среда данных о держателях карт (Cardholder Data Environment) Среда ДДК — это люди, процессы и технологии, которые хранят, обрабатывают или передают ДДК или КАД.
Технологии сотовой связи (Cellular Technologies)	Мобильная связь по беспроводным телефонным сетям, включая, среди прочего, стандарты GSM, CDMA и GPRS.
CERT	Аббревиатура — Computer Emergency Response Team («Группа реагирования на компьютерные инциденты» Университета Карнеги-Меллона). Программа CERT разрабатывает и продвигает использование надлежащих методов управления технологиями и системами для противостояния атакам на подключенные к сети системы, для минимизации ущерба и для обеспечения непрерывности работы критичных служб.
Контроль изменений (Change Control)	Процессы и процедуры изучения, тестирования и утверждения изменений в системе и ПО с проверкой их влияния перед применением.
CIS	Аббревиатура — Center for Internet Security («Центр интернет-безопасности»). Некоммерческое учреждение, целью которого является содействие организациям в снижении рисков перебоев в работе и ведении электронной коммерции из-за недостаточных технических защитных мер.
Шифрование базы данных на уровне столбцов (Column-Level Database Encryption)	Метод или технология (программные или аппаратные) для шифрования не всего содержимого базы данных, а определенного столбца. См. также *«Шифрование диска» (Disk Encryption)* или *«Шифрование на уровне файла» (File-Level Encryption).*

Термин	Определение
Компенсационные меры (Compensating Controls)	Если проверяемая организация не может напрямую выполнить исходное требование PCI DSS в силу обоснованных технических ограничений или задокументированных ограничений, связанных с ее деятельностью, но при этом успешно снизила риск, связанный с данным требованием, путем реализации других мер, такие меры могут быть признаны компенсационными. Компенсационные меры должны: (1) отвечать цели и строгости исходного требования PCI DSS; (2) обеспечивать такой же уровень защиты, как и исходное требование PCI DSS; (3) обеспечивать дополнительный уровень защиты по сравнению с прочими требованиями PCI DSS (а не только не противоречить прочим требованиям PCI DSS); (4) быть соизмеримыми с дополнительным риском, который вызван несоблюдением требования PCI DSS. См. Приложения B и C «Компенсационные меры» к документу *«Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования и процедуры оценки безопасности»*.
Компрометация (Compromise)	Синоним: «компрометация данных» (data compromise, data breach). Вторжение в компьютерную систему, при котором существует подозрение на несанкционированное раскрытие, кражу, изменение или уничтожение ДДК.
Консоль (Console)	Экран и клавиатура, с помощью которых осуществляется доступ и управление сервером, мейнфреймом или другим типом системы в сетевом окружении.
Клиент (Consumer)	Лицо, которое приобретает товары и (или) пользуется услугами.
Подделка межсайтовых запросов (CSRF)	Уязвимость, возникающая в результате небезопасных методов программирования, которая позволяет выполнять нежелательные действия через аутентифицированный сеанс связи. Часто используется в сочетании с межсайтовым скриптингом (XSS) и (или) SQL-инъекцией.
Межсайтовый скриптинг (XSS)	Уязвимость, возникающая в результате небезопасных методов программирования, выражающихся в некорректной проверке введенных данных. Часто используется в сочетании с подделкой межсайтовых запросов (CSRF) и (или) SQL-инъекцией.
Криптографический ключ (Cryptographic Key)	Значение, определяющее результаты исполнения криптографического алгоритма при преобразовании открытого текста в криптотекст. Сложность дешифрования шифрованного текста в исходное сообщение в основном определяется длиной ключа. См. *«Стойкая криптография» (Strong Cryptography).*
Управление криптографическими ключами (Cryptographic Key Management)	Набор процессов и механизмов, которые поддерживают создание и обслуживание криптографических ключей, включая замену старых ключей новыми при необходимости.

Термин	Определение
Криптография (Cryptography)	Раздел математики и информатики, занимающийся безопасностью информации, в частности шифрованием и аутентификацией. В области безопасности сети и приложений это инструмент для обеспечения контроля доступа, конфиденциальности и целостности информации.
Криптопериод (Cryptoperiod)	Отрезок времени, в течение которого определенный криптографический ключ может использоваться по определенному для него назначению. Такой отрезок определяется, например, с учетом какого-либо определенного срока действия и (или) объема полученного криптотекста, а также в соответствии с практическими отраслевыми рекомендациями и руководствами (такими как, например, специальное издание *NIST 800-57*).
CVSS	Аббревиатура — Common Vulnerability Scoring System («общая система оценки уязвимостей»). Независимый открытый отраслевой стандарт, предназначенный для оценки уровня опасности уязвимостей в компьютерной системе безопасности и определения срочности и приоритета ответных мер. См. дополнительную информацию в *«Руководстве по программе ASV» (ASV Program Guide)*.
Схема потоков данных (Data-Flow Diagram)	Схема, на которой указаны потоки данных в приложении, системе или сети.
База данных (Database)	Структурированная форма данных для упорядочивания, обслуживания и удобного извлечения данных. Простейшими примерами базы данных являются таблицы, в т.ч. электронные.
Администратор базы данных (Database Administrator, DBA)	Синоним: «администратор БД». Лицо, ответственное за управление и администрирование баз данных.
Учетная запись по умолчанию (Default Account)	Учетная запись для входа, предварительно заданная в системе, приложении или устройстве и предназначенная для первоначального доступа к системе при ее начальном запуске. В процессе установки система может сгенерировать дополнительные учетные записи по умолчанию.
Пароль по умолчанию (Default Password)	Пароль (как правило, связанный с учетной записью по умолчанию) к административным, пользовательским или служебным учетным записям, предварительно заданный в системе, приложении или устройстве. Учетные записи по умолчанию и пароли по умолчанию опубликованы, хорошо известны и поэтому легко угадываются.
Размагничивание (Degaussing)	Синоним: «размагничивание диска» (disk degaussing). Процесс или метод размагничивания диска для безвозвратного уничтожения всех данных, которые хранятся на диске.
Зависимость (Dependency)	В контексте PA-DSS зависимость означает определенный программный или аппаратный компонент (например, аппаратный терминал, база данных, операционная система, API, библиотека кода и т. д.), необходимый для соответствия платежного приложения требованиям PA-DSS.

Термин	Определение
Шифрование диска (Disk Encryption)	Метод или технология (программная или аппаратная) для шифрования всех данных, которые хранятся на устройстве (например, на жестком диске или флэш-накопителе). Также для шифрования содержимого определенных файлов или столбцов базы данных могут использоваться такие методы, как *«Шифрование на уровне файла» (File-Level Encryption)* или*«Шифрование базы данных на уровне столбцов» (Column-Level Database Encryption)*.
DMZ	Аббревиатура — demilitarized zone («демилитаризованная зона»). Физическая или логическая подсеть, которая обеспечивает дополнительный уровень защиты для внутренней частной сети организации. DMZ создает дополнительный уровень защиты сети между сетью Интернет и внутренней сетью организации, чтобы внешние стороны могли подключаться напрямую только к устройствам в DMZ, а не ко всей внутренней сети.
DNS	Аббревиатура — domain name system («система доменных имен») или domain name server («сервер доменных имен»). Система, которая хранит в распределенной базе данных информацию, связанную с доменными именами, для предоставления пользователям в сети, такой как сеть Интернет, услуг по разрешению имен.
DSS	Аббревиатура — Data Security Standard («Стандарт безопасности данных»). См. *PA-DSS* и *PCI DSS.*
Двойной контроль (Dual Control)	Процесс привлечения с целью защиты критичных функций или данных двух или более независимых субъектов (как правило, физических лиц) к совместной работе. Оба субъекта несут одинаковую ответственность за физическую защиту материалов, вовлеченных в уязвимые транзакции. Ни одно из этих физических лиц не допускается к материалам (например, к криптографическому ключу) и работе с ними без присутствия другого лица (лиц). Для генерации ключа вручную, а также для его передачи, загрузки, хранения и извлечения в соответствии с принципом двойного контроля необходимо, чтобы каждому субъекту был известен только компонент ключа. (См. также *«Разделение знания»* (Split Knowledge)).
Динамическая фильтрация пакетов (Dynamic Packet Filtering)	См. *«Проверка с сохранением состояния» (Stateful Inspection).*
ECC	Аббревиатура — elliptic curve cryptography («криптография на основе эллиптических кривых»). Метод, применяемый в криптографии с открытым ключом, использующий конечные поля точек эллиптических кривых. См. *«Стойкая криптография» (Strong Cryptography).*
Фильтрация исходящего трафика (Egress Filtering)	Метод фильтрации исходящего сетевого трафика, при котором только явно разрешенный трафик может выходить за пределы сети.

Термин	Определение
Шифрование (Encryption)	Процесс преобразования информации в форму, нечитаемую всеми, кроме держателей соответствующего криптографического ключа. Использование алгоритмов шифрования позволяет защитить информацию от несанкционированного раскрытия в период между процессом шифрования и процессом расшифрования (процессом, противоположным шифрованию). См. *«Стойкая криптография» (Strong Cryptography).*
Алгоритм шифрования (Encryption Algorithm)	Также называется «криптографическим алгоритмом» (cryptographic algorithm). Последовательность математических инструкций, используемых для преобразования незашифрованного текста или данных в зашифрованный текст или данные, и наоборот. См. *«Стойкая криптография» (Strong Cryptography).*
Организация (Entity)	Термин, используемый для обозначения корпорации, организации или предприятия, которые проходят проверку на соответствие PCI DSS.
Мониторинг целостности файлов (File Integrity Monitoring)	Метод или технология мониторинга определенных файлов или журналов аудита на предмет их изменений. При изменении критичных файлов или журналов соответствующим работникам, отвечающим за безопасность, должны отсылаться уведомления.
Шифрование на уровне файла (File-Level Encryption)	Метод или технология (программная или аппаратная) для шифрования всего содержимого определенных файлов. См. также *«Шифрование диска» (Disk Encryption)* или *«Шифрование базы данных на уровне столбцов» (Column-Level Database Encryption).*
FIPS	Аббревиатура — Federal Information Processing Standards (Федеральные стандарты обработки информации). Стандарты, которые официально признаны Федеральным правительством США; которые также предназначены для использования неправительственными учреждениями и подрядчиками.
Межсетевой экран (Firewall)	Аппаратная и (или) программная технология, которая защищает сетевые ресурсы от несанкционированного доступа. Межсетевой экран разрешает или запрещает трафик между сетями с различными уровнями безопасности на основе набора правил и других критериев.
Компьютерная экспертиза (Forensics)	В области информационной безопасности применение инструментов расследования и методов анализа для сбора доказательств из компьютерных ресурсов с целью определения причины компрометации данных.
FTP	Аббревиатура — File Transfer Protocol («протокол передачи файлов»). Сетевой протокол, который используется для передачи данных от одного компьютера другому через общедоступную сеть, такую как Интернет. FTP считается небезопасным протоколом, поскольку пароли и содержимое файлов передаются незащищенными и в виде незашифрованного текста. Для защиты FTP может использоваться технология SSH или какая-либо другая. См. *S-FTP*.

Термин	Определение
GPRS	Аббревиатура — General Packet Radio Service («технология пакетной радиосвязи общего пользования»). Служба мобильной связи, доступная пользователям мобильных телефонов GSM. Позволяет эффективно использовать ограниченную полосу пропускания сети. Обычно используется для передачи и получения небольших объемов данных, например, для чтения электронной почты или просмотра веб-страниц.
GSM	Аббревиатура — Global System for Mobile Communications (глобальная система мобильной связи). Популярный стандарт для мобильных телефонов и сетей. Повсеместное использование стандарта GSM привело к тому, что международный роуминг между операторами мобильной связи стал обычной практикой, что позволяет абонентам мобильной связи пользоваться своими телефонами во многих странах мира.
Хеширование (Hashing)	Процесс приведения ДДК к нечитаемому виду путем преобразования данных в сообщение фиксированной длины с использованием *«Стойкой криптографии» (Strong Cryptography).* Хеширование — это однонаправленная математическая функция, при использовании которой несекретный алгоритм преобразует сообщение любой длины в сообщение фиксированной длины (обычно это называется «хеш-код» или «дайджест сообщения»). Хеш-функция должна иметь следующие свойства: (1) вычислительно невозможно определить оригинальное исходное значение только по хеш-коду; (2) вычислительно невозможно найти два исходных значения, которые дают один и тот же хеш-код. В контексте PCI DSS хеширование должно применяться ко всему номеру PAN, чтобы он считался приведенным к нечитаемому виду. Рекомендуется, чтобы хешированные данные о держателях карт включали в себя вводную переменную для функции хеширования (например, «соль») для снижения или исключения успешности атак по предварительно вычисленным радужным таблицам (см. *«Вводная переменная» (Input Variable)*).
Хост (Host)	Основное аппаратное обеспечение компьютера, на котором исполняется ПО.

Термин	Определение
Поставщик услуг хостинга (Hosting Provider)	Организация, которая предлагает различные услуги ТСП и другим поставщикам услуг. Поставщики услуг хостинга оказывают как простые, так и сложные услуги: — от предоставления совместно используемого места на сервере и до полного спектра возможностей корзины покупок ("shopping cart"); — от платежных приложений до подключения к платежным шлюзам и процессинговым центрам; — от выделенного хостинга до выделенного клиенту сервера. Поставщиком услуг хостинга может быть поставщик услуг хостинга с общей средой, который размещает несколько организаций на одном сервере.
HSM	Аббревиатура — hardware security module («аппаратный модуль безопасности») Физически и логически защищенное аппаратное устройство, предоставляющее защищенный комплекс криптографических служб для управления ключами шифрования и (или) для расшифрования данных платежных карт.
HTTP	Аббревиатура — hypertext transfer protocol («протокол передачи гипертекста»). Открытый интернет-протокол для передачи данных в сети Интернет.
HTTPS	Аббревиатура — hypertext transfer protocol over secure socket layer («протокол передачи гипертекста поверх уровня защищенных сокетов»). Защищенный протокол HTTP, который обеспечивает аутентификацию и шифрование соединения в сети Интернет. Протокол разработан для критичного с точки зрения безопасности обмена данными, такого как вход в систему через веб-интерфейс.
Гипервизор (Hypervisor)	Программное или микропрограммное обеспечение для размещения и управления виртуальными машинами. Для целей PCI DSS системный компонент с функцией гипервизора также включает монитор виртуальных машин (VMM).
Идентификатор (ID)	Идентификатор определенного пользователя или определенного приложения.
СОВ (IDS)	Аббревиатура — система обнаружения вторжений (intrusion detection system). Программное или аппаратное обеспечение, которое используется для обнаружения аномалий или попыток вторжения в сеть или систему и оповещения об этом. СОВ состоит из следующих компонентов: — датчики, генерирующие события безопасности; — консоль для отслеживания событий и оповещений и управления датчиками; — центральный механизм, записывающий в базу данных события, зафиксированные датчиками. Использует систему правил для генерации оповещений при обнаружении событий безопасности. См. *СПВ (IPS)*

Термин	Определение
IETF	Аббревиатура — Internet Engineering Task Force («Специальная комиссия инженерии сети Интернет»). Открытое международное сообщество проектировщиков, операторов, поставщиков и исследователей сети, которое занимается развитием архитектуры сети Интернет и обеспечением ее бесперебойной работы. В этом сообществе отсутствует процедура официального приема в члены и в него может вступить любой желающий.
IMAP	Аббревиатура — Internet Message Access Protocol (сетевой протокол доступа к сообщениям). Сетевой протокол прикладного уровня, позволяющий почтовому клиенту получить доступ к электронным сообщениям на удаленном почтовом сервере.
Индексный маркер (Index Token)	Криптографическое значение, которое заменяет номер PAN, основанное на определенном индексе значений, не поддающихся вычислению.
Информационная безопасность (Information Security)	Защита информации для обеспечения конфиденциальности, целостности и доступности.
Информационная система (Information System)	Отдельный структурированный набор информационных ресурсов, организованный для сбора, обработки, обслуживания, использования, обмена, распространения или удаления информации.
Фильтрация входящего трафика (Ingress Filtering)	Метод фильтрации входящего сетевого трафика, при котором только явно разрешенный трафик может проникать в сеть.
Инъекции (Injection Flaws)	Уязвимость, возникающая в результате небезопасных методов программирования, выражающихся в некорректной проверке введенных данных, которая позволяет злоумышленникам передать в нижележащую систему вредоносный код через веб-приложение. Данный класс уязвимостей включает SQL-инъекцию, инъекцию LDAP и инъекцию XPath.
Вводная переменная (Input Variable)	Случайная строка, которая присоединяется к исходным данным перед применением однонаправленной хеш-функции. Вводные переменные могут снизить успешность атак по предварительно вычисленным радужным таблицам. См. также *«Хеширование» (Hashing)* и *«Радужные таблицы» (Rainbow Tables).*

Термин	Определение
Небезопасный протокол, служба или порт (Insecure Protocol/Service/Port)	Протокол, служба или порт, которые создают проблемы безопасности вследствие недостатков механизмов защиты конфиденциальности и (или) целостности. К таким проблемам безопасности относятся службы, протоколы или порты, которые: — передают данные или учетные данные для аутентификации (например, пароль или парольные фразы) в виде незашифрованного текста по сети Интернет; — позволяют легко воспользоваться уязвимостями, имеющимися в них по умолчанию или вследствие неправильной настройки. Примеры небезопасных сервисов, протоколов или портов включают, помимо прочих, FTP, Telnet, POP3, IMAP и SNMP версии 1 и 2.
IP	Аббревиатура — internet protocol («протокол сети Интернет»). Протокол сетевого уровня, содержащий данные об адресе и некоторую управляющую информацию, необходимую для маршрутизации и доставки пакетов от исходного хоста к хосту назначения. IP — основной протокол сетевого уровня, входящий в стек протоколов TCP/IP. См. *TCP*.
IP-адрес (IP Address)	Синоним: «адрес протокола сети Интернет» (internet protocol address). Числовой код, который уникально идентифицирует конкретный компьютер (хост) в сети Интернет.
Подмена IP-адреса (IP address spoofing)	Метод атаки, используемый для получения несанкционированного доступа к сетям или компьютерам. Злоумышленник направляет компьютеру ложные сообщения с IP-адресом, указывающим на доверенный хост в качестве источника сообщения.
СПВ (IPS)	Аббревиатура — система предотвращения вторжений (intrusion prevention system). СПВ дополняет СОВ механизмом блокирования попыток вторжения.
IPSEC	Сокращение — Internet Protocol Security («протокол безопасности сети Интернет»). Стандарт для защиты соединений по протоколу IP на сетевом уровне посредством шифрования и (или) аутентификации всех IP-пакетов в коммуникационной сессии.
ISO	Более известна как International Organization for Standardization («Международная организация по стандартизации»). Неправительственная организация, состоящая из сети национальных организаций по стандартизации.
Эмитент (Issuer)	Организация, которая выпускает платежные карты или оказывает, содействует в оказании или поддерживает услуги выпуска карт. К таким организациям относятся, среди прочего, банки-эмитенты и эмиссионные процессинговые центры. Синоним: «банк–эмитент» (issuing bank) или «финансовая организация – эмитент» (issuing financial institution).
Услуги выпуска (Issuing Services)	Примеры услуг выпуска включают, среди прочего: авторизацию и персонализацию карт.

Термин	Определение
LAN	Аббревиатура — локальная сеть (local area network). Это группа компьютеров и (или) других устройств, совместно использующих единые каналы связи, часто расположенных в пределах одного или нескольких зданий.
LDAP	Аббревиатура — Lightweight Directory Access Protocol («облегченный протокол доступа к каталогам»). Хранилище данных аутентификации и авторизации, используемое для запроса и изменения полномочий пользователей, а также для разрешения доступа к защищенным ресурсам.
Минимально необходимые права (Least Privilege)	Обладание правами доступа и (или) привилегиями, минимально необходимыми для выполнения ролей и должностных обязанностей.
Журнал (Log)	См. *«Журнал аудита» (Audit Log).*
LPAR	Сокращение — logical partition («логический раздел»). Система разделения совокупности ресурсов компьютера – процессоров, памяти и хранилища – на блоки меньшего размера, которые могут функционировать с их собственной отдельной копией ОС и приложений. Логическое разделение обычно применяется для обеспечения возможности использования различных ОС и приложений на одном устройстве. Разделы можно настроить таким образом, чтобы они могли или не могли взаимодействовать друг с другом или совместно использовать ресурсы сервера, например, сетевые интерфейсы.
MAC	В криптографии аббревиатура — message authentication code («код аутентификации сообщения»). Небольшая часть информации, используемая для аутентификации сообщения. См. *«Стойкая криптография» (Strong Cryptography).*
MAC-адрес (MAC address)	Сокращение — media access control address («адрес управления доступом к среде»). Уникальный идентификатор, который присваивается производителями сетевым адаптерам и сетевым интерфейсным картам.
Данные магнитной полосы (Magnetic-Stripe Data)	См. *«Данные треков» (Track Data).*
Мейнфрейм (Mainframe)	Компьютеры, которые предназначены для работы с очень большими объемами входных и выходных данных и которые обеспечивают высокую вычислительную мощность. Мейнфреймы могут обеспечить работу нескольких ОС на уровне полноценной работы нескольких компьютеров. Многие устаревшие системы имеют структуру мейнфрейма.

Термин	Определение
Вредоносное ПО (Malicious Software, Malware)	Программа или микропрограмма, разработанная для проникновения в компьютерную систему или ее повреждения без ведома или согласия ее владельца с целью нарушения конфиденциальности, целостности или доступности данных, приложений или операционной системы. Такое ПО обычно проникает в сеть при выполнении многих разрешенных бизнесом действий, что приводит к использованию уязвимостей системы. Примерами вредоносного ПО являются вирусы, черви, трояны, шпионское и рекламное ПО, руткиты.
Маскирование (Masking)	В контексте PCI DSS это метод сокрытия сегмента данных при отображении или печати. Маскирование используется, когда нет служебной необходимости просмотра полного номера PAN. Маскирование относится к защите номера PAN при его отображении на экране или печати. См. *«Усечение» (Truncation)* для получения информации о защите номера PAN при его хранении в файлах, базах данных и т. д.
Атаки сканирования содержимого памяти (Memory-Scraping Attacks)	Вредоносная активность по изучению и извлечению данных, находящихся в памяти при обработке, или данных, которые не были должным образом очищены или перезаписаны.
Торгово-сервисное предприятие, ТСП (Merchant)	В контексте PCI DSS торгово-сервисное предприятие — это организация, которая принимает платежные карты с логотипом любого из пяти членов Совета PCI SSC (American Express, Discover, JCB, MasterCard или Visa) для оплаты товаров и (или) услуг. Стоит учитывать, что ТСП, которое принимает платежные карты в качестве оплаты за товары и (или) услуги, может быть также поставщиком услуг, если предоставляемые услуги приводят к хранению, обработке или передаче ДДК по поручению других ТСП или поставщиков услуг. Например, интернет-провайдер — это ТСП, которое принимает платежные карты для ежемесячной оплаты счетов, но также является поставщиком услуг, если оно обслуживает ТСП как клиентов.
MO/TO	Аббревиатура — Mail-Order/Telephone-Order («обработка заказов по почте или по телефону»).
Мониторинг (Monitoring)	Использование систем или процессов для постоянного наблюдения за компьютерами или сетевыми ресурсами с целью уведомления персонала в случае сбоя в работе, поступления сигнала тревоги или наступления иных предопределенных событий.
MPLS	Аббревиатура — multi protocol label switching («многопротокольная коммутация по меткам»). Сетевой или телекоммуникационный механизм для объединения группы сетей с пакетной коммутацией.
NAC	Аббревиатура — network access control («контроль доступа к сети») или network admission control («контроль доступа в сеть»). Метод обеспечения безопасности на сетевом уровне путем предоставления доступа к сетевым ресурсам только конечным устройствам согласно заданной политике информационной безопасности.

Термин	Определение
NAT	Аббревиатура — network address translation («преобразование сетевых адресов»). Синоним: «трансляция IP-адресов» (network masquerading, IP masquerading). Смена IP-адреса, используемого в одной сети, на другой IP-адрес, известный в другой сети, позволяет организации использовать внутренние адреса, которые видны внутри сети, и внешние адреса, которые видны только за пределами сети.
Сеть	Два или более компьютеров, которые подключены друг к другу физически или через беспроводные технологии.
Администратор сети (Network Administrator)	Работник, ответственный за управление сетью в организации. Обязанности обычно включают, среди прочего: — обеспечение безопасности сети, — выполнение установок и обновлений, — обслуживание и мониторинг действий.
Сетевые компоненты (Network Components)	Включают, среди прочего: — межсетевые экраны, — коммутаторы, — маршрутизаторы, — беспроводные точки доступа, — устройства сетевой безопасности, — иные устройства безопасности.
Схема сети (Network Diagram)	Схема, на которой указаны системные компоненты и соединения в сетевом окружении.
Сканирование сети на наличие уязвимостей (Network Security Scan)	Процесс, позволяющий ручными или автоматизированными средствами выполнять удаленную проверку систем организации на наличие уязвимостей, который включает в себя тестирование внешних и внутренних систем, а также предоставление отчетов о службах, доступных по сети. Сканирование может выявлять уязвимости в ОС, службах и устройствах, которыми могут воспользоваться злоумышленники.
Сегментация сети (Network Segmentation)	Синонимы: сегментация (segmentation) или изоляция (isolation). Сегментация сети позволяет изолировать системные компоненты, которые используются для хранения, обработки или передачи ДДК, от других систем. С помощью надлежащей сегментации сети можно уменьшить размер среды ДДК и область оценки соответствия требованиям PCI DSS. См. раздел «Сегментация сети» в документе *«Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования и процедуры оценки безопасности»*. Сегментация сети не является требованием PCI DSS.
Перехват сетевого трафика (Network Sniffing)	Синонимы: «перехват» (sniffing) или «перехват пакетов» (packet sniffing). Метод пассивного мониторинга или сбора сетевых коммуникаций, декодирования протоколов и изучения содержимого на предмет наличия интересующей информации.

Термин	Определение
NIST	Аббревиатура — National Institute of Standards and Technology («Национальный институт стандартов и технологий»). Федеральное агентство, не осуществляющее надзорных функций, входящее в Управление по технологиям Министерства торговли США.
NMAP	ПО для сканирования в целях безопасности, которое сканирует сети и идентифицирует открытые порты в сетевых ресурсах.
Неконсольный административный доступ (Non-Console Administrative Access)	Логический административный доступ к системному компоненту через сетевой интерфейс, а не через прямое физическое подключение к системному компоненту. Неконсольный административный доступ включает в себя доступ как из локальных или внутренних сетей, так и из внешних или удаленных сетей.
Пользователи, не являющиеся клиентами (Non-Consumer Users)	Любые лица, исключая держателей карт, имеющие доступ к системным компонентам, включая, среди прочего: работников, администраторов и третьи стороны.
NTP	Аббревиатура — Network Time Protocol («сетевой протокол службы времени»). Сетевой протокол для синхронизации часов компьютерных систем, сетевых устройств и других системных компонентов.
NVD	Аббревиатура — National Vulnerability Database («Национальная база данных уязвимостей»). Хранилище данных правительства США о стандартизованном управлении уязвимостями. NVD включает базы данных, содержащие перечни контрольных вопросов по безопасности, уязвимости ПО, неверные конфигурации, названия продуктов и метрики воздействия.
OCTAVE®	Аббревиатура — Operationally Critical Threat, Asset, and Vulnerability Evaluation («оценка критичных угроз, активов и уязвимостей»). Набор средств, технологий и методов стратегической оценки и планирования риск-ориентированной информационной безопасности.
Серийный продукт (Off-the-Shelf)	Готовый к использованию продукт массового производства, который ни дорабатывался, ни разрабатывался для какого-то конкретного пользователя или заказчика.
Операционная система, ОС (Operating System, OS)	Программное обеспечение компьютерной системы, которое отвечает за управление и координацию всех операций и совместного использования компьютерных ресурсов. В качестве примера можно привести ОС Microsoft Windows, Mac OS, Linux и Unix.
Организационная независимость (Organizational Independence)	Структура организации, исключающая конфликт интересов между лицом или отделом, выполняющим работу, и лицом или отделом, эту работу оценивающим. Например, лица, выполняющие оценку, организационно независимы от руководства оцениваемой среды.

Термин	Определение
OWASP	Аббревиатура — Open Web Application Security Project («Открытый проект безопасности веб-приложений»). Некоммерческая организация, задача которой заключается в повышении безопасности прикладного ПО. OWASP ведет список критических уязвимостей для веб-приложений. (См. http://www.owasp.org).
PA-DSS	Аббревиатура — Payment Application Data Security Standard («Стандарт безопасности данных платежных приложений»).
PA-QSA	Аббревиатура — Payment Application Qualified Security Assessor («Сертифицированный аудитор безопасности платежных приложений»). PA-QSA сертифицированы Советом PCI SSC для проведения оценки платежных приложений на соответствие стандарту PA-DSS. См. подробную информацию о требованиях к компаниям PA-QSA и их работникам в документе PA-DSS Program Guide («Руководство по программе PA-DSS») и *PA-QSA Qualification Requirements («Требованиях к Сертифицированным аудиторам безопасности платежных приложений»)*.
Блокнот (Pad)	В криптографии одноразовый блокнот — это алгоритм шифрования, в котором текст объединен со случайно генерируемым ключом («блокнотом»), имеющим такую же длину, как незашифрованный текст и используемым только один раз. Кроме того, если ключ действительно является случайно генерируемым, не используется повторно и хранится в секрете, то этот алгоритм шифрования невозможно взломать.
PAN	Аббревиатура — primary account number («основной номер платежной карты»), синоним: «номер карты». Уникальный номер платежной карты (как правило, кредитной или дебетовой), который идентифицирует эмитента и соответствующий счет держателя карты.
Параметризованные запросы (Parameterized Queries)	Средство структурирования SQL-запросов для ограничения срабатывания экранирующих символов, и, таким образом, предотвращения инъекций кода.
Пароль, парольная фраза (Password, Passphrase)	Строка символов, которая служит для аутентификации пользователя.
PAT	Аббревиатура — Port Address Translation («преобразование портов в адреса»), синоним: «преобразование сетевых адресов на основе портов» (network address port translation). Тип технологии *NAT*, в которой также преобразуются и номера портов.
Обновление (Patch)	Обновление к существующей версии ПО для расширения функциональности или исправления дефектов.

Термин	Определение
Платежное приложение (Payment Application)	В контексте стандарта PA-DSS это приложение, которое хранит, обрабатывает или передает ДДК при выполнении авторизации или проведении расчетов, в случае продажи приложения, его распространения или лицензирования для третьих сторон. См. *дополнительную информацию в PA-DSS Program Guide* («Руководстве по программе PA-DSS»).
Платежные карты (Payment Cards)	Для целей PCI DSS это любая платежная карта или устройство с логотипом одного из основателей Совета PCI SSC: American Express, Discover Financial Services, JCB International, MasterCard Worldwide или Visa, Inc.
PCI	Аббревиатура — Payment Card Industry («индустрия платежных карт»).
PCI DSS	Аббревиатура — Payment Card Industry Data Security Standard («Стандарт безопасности данных индустрии платежных карт»).
PDA	Аббревиатура — personal data assistant или personal digital assistant («карманный персональный компьютер»). Карманные мобильные устройства, которые можно использовать для совершения и приема телефонных звонков, работы с электронной почтой или просмотра веб-страниц.
PED	Устройство ввода ПИН-кода (PIN entry device).
Тест на проникновение (Penetration Test)	При тестах на проникновение осуществляется попытка выявить способы использования уязвимостей для обхода или преодоления защитных механизмов системных компонентов. Тестирование на проникновение включает тестирование сети и приложений, а также защитных мер и процессов, связанных с сетями и приложениями, и осуществляется как из-за пределов среды (внешнее тестирование), так и изнутри среды.
Программный персональный межсетевой экран (Personal Firewall Software)	Программный продукт, представляющий собой межсетевой экран, установленный на отдельном компьютере.
Данные, идентифицирующие личность (Personally Identifiable Information)	Информация, которая может использоваться для идентификации или отслеживания личности лица, в том числе: его имя, адрес, номер страхового свидетельства, биометрические данные, дата рождения и т. д.
Работники (Personnel)	Работники, работающие как полный, так и неполный рабочий день, временные работники, подрядчики, консультанты, находящиеся на объекте организации или иным образом имеющие доступ к среде ДДК

Термин	Определение
ПИН	Аббревиатура — персональный идентификационный номер (personal identification number). Секретный пароль из цифр, известный только пользователю и системе и используемый для аутентификации пользователя в системе. Пользователю предоставляется доступ, только если ПИН-код, указанный пользователем, соответствует ПИН-коду в системе. Обычно ПИН-коды используются для получения наличных денег через банкомат. Другой тип ПИН-кода используется в картах с чипом EMV, где ПИН-код заменяет подпись держателя карты.
ПИН-блок (PIN Block)	Блок данных, используемый для инкапсуляции ПИН-кода при обработке. Формат ПИН-блока определяет содержимое ПИН-блока и порядок его обработки для извлечения ПИН-кода. ПИН-блок состоит из ПИН-кода, длины ПИН-кода и может содержать часть PAN.
POI	Аббревиатура — point of interaction («точка взаимодействия»), начальная точка, где данные считываются с карты. Будучи электронным устройством для осуществления транзакций, POI состоит из аппаратного и программного обеспечения и размещается в оборудовании для приема платежных карт, позволяя держателю карты выполнить транзакцию по карте. Работа с POI может выполняться как с участием, так и без участия пользователя. Транзакции через POI обычно представляют собой платежные транзакции с применением карты со встроенным чипом и (или) магнитной полосой.
Политика (Policy)	Совокупность установленных в организации правил, регламентирующих допустимое использование вычислительных ресурсов, практические меры по обеспечению безопасности и принципы разработки рабочих процедур.
POP3	Аббревиатура — Post Office Protocol v3 («почтовый протокол версии 3»). Протокол прикладного уровня, используемый почтовыми клиентами для получения электронных сообщений с удаленного сервера через подключение по протоколу TCP/IP.
Порт (Port)	Логические (виртуальные) точки подключения, связанные с определенным коммуникационным протоколом для обеспечения межсетевого обмена.
POS	Аббревиатура — point of sale («точка продаж»). Аппаратное и (или) программное обеспечение, которое используется для обработки транзакций с платежными картами на территории ТСП.
Частная сеть (Private Network)	Сеть организации, которая использует частное пространство IP-адресов. Частные сети обычно проектируются как локальные сети. Доступ к частной сети из общедоступных сетей должен быть надлежащим образом защищен с помощью межсетевых экранов и маршрутизаторов.
Привилегированный пользователь (Privileged User)	Любая учетная запись с правами доступа, превышающими базовые. Обычно такие учетные записи имеют больше прав, чем стандартная учетная запись. Однако объем прав разных привилегированных учетных записей может существенно различаться в зависимости от организации, должностных обязанностей или ролей и используемых технологий.

Термин	Определение
Процедура (Procedure)	Разъяснительная информация к политике. Процедура — это порядок действий и описание методов реализации политики.
Протокол (Protocol)	Согласованный метод обмена данными, используемый в сетях. Спецификация, описывающая правила и процедуры, которым должны следовать компьютерные продукты для выполнения операций в сети.
Прокси-сервер (Proxy Server)	Сервер, выступающий в качестве посредника между внутренней сетью и Интернетом. Например, одна из функций прокси-сервера — принимать или устанавливать соединения между внутренними и внешними узлами так, чтобы каждый отдельный узел обменивался данными только с прокси-сервером.
PTS	Аббревиатура — PIN Transaction Security («безопасность транзакций с использованием ПИН-кода»), PTS — это набор требований, контролируемых Советом PCI SSC, для модульной оценки POI-терминалов, принимающих ПИН-коды. См. www.pcisecuritystandards.org.
Общедоступная сеть (Public Network)	Сеть, созданная и управляемая поставщиком телекоммуникационных услуг с целью предоставления услуг передачи данных населению. При передаче через общедоступные сети данные могут быть перехвачены, изменены и (или) их маршрут может быть изменен. Примеры общедоступных сетей, на которые распространяется PCI DSS, включают, среди прочего, Интернет, беспроводные и мобильные технологии.
PVV	Аббревиатура — PIN verification value («значение проверки ПИН-кода»). Дискретное значение, записанное в магнитной полосе платежной карты.
QIR	Аббревиатура — Qualified Integrator or Reseller («сертифицированный интегратор или реселлер»). См. дополнительную информацию в *«Руководстве по программе QIR» (QIR Program Guide)*на сайте PCI SSC.
QSA	Аббревиатура — Qualified Security Assessor («сертифицированный аудитор безопасности»). QSA сертифицированы Советом PCI SSC для проведения оценки на соответствие стандарту PCI DSS на территории организаций. См. подробную информацию о требованиях к компаниям QSA и их работникам в разделе *«Требования к сертифицированным аудиторам безопасности» (QSA Qualification Requirements)*.
RADIUS	Аббревиатура — Remote Authentication Dial-In User Service («Служба аутентификации RADIUS»). Система аутентификации и учета. Проверяет правильность информации, такой как имя пользователя и пароль, которая поступает на сервер RADIUS, и затем предоставляет доступ к системе. Этот метод аутентификации может использоваться с токеном, смарт-картой и т. д. для обеспечения двухфакторной аутентификации.
Атака по радужным таблицам (Rainbow Table Attack)	Метод атаки с применением предварительно вычисленной таблицы хеш-строк (дайджестов сообщений фиксированной длины) для определения исходных данных, как правило, с целью взлома пароля или хешей ДДК.

Термин	Определение
Смена ключей (Re-keying)	Процесс смены криптографических ключей. Периодическая смена ключей ограничивает объем данных, зашифрованных одним ключом.
Удаленный доступ (Remote Access)	Доступ к компьютерным сетям из удаленного местоположения. Удаленный доступ может осуществляться как внутри сети организации, так и из удаленного местоположения за пределами сети организации. Примером технологии для удаленного доступа может быть *VPN*.
Удаленная лабораторная среда (Remote Lab Environment)	Лаборатория, которая не находится в ведении организации, имеющей статус PA-QSA.
Съемные электронные носители (Removable Electronic Media)	Носители, которые содержат цифровые данные и которые можно легко извлечь и (или) переместить с одной компьютерной системы на другую. Например, к таким носителям относятся CD и DVD-диски, USB-накопители и съемные жесткие диски.
Реселлер, интегратор (Reseller, Integrator)	Организация, которая продает и (или) интегрирует платежные приложения, но не разрабатывает их.
RFC 1918	Стандарт, разработанный Специальной комиссией инженерии сети Интернет (IETF), который определяет использование и соответствующие диапазоны адресов для частных (не маршрутизируемых в сети Интернет) сетей.
Анализ рисков, оценка рисков (Risk Analysis, Risk Assessment)	Процесс, при котором: — выявляются значимые системные ресурсы и угрозы; — измеряется предполагаемый (потенциальный) ущерб на основе предполагаемой частоты реализации угрозы и расходов, в случае ее реализации; — (опционально) вырабатываются рекомендации по распределению ресурсов на защитные меры с целью повышения уровня защищенности.
Ранжирование рисков (Risk Ranking)	Определенный критерий измерения уровня риска на основании оценки и анализа рисков в определенной организации.
Отчет о соответствии (ROC, Report on Compliance)	Отчет, в котором содержатся подробные сведения о результатах оценки организации на соответствие стандарту PCI DSS.
Руткит (Rootkit)	Тип вредоносного ПО, которое при несанкционированной установке может скрыть свое присутствие и получить административный контроль над компьютерной системой.

Термин	Определение
Маршрутизатор (Router)	Аппаратное или программное обеспечение, которое соединяет две или более сетей. Маршрутизатор выполняет функции сортировщика и интерпретатора, просматривая адреса и передавая пакеты данных по соответствующим адресам назначения. Программные маршрутизаторы иногда называют шлюзами.
Отчет о проверке (ROV, Report on Validation)	Отчет, в котором содержатся подробные сведения о результатах оценки на соответствие стандарту PA-DSS в рамках программы PA-DSS.
RSA	Алгоритм шифрования с открытым ключом, описанный в 1977 г. Рональдом Ривестом (Ron Rivest), Ади Шамиром (Adi Shamir) и Леонардом Адлеманом (Len Adleman) из Массачусетского технологического института (МТИ). Аббревиатура RSA — это инициалы их фамилий.
S-FTP	Аббревиатура — Secure-FTP («безопасное FTP-соединение»). S-FTP позволяет шифровать при передаче аутентификационную информацию и файлы данных. См. *FTP.*
Выборка (Sampling)	Процесс выборки элементов группы, которые репрезентативно отражают всю группу. Выборка может использоваться аудиторами для снижения объема тестирования, если подтверждено, что в организации централизованно установлены стандартные операционные и защитные процессы и механизмы выполнения требований PCI DSS. Выборка не является требованием PCI DSS.
SANS	Аббревиатура — SysAdmin, Audit, Networking and Security («Системное администрирование, аудит, сетевые технологии и безопасность»), институт, который предоставляет услуги обучения и профессиональной сертификации в области компьютерной безопасности. (См. www.sans.org).
ОЛС (SAQ)	Аббревиатура — Опросный лист для самооценки (Self-Assessment Questionnaire). Инструмент составления отчета, применяемый для документирования результатов самооценки организации на соответствие стандарту PCI DSS.
Схема (Schema)	Формализованное описание архитектуры базы данных, включая организацию элементов данных.
Определение области оценки (Scoping)	Процесс идентификации всех системных компонентов, людей и процессов, подлежащих включению в область оценки соответствия требованиям PCI DSS. Первым этапом выполнения оценки соответствия требованиям PCI DSS является точное определение области оценки.
SDLC	Аббревиатура — system development life cycle («жизненный цикл разработки системы») или software development lifecycle («жизненный цикл разработки ПО»). Этапы разработки ПО или компьютерной системы, которые включают планирование, анализ, проектирование, тестирование и внедрение.

Термин	Определение
Безопасное программирование (Secure Coding)	Процесс создания и внедрения приложений, которые обладают устойчивостью к компрометации и (или) вмешательству в работу приложения.
Защищенное криптографическое устройство (Secure Cryptographic Device)	Набор аппаратных, программных и микропрограммных средств, реализующих криптографические процессы (включая криптографические алгоритмы и генерацию ключей), которые содержатся в определенных криптографических границах. К защищенным криптографическим устройствам относятся аппаратные и (или) хост-модули безопасности (HSM) и POI-терминалы, утвержденные согласно PCI PTS.
Безопасное стирание данных (Secure Wipe)	Другое название — безопасное удаление. Метод перезаписи данных на жестком диске или другом цифровом носителе, исключающий возможность восстановления данных.
Событие безопасности (Security Event)	Событие, которое рассматривается организацией как потенциально воздействующее на безопасность системы или среды. В контексте PCI DSS события безопасности указывают на подозрительные или аномальные действия.
Специалист по безопасности (Security Officer)	Главное лицо, отвечающее за обеспечение безопасности организации.
Политика безопасности (Security Policy)	Набор норм, правил и рекомендаций, устанавливающих порядок управления, защиты и распространения критичной информации в организации.
Протоколы безопасности (Security Protocols)	Сетевые коммуникационные протоколы, разработанные для защиты передачи данных. Примеры протоколов безопасности включают, в том числе: SSL/TLS, IPSEC, SSH, HTTPS и другие.
Критичные помещения (Sensitive Area)	Любые центр обработки данных, серверная комната или другое помещение, в которых расположены системы, хранящие, обрабатывающие или передающие ДДК. Исключением являются места, где присутствуют только POS-терминалы, например, кассовые зоны розничных магазинов.
Критичные аутентификационные данные, КАД (Sensitive Authentication Data)	Данные, связанные с обеспечением безопасности (включая, среди прочего: коды и значения проверки подлинности карт, полные данные треков (с магнитной полосы или ее эквивалента на чипе), ПИН-коды и ПИН-блоки) и используемые для аутентификации держателей карт и (или) авторизации транзакций с платежной картой.
Разделение полномочий (Separation Of Duties)	Практика распределения этапов выполнения какой-либо функции между различными людьми для исключения возможности нарушения процесса одним человеком.
Сервер (Server)	Компьютер, который предоставляет службы другим компьютерам, такие как обработка данных, хранение файлов или доступ к принтеру. Серверы включают, среди прочего: веб-серверы, серверы баз данных, серверы приложений, серверы аутентификации, DNS-серверы, почтовые серверы, прокси-серверы и серверы NTP.

Термин	Определение
Сервисный код (Service Code)	Трех- или четырехзначное число на магнитной полосе карты, которое в данных треков следует за датой истечения срока действия платежной карты. Сервисный код используется в различных целях, например, для определения сервисных атрибутов, разграничения между местными и международными комиссиями за проведение транзакций по карте или для определения ограничений использования.
Поставщик услуг (Service Provider)	Организация (кроме международных платежных систем), непосредственно вовлеченная в процесс обработки, хранения или передачи ДДК от имени другой организации. К поставщикам услуг относятся также организации, предоставляющие услуги, которые контролируют или могут влиять на безопасность ДДК. К таким организациям, например, относятся поставщики управляемых услуг (managed service provider, MSP), предоставляющие услуги по межсетевому экранированию, обнаружению вторжений и прочие услуги, а также поставщики услуг хостинга и другие организации. Если организация предоставляет услуги, включающие *только* предоставление доступа к общедоступной сети (например, телекоммуникационная компания, предоставляющая только коммуникационное соединение), то такая организация не считается поставщиком услуг в отношении таких услуг (хотя и может считаться поставщиком других услуг).
SHA-1, SHA-2	Аббревиатура — Secure Hash Algorithm («безопасный алгоритм хеширования»). Представляет собой семейство или набор соответствующих криптографических хеш-функций, включая алгоритмы SHA-1 и SHA-2. См. *«Стойкая криптография» (Strong Cryptography).*
Смарт-карта (Smart Card)	Синонимы: «чиповая карта» (chip card) или «карта с микропроцессором» (integrated circuit card). Тип платежной карты, которая имеет встроенный микропроцессор. Микропроцессор (т. н. чип), содержит данные платёжной карты, включая, среди прочих, данные, эквивалентные данным магнитной полосы.
SNMP	Аббревиатура — Simple Network Management Protocol («простой протокол управления сетью»). Поддерживает мониторинг устройств, подключенных к сети, на предмет появления состояний, требующих внимания администратора.
Разделение знания (Split Knowledge)	Метод, при использовании которого две или более стороны раздельно владеют компонентами одного ключа, которые по отдельности не дают знания результирующего криптографического ключа.
Шпионское ПО (Spyware)	Тип вредоносного ПО, которое при установке перехватывает или получает частичный контроль над компьютером пользователя без согласия пользователя.
SQL	Аббревиатура — Structured Query Language («язык структурированных запросов»). Компьютерный язык, который используется для создания, изменения и извлечения данных из систем управления реляционными базами данных.

Термин	Определение
SQL-инъекция (SQL Injection)	Тип атаки на веб-сайт с базой данных. Злоумышленник выполняет несанкционированные команды SQL, применяя их к небезопасному коду в системе, подключенной к сети Интернет. SQL-инъекции используются для кражи из базы данных информации, к которой при обычных условиях отсутствует доступ, и (или) для получения доступа к хост-машинам организации через компьютер, на котором размещена база данных.
SSH	Сокращение — Secure Shell («безопасная оболочка»). Набор протоколов, которые обеспечивают шифрование для сетевых служб, таких как удаленный вход в систему или удаленная передача файлов.
SSL	Аббревиатура — Secure Sockets Layer («уровень защищенных сокетов»). Общепринятый отраслевой стандарт шифрования канала связи между веб-браузером и веб-сервером, которое обеспечивает конфиденциальность и достоверность данных, передаваемых по этому каналу. См. *TLS.*
Динамическая пакетная фильтрация с запоминанием состояния (Stateful Inspection).	Синоним: «динамическая фильтрация пакетов» (dynamic packet filtering). Это функция межсетевого экрана, которая обеспечивает повышенную безопасность, отслеживая состояние сетевых соединений. Межсетевой экран, запрограммированный отличать закономерные пакеты для различных соединений, будет разрешать только пакеты, соответствующие установленному соединению, и запрещать все остальные.
Стойкая криптография (Strong Cryptography)	Криптография, основанная на: — протестированных и принятых в отрасли алгоритмах, — использовании ключей надлежащей длины (с эффективной длиной ключа не менее 112 бит), — надлежащих методах управления ключами. Криптография — это метод защиты данных, который включает как шифрование (которое обратимо), так и хеширование (которое необратимо, то есть является однонаправленным). Примерами протестированных и принятых в отрасли стандартов и алгоритмов минимально допустимой стойкости шифрования на момент публикации являются: — AES (128 бит или больше), — TDES (ключи, как минимум, тройной длины) — RSA (2048 бит и больше), — ECC (160 бит и больше); — ElGamal (2048 бит и больше). Для получения дополнительных инструкций по стойкости криптографических ключей и алгоритмам см. специальное издание NIST 800-57, часть 1 (http://csrc.nist.gov/publications/).
Системный администратор (SysAdmin)	Лицо, обладающее расширенными полномочиями и несущее ответственность за управление компьютерной системой или сетью.

Термин	Определение
Системные компоненты (System Components)	Любые сетевые устройства, серверы, вычислительные устройства или приложения, которые являются частью среды ДДК или подключены к ней.
Объект системного уровня (System-Level Object)	Любой элемент системного компонента, необходимый для его функционирования, включая, среди прочего, таблицы баз данных, хранимые процедуры, исполняемые и конфигурационные файлы приложения, конфигурационные файлы системы, статические и совместно используемые библиотеки (в т.ч. динамические — DLL), исполняемые файлы системы, драйверы и конфигурационные файлы устройств, а также дополнительные сторонние компоненты.
TACACS	Аббревиатура — Terminal Access Controller Access Control System («система управления доступом к контроллеру терминального доступа»). Протокол удаленной аутентификации, обычно используемый в сетях при обмене данными между сервером удаленного доступа и сервером аутентификации для определения прав доступа пользователя к сети. Этот метод аутентификации может использоваться с токеном, смарт-картой и т. д. для обеспечения двухфакторной аутентификации.
TCP	Аббревиатура — Transmission Control Protocol («протокол управления передачей»). Один из базовых протоколов транспортного уровня стека протоколов TCP/IP, а также базовый язык коммуникации или протокол Интернета. См. *IP*.
TDES	Аббревиатура — Triple Data Encryption Standard («стандарт трехкратного применения алгоритма DES к шифруемым данным»). Также называется 3DES или Triple DES. Алгоритм блочного шифрования, основанный на алгоритме DES путем трехкратного его применения. См. *«Стойкая криптография» (Strong Cryptography).*
TELNET	Аббревиатура — telephone network protocol («протокол телефонной сети»). Обычно используется для предоставления пользователям сеансов доступа через командную строку к устройствам в сети. Учетные данные пользователя передаются в виде незашифрованного текста.
Угроза (Threat)	Состояние или действие, при котором данные или ресурсы, обрабатывающие данные, могут быть намеренно или непреднамеренно потеряны, изменены, раскрыты, сделаны недоступными либо подвержены иному влиянию с ущербом для организации.
TLS	Аббревиатура — Transport Layer Security («безопасность транспортного уровня»). Протокол предназначен для обеспечения конфиденциальности и целостности данных между двумя взаимодействующими приложениями. TLS является преемником протокола SSL.
Токен (Token)	В контексте аутентификации и контроля доступа токен является значением, предоставляемым оборудованием или программным обеспечением, которое работает с сервером аутентификации или сетью VPN для выполнения динамической или двухфакторной аутентификации. См. *RADIUS, TACACS* и *VPN.*

Термин	Определение
Данные треков (Track Data)	Синонимы: «полные данные треков» (full track data) или «данные магнитной полосы» (magnetic-stripe data). Данные, записанные на магнитной полосе или чипе, которые используются для аутентификации и (или) авторизации при платежных транзакциях. Это может быть образ магнитной полосы на чипе или данные трека 1 и (или) трека 2 на магнитной полосе.
Данные транзакции (Transaction Data)	Данные, относящиеся к электронным транзакциям с платежными картами.
Троян (Trojan)	Синоним: «программа типа троянский конь» (Trojan horse). Тип вредоносного ПО, которое при установке разрешает пользователю выполнять обычные функции, в то время как троян выполняет вредоносные функции в компьютерной системе без ведома пользователя.
Усечение (Truncation)	Метод приведения полного номера PAN к нечитаемому виду посредством удаления сегмента номера PAN без возможности восстановления. Усечение относится к защите номера PAN при *хранении* в файлах, базах данных и т. д. См. *«Маскирование» (Masking)* для получения информации о защите номера PAN при его *отображении* на экранах, печати на бумажных квитанциях и т.п.
Доверенная сеть (Trusted Network)	Сеть организации, которая находится под контролем или управлением организации.
Двухфакторная аутентификация (Two-Factor Authentication)	Порядок аутентификации пользователя, при котором проверяются не менее двух факторов. В числе этих факторов: — обладание предметом (например, аппаратным или программным токеном); — обладание информацией (например, паролем, парольной фразой или ПИН-кодом); — обладание параметрами или навыками (например, отпечатками пальцев или другими биометрическими параметрами).
Недоверенная сеть (Untrusted Network)	Сеть, которая является внешней по отношению к сетям, принадлежащим организации, и которая не может контролироваться или управляться организацией.
URL	Аббревиатура — Uniform Resource Locator («унифицированный указатель ресурсов»). Текстовая строка определенного формата, используемая веб-браузерами, почтовыми клиентами и другими программами для идентификации сетевого ресурса в Интернете.

Термин	Определение
Методология присвоения версий (Versioning Methodology)	Процесс присвоения схем нумерации версий для уникальной идентификации определенного состояния приложения или программного обеспечения. Такие схемы включают формат нумерации версий, правила применения формата нумерации версий и любой подстановочный знак, определяемый производителем программного обеспечения. Номера версий обычно присваиваются в порядке возрастания и соответствуют определенным изменениям в программном обеспечении.
Виртуальное устройство (Virtual Appliance, VA)	Виртуальное устройство моделирует предустановленное устройство для выполнения определенного набора функций и запускается как исполняемая задача. Часто существующее сетевое устройство, например, маршрутизатор, коммутатор или межсетевой экран, виртуализируется для запуска в качестве виртуального устройства.
Виртуальный гипервизор (Virtual Hypervisor)	См. *«Гипервизор» (Hypervisor)*.
Виртуальная машина (Virtual Machine)	Автономная операционная среда, которая функционирует как отдельный компьютер. Она также называется «гостевой ОС», которая работает поверх гипервизора.
Монитор виртуальных машин (Virtual Machine Monitor, VMM)	Монитор виртуальных машин входит в состав гипервизора. Это программное обеспечение, которое реализует аппаратную абстракцию виртуальной машины. Монитор виртуальной машины управляет процессором, памятью и другими ресурсами системы, выделяя их для каждой гостевой ОС в соответствии с ее потребностями.
Виртуальный платежный терминал (Virtual Payment Terminal)	Виртуальный платежный терминал обеспечивает доступ через веб-браузер к сайту эквайрера, процессингового центра или стороннего поставщика услуг для авторизации транзакций с платежной картой, где ввод данных с платежных карт выполняется ТСП вручную через защищенное подключение веб-браузера. В отличие от физических терминалов, виртуальные платежные терминалы не считывают данные непосредственно с платежной карты. Поскольку транзакции с платежной картой выполняются вручную, виртуальные платежные терминалы обычно используются вместо физических терминалов в средах ТСП с низкими объемами транзакций.
Виртуальный коммутатор или маршрутизатор (Virtual Switch, Virtual Router)	Виртуальный коммутатор или маршрутизатор — это логический объект, который выполняет функции коммутации и маршрутизации данных на уровне сетевой инфраструктуры. Виртуальный коммутатор — это такая же неотъемлемая часть виртуализированной серверной платформы, как драйвер гипервизора или (подключаемый) модуль.

Термин	Определение
Виртуализация (Virtualization)	Виртуализация — это логическое абстрагирование вычислительных ресурсов от физических ограничений. Одной из типовых абстракций является виртуальная машина, на которой размещено содержимое одной физической машины и которая позволяет ему работать на другом физическом аппаратном обеспечении и (или) вместе с другими виртуальными машинами на одном физическом оборудовании. Кроме виртуальных машин, виртуализация может выполняться в отношении множества других вычислительных ресурсов, таких как приложения, настольные компьютеры, сети и системы хранения.
Виртуальная локальная сеть (VLAN)	Аббревиатура — virtual LAN или virtual local area network («виртуальная локальная сеть»). Логическая локальная сеть, которая выходит за пределы одной традиционной физической локальной сети.
VPN	Аббревиатура — virtual private network («виртуальная частная сеть»). Компьютерная сеть, в которой некоторые подключения являются виртуальными каналами внутри более крупных сетей, таких как сеть Интернет, а не прямыми подключениями по физическим проводам. В таких случаях говорится, что конечные точки виртуальной сети туннелируются через более крупную сеть. Несмотря на то, что основная сфера применения таких сетей – обеспечение безопасного обмена данными через общедоступную сеть Интернет, VPN может как обладать, так и не обладать функциями обеспечения усиленной безопасности, такими как аутентификация или шифрование содержимого. VPN может использоваться с токеном, смарт-картой и т. д. для обеспечения двухфакторной аутентификации.
Уязвимость (Vulnerability)	Недостаток или слабое место, которое при использовании может привести к умышленной или неумышленной компрометации системы.
WAN	Аббревиатура — wide area network («глобальная сеть»). Компьютерная сеть, охватывающая большую область, часто это региональная компьютерная система или система масштаба компании.
Веб-приложение (Web Application)	Приложение, доступ к которому обычно осуществляется через веб-браузер или веб-службы. Веб-приложения могут быть доступны в сети Интернет или в частной, внутренней сети.
Веб-сервер (Web Server)	Компьютер, на котором установлена программа, принимающая HTTP-запросы от веб-клиентов и предоставляющая HTTP-ответы (обычно веб-страницы).
WEP	Аббревиатура — Wired Equivalent Privacy («безопасность, аналогичная защите проводных сетей»). Слабый алгоритм шифрования, используемый для беспроводных сетей. Эксперты обнаружили ряд значительных недостатков этого алгоритма. Как выяснилось, защиту на базе этого алгоритма можно взломать с использованием доступного ПО за несколько минут. См. *WPA.*

Термин	Определение
Подстановочный знак (Wildcard)	Знак, который можно заменить определенным подмножеством возможных знаков в схеме нумерации версий приложения. В контексте PA-DSS подстановочный знак может использоваться для обозначения изменения, не влияющего на функции безопасности. Подстановочный знак является единственным переменным элементом схемы нумерации версий и используется для обозначения незначительных изменений, не влияющих на безопасность, между каждой версией, обозначаемой подстановочным знаком.
Беспроводная точка доступа (Wireless Access Point)	Также обозначается как AP. Устройство, с помощью которого беспроводные коммуникационные устройства подключаются к беспроводной сети. Обычно беспроводная точка доступа подключается к проводной сети и может передавать данные между беспроводными и проводными устройствами в сети.
Беспроводные сети (Wireless Networks)	Сети, которые соединяют компьютеры без физического подключения к кабелю.
WLAN	Аббревиатура — wireless local area network («беспроводная локальная сеть»). Локальная сеть, которая связывает два или более компьютеров или устройств без использования кабеля.
WPA, WPA2	Аббревиатура — WiFi Protected Access («защищенный доступ WiFi»). Протокол безопасности, созданный для защиты беспроводных сетей. WPA является преемником протокола WEP. WPA2 — это новое поколение технологии WPA.