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

Глоссарий. Основные определения, аббревиатуры и сокращения

Версия 2.0

Октябрь 2010 г.

БЛАГОДАРНОСТЬ:

PCI SSC благодарит Центральный банк Российской Федерации и Некоммерческое партнерство "Сообщество пользователей стандартов по информационной безопасности АБИСС" (НП "АБИСС") за поддержку, оказанную при подготовке перевода настоящего документа.

Английская версия этого документа является окончательной для всех целей и считается официальной версией. В случае каких-либо неоднозначностей или противоречий между текстом этого документа и английским текстом английский текст имеет преимущественное значение.

Термин	Определение
Авторизация (Authorization)	Предоставление доступа или других прав пользователю, программе или процессу. Если речь идет о сети, авторизация определяет, что человек (персона) или программа может делать после успешной аутентификации. Для целей проведения транзакции с платежной картой авторизация выполняется, когда торгово-сервисное предприятие получает одобрение транзакции, после того как эквайер подтверждает транзакцию с эмитентом/процессинговой системой.
Администратор базы данных (Database Administrator)	Также обозначается как "DBA". Специалист, ответственный за управление и администрирование баз данных.
Администратор сети (Network Administrator)	Лицо, ответственное за управление сетью в организации. Обязанности обычно включают, но не ограничиваются: обеспечение безопасности сети, выполнение установок и обновлений, обслуживание и мониторинг активности.
Алгоритм шифрования (Encryption Algorithm)	Последовательность математических инструкций, используемых для преобразования незашифрованного текста или данных в зашифрованный текст или данные, и наоборот. См. *Стойкая криптография.*
Анализ рисков / Оценка рисков (Risk Analysis / Risk Assessment)	Процесс, который выявляет угрозы и значимые системные ресурсы; измеряет ожидаемые потери (потенциальные потери) на основе ожидаемой частоты и стоимости события; и (опционально) вырабатывает рекомендации по выбору для каждого ресурса системы соответствующих защитных мер с целью сокращения общих потерь.
Антивирус (Anti-Virus)	Программа или программное обеспечение для обнаружения, удаления и защиты от различных форм вредоносных программ, таких как вирусы, черви, трояны, шпионское и рекламное ПО, руткиты.
Аутентификация (Authentication)	Процесс проверки подлинности человека (персоны), устройства или процесса. Обычно выполняется посредством использования одного или нескольких аутентификационных факторов, таких как: ▪ То, что вы знаете (например, пароль или парольная фраза) ▪ То, что у вас есть (например, ключи или смарт-карты) ▪ То, что вы есть (например, биометрические параметры)
База данных (Database)	Структурированная форма для упорядочивания и удобного извлечения данных. Простейшими примерами базы данных являются таблицы и электронные таблицы.
Безопасное программирование (Secure Coding)	Процесс создания и внедрения приложений, которые обладают устойчивостью к компрометации.
Безопасное стирание данных (Secure Wipe)	Также называется безопасным удалением; программная утилита, которая используется для безвозвратного удаления определенных файлов из компьютерной системы.
Беспроводная сеть (Wireless Networks)	Сеть, которая соединяет компьютеры без использования кабелей.

Термин	Определение
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.
Блокнот (Pad)	В криптографии одноразовый блокнот — это криптографический алгоритм, в котором текст объединен со случайно генерируемым ключом, который имеет такую же длину, как незашифрованный текст, и используется только один раз. Если ключ действительно является случайно генерируемым, не используется повторно и хранится в секрете, то этот алгоритм шифрования имеет высшую степень надежности
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 запросы HTTP от веб-клиентов и предоставляющая HTTP-ответы (обычно веб-страницы).
Виртуализация (Virtualization)	Виртуализация — это логическое абстрагирование вычислительных ресурсов от физических ограничений. Одной из таких абстракций является виртуальная машина, на которой размещено содержимое физической машины и которая может работать вместе с другими виртуальными машинами на одном физическом оборудовании. Кроме виртуальных машин, виртуализация может выполняться на других вычислительных ресурсах, таких как приложения, настольные компьютеры, сети и системы хранения.
Виртуальная машина (Virtual Machine)	Автономная операционная среда, которая функционирует как отдельный компьютер. Она также называется "гостевой операционной системой", которая работает поверх гипервизора.
Виртуальное устройство	Виртуальное устройство выполняет определенный набор функций, управление им осуществляется как рабочей нагрузкой. Часто существующее сетевое устройство, например маршрутизатор, коммутатор или межсетевой экран, виртуализируется для работы в качестве виртуального устройства.
Виртуальный гипервизор (Virtual Hypervisor)	См. *Гипервизор*.
Виртуальный коммутатор или маршрутизатор	Виртуальный коммутатор или маршрутизатор — это логический объект, который выполняет функции коммутации и маршрутизации данных на уровне сетевой инфраструктуры. Виртуальный коммутатор — это неотъемлемая часть виртуализированной серверной платформы, как драйвер гипервизора, модуль или подключаемый модуль.

Термин	Определение
Виртуальный терминал	Виртуальный терминал обеспечивает доступ через веб-интерфейс к сайту банка-эквайера, процессинговой системы или стороннего поставщика услуг для авторизации операций с платежной картой, где ввод данных о держателе карт выполняется вручную через защищенный веб-браузер. В отличие от физических терминалов, виртуальные терминалы не считывают данные непосредственно с платежной карты. Поскольку операции с платежной картой выполняются вручную, виртуальные терминалы обычно используются вместо физических терминалов в средах торгово-сервисных предприятий с низкими объемами транзакций.
Вредоносное ПО (Malicious Software / Malware)	Программное обеспечение, разработанное для проникновения в компьютерную систему или ее повреждения без ведома или согласия ее владельца. 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.
Выборка (Sampling)	Процесс выборки элементов группы, которые репрезентативно отражают всю группу. Выборка может использоваться аудиторами для минимизации усилий по тестированию, если известно, что организация имеет в наличии стандартные процессы и механизмы обеспечения безопасности. Выборка не является требованием стандарта PCI DSS.
Гипервизор (Hypervisor)	Программное или микропрограммное обеспечение для размещения и управления виртуальными машинами. Для целей PCI DSS гипервизор также включает монитор виртуальной машины (VMM).
Данные магнитной полосы (Magnetic-Stripe Data)	Также называются "данными дорожки". Данные, записанные на магнитной полосе или чипе, которые используются для аутентификации или авторизации при платежных транзакциях. Это может быть изображение магнитной полосы на чипе или данные дорожки 1 и/или дорожки 2 на магнитной полосе.
Данные о держателе карты - ДДК (Cardholder Data)	Данные о держателе карты включают в себя как минимум полный номер PAN. Данные о держателе карты также могут быть представлены в виде сочетания полного номера PAN с: именем держателя карты, датой истечения срока действия карты и/или сервисным кодом. См. *Критичные аутентификационные данные*, чтобы узнать о дополнительных элементах данных, которые можно передавать или обрабатывать (но не хранить) в процессе выполнения платежной транзакции.
Данные платежных карт (Account Data)	Данные платежных карт включают в себя данные о держателе карты и критичные аутентификационные данные См. *Данные о держателе карты* и *Критичные аутентификационные данные*
Данные транзакции (Transaction Data)	Данные, относящиеся к электронным транзакциям с использованием платежных карт.
Данные, идентифицирующие личность (Personally Identifiable Information)	Информация, которая может использоваться для идентификации лица, включая, но не ограничиваясь: его имя, адрес, номер страхового свидетельства, телефонный номер и т. д.

Термин	Определение
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, используемых при транзакциях, имеющих уязвимости. Лицо не допускается к материалам (например, к ключу шифрования) и работе с ними без присутствия другого лица (лиц). Для создания ключа вручную, передачи его другим лицам, а также для его загрузки, хранения и извлечения в соответствии с принципом двойного контроля необходимо, чтобы каждому субъекту был известен только компонент ключа. (См. также *Разделенные знания*).
Двухфакторная аутентификация (Two-Factor Authentication)	Метод аутентификации пользователя, при котором проверяются два или более факторов. В числе этих факторов то, что у пользователя есть (например, токен), то, что пользователь знает (например, пароль, парольная фраза или PIN-код) или то, что он из себя представляет или что он делает (например, отпечатки пальцев и другие биометрические параметры).
Держатель карты	Клиент, на имя которого выпущена платежная карта, или любой пользователь, который имеет право пользоваться платежной картой.
Динамическая фильтрация пакетов (Dynamic Packet Filtering)	См. *Проверка с сохранением состояния.*
Доверенная сеть (Trusted Network)	Сеть организации, которая может контролироваться или управляться ею.
Журнал (Log)	См. *Журнал аудита.*
Журнал аудита (Audit Log)	Также называется "журналом регистрации событий". Перечень записей действий в системе в хронологическом порядке. Журнал предоставляет возможность независимого анализа записей, достаточного для восстановления, изучения и анализа последовательности состояний и действий, связанных с операцией, процедурой или событием в транзакции от начала ее выполнения и до завершения.
Журнал регистрации событий (Audit Trail)	См. *Журнал аудита.*
Замена ключей (Re-keying)	Процесс замены криптографических ключей. Периодическая замена ключей ограничивает объем данных, которые можно зашифровать с помощью одного ключа.
Идентификатор (ID)	Идентификатор пользователя или приложения.
Индексный маркер (Index Token)	Криптографический параметр, который заменяет номер PAN на основе заданного индекса для получения непредсказуемого значения.
Информационная безопасность (Information Security)	Защита информации для обеспечения конфиденциальности, целостности и доступности.
Информационная система (Information System)	Структурированный набор информационных ресурсов, организованный для сбора, обработки, обслуживания, использования, обмена, распространения или удаления данных.

Термин	Определение
Клиент (Consumer)	Человек (персона), который приобретает товары и/или пользуется услугами.
Ключ (Key)	В криптографии ключ – это значение, определяющее результаты исключения криптографического алгоритма при преобразовании открытого текста в зашифрованный. Сложность дешифрования шифрованного текста в исходное сообщение в основном определяется длиной ключа. См. *Стойкая криптография.*
Код или значение проверки подлинности карты (Card Verification Code or Value)	Также известен как код или значение подтверждения подлинности карты или код безопасности. Обозначает следующее: (1) данные магнитной полосы, или (2) напечатанные элементы обеспечения безопасности. (1) Элемент данных магнитной полосы карты, использующий алгоритм шифрования для защиты целостности данных магнитной полосы и предохраняющий карту от изменения и подделки. В зависимости от платежной системы существуют следующие коды проверки подлинности карты: CAV, CVC, CVV или CSC. Ниже приведены термины для различных международных платежных систем: ▪ **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 это последние три цифры (справа от номера кредитной карты), напечатанные на полосе для подписи на оборотной стороне карты. Код проверки подлинности карт American Express — это четыре неэмбоссированные цифры над номером карты на лицевой стороне карты. Код проверки подлинности уникален для каждой пластиковой карты и связан с номером PAN. Ниже приведены термины для различных международных платежных систем: ▪ **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
Компенсационные меры (Compensating Controls)	В том случае, если проверяемая организация не может напрямую выполнить исходное требование стандарта PCI DSS по обоснованным техническим или задокументированным бизнес-ограничениям, однако успешно снизила риск, связанный с требованием, путем реализации других мер, такие меры могут быть признаны компенсационными. Компенсационные меры должны: (1) отвечать цели и строгости изначального требования PCI DSS; (2) обеспечивать такой же уровень защиты, как и оригинальное требование стандарта PCI DSS; (3) обеспечивать дополнительный уровень защиты по сравнению с прочими требованиями PCI DSS (не дублировать прочие требования PCI DSS); (4) быть соизмеримыми с дополнительным риском, вызванным невозможностью выполнить требование PCI DSS; См. Приложения B и C "Компенсационные меры" к документу *"Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования и процедуры аудита безопасности"*.
Компрометация (Compromise)	Также называется "компрометацией данных". Вторжение в компьютерную систему, при котором существует подозрение о несанкционированном раскрытии, изменении или уничтожении данных о держателях карт.
Консоль (Console)	Экран и клавиатура, с помощью которых осуществляется доступ и управление сервером, мейнфреймом или другим типом системы в сетевом окружении.
Контроль доступа (Access Control)	Механизмы, которые ограничивают доступность данных или ресурсов, задействованных в обработке данных, только авторизованным кругом людей или приложений.
Криптография (Cryptography)	Раздел математики и информатики о безопасности данных и соответствующих понятиях и функциях, в частности о шифровании и аутентификации. В области безопасности сети и приложений это инструмент для управления доступом к данным, обеспечения конфиденциальности и целостности информации.
Криптопериод (Cryptoperiod)	Временной промежуток, в течение которого может использоваться определенный криптографический ключ для решения определенной задачи, например, до того момента, как истечет установленный срок и/или будет создано некоторое количество криптотекста, и в соответствии с передовыми практическими методами индустрии безопасности и руководствами (такими как, например, специальное издание *NIST 800-57*).
Критичные аутентификационные данные (Sensitive Authentication Data)	Связанные с обеспечением безопасности данные (включая, но не ограничиваясь: коды/значения проверки подлинности карт, полные данные дорожки магнитной полосы, PIN-коды и PIN-блоки), используемые для аутентификации держателей карт и/или авторизации платежных транзакций.

Термин	Определение
Критичные помещения (Sensitive Area)	Любой центр обработки данных, серверная комната или другое помещение, в котором расположены системы, хранящие, обрабатывающие или передающие данные о держателях карт. Исключением являются места расположения POS-терминалов, такие как кассовые зоны торговых комплексов.
Токен	Значение, предоставляемое оборудованием или программным обеспечением, которое обычно работает с сервером аутентификации или сетью VPN для выполнения динамической или двухфакторной аутентификации. См. *RADIUS, TACACS* и *VPN.*
Маршрутизатор (Router)	Оборудование или программное обеспечение, которое соединяет две или более сетей. Маршрутизатор выполняет функции сортировщика и интерпретатора, просматривая IP-адреса и передавая пакеты данных по соответствующим адресам получателя. Программные маршрутизаторы иногда называют шлюзами.
Маскирование (Masking)	В контексте PCI DSS это метод сокрытия сегмента данных при отображении или печати. Маскирование используется, когда нет бизнес-требований по просмотру всего номера PAN. Маскирование относится к защите номера PAN при его отображении на экране или печати. См. *Усечение* для получения информации о защите номера PAN при его хранении в файлах, базах данных и т. д.
Межсетевой экран (Firewall)	Аппаратная и/или программная технология, которая защищает сетевые ресурсы от несанкционированного доступа. Межсетевой экран разрешает или запрещает обмен данными между сетями с различными уровнями безопасности на основе набора правил и других критериев.
Мейнфрейм (Mainframe)	Компьютеры, которые предназначены для работы с большими объемами данных. На базе мейнфреймов могут работать несколько операционных систем. Многие устаревшие системы имеют структуру мейнфрейма.
Монитор виртуальной машины	Монитор виртуальной машины 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 операционной системы в соответствии с потребностями.
Мониторинг (Monitoring)	Использование системы или процессов для постоянного наблюдения за компьютерами или сетевыми ресурсами с целью уведомления персонала в случае сбоя в работе, поступления сигнала тревоги, либо в других предопределенных случаях.
Мониторинг целостности файлов (File Integrity Monitoring)	Метод или технология мониторинга определенных файлов или журналов аудита на предмет их изменений. Когда критичные файлы или журналы изменяются, специалисты по безопасности должны получать соответствующие уведомления.

Термин	Определение
Небезопасный протокол/сервис/порт (Insecure Protocol/Service/Port)	Протокол, сервис или порт, который создает угрозы для системы безопасности вследствие отсутствия механизмов управления конфиденциальностью и/или целостностью. Это могут быть сервисы, протоколы или порты, которые передают данные о держателях карт и аутентификационные данные (например, пароль или парольные фразы в виде незашифрованного текста по сети Интернет) или которые позволяют злоумышленникам воспользоваться уязвимостями вследствие неправильной настройки. Примеры небезопасных сервисов, протоколов или портов включают, (но не ограничиваются: FTP, Telnet, POP3, IMAP и SNMP.
Недоверенная сеть (Untrusted Network)	Сеть, которая является внешней по отношению к сетям, принадлежащим организации, и которая не может контролироваться или управляться организацией.
Номер карты (Account Number)	См. *Номер платежной карты (PAN).*
Обновление (Patch)	Обновление до существующей версии ПО для расширения функциональности или исправления ошибок.
Общедоступная сеть (Public Network)	Сеть, созданная и управляемая телекоммуникационной компанией с целью предоставления услуг передачи данных абонентам. При передаче данные могут быть перехвачены, изменены и/или может быть изменен их маршрут. Примеры общедоступных сетей, на которые распространяется стандарт PCI DSS, включают, но не ограничиваются: Интернет, беспроводные и мобильные технологии.
Объект системного уровня (System-level object)	Любой элемент системного компонента, необходимый для его функционирования, включая, но не ограничиваясь исполняемые и конфигурационные файлы приложения, конфигурационные файлы системы, статические и совместно используемые библиотеки и DLL, исполняемые файлы системы, драйверы устройств и конфигурационные файлы устройств, а также дополнительные сторонние компоненты.
Операционная система /ОС (Operating System / OS)	Программное обеспечение, которое используется для управления и координации всех операций и обмена компьютерными ресурсами. В качестве примера можно привести операционные системы Microsoft Windows, Mac OS, Linux и Unix.
Определение области оценки (Scoping)	Процесс выявления всех системных компонентов, людей и процессов для включения в область оценки на соответствие стандарту PCI DSS. Первым этапом выполнения оценки соответствия требованиям PCI DSS должно быть определение области аудита.
Организация (Entity)	Термин, используемый для обозначения корпорации, организации или предприятия, которое проходит проверку на соответствие стандарту PCI DSS.
Отчет о проверке (Report on Validation)	Также обозначается как "ROV" (Report on Validation). Отчет, в котором содержатся детальные сведения о статусе соответствия платежного приложения стандарту PCI PA-DSS.
Отчет о соответствии (Report on Compliance)	Также обозначается как "ROC" (Report on Compliance). Отчет, в котором содержатся детальные сведения о статусе соответствия организации стандарту PCI DSS.

Термин	Определение
Параметризованные запросы (Parameterized Queries)	Средство структурирования SQL-запросов для предотвращения инъекций кода.
Пароль по умолчанию	Предварительно заданный пароль для получения доступа к учетным записям администрирования системы, пользователей или сервисов. Он обычно связан с учетной записью по умолчанию. Установленные по умолчанию учетные записи и пароли опубликованы и хорошо известны, и поэтому легко угадываются.
Пароль / Парольная фраза (Password / Passphrase)	Строка символов, которая служит для аутентификации пользователя.
Персонал (Personnel)	Постоянные сотрудники, временные сотрудники, сотрудники, работающие по совместительству, и консультанты, находящиеся на объекте компании либо так или иначе имеющие доступ к среде данных о держателях карт.
Платежное приложение (Payment Application)	Любое приложение, которое используется для хранения, обработки или передачи данных о держателях карт в процессе авторизации или расчетов.
Платежные карты (Payment Cards)	Для целей PCI DSS это любая платежная карта или устройств с логотипом одного из членов Совета PCI SSC: American Express, Discover Financial Services, JCB International, MasterCard Worldwide или Visa, Inc.
Подмена IP-адреса (IP Address Spoofing)	Методика, используемая злоумышленниками для получения неавторизованного доступа к компьютерам. Злоумышленник направляет ложные сообщения на компьютер с IP-адреса, указывающего на принадлежность к надежному хосту.
Политика (Policy)	Совокупность правил управления допустимыми методами использования вычислительных ресурсов, практических мер по обеспечению безопасности и принципов разработки рабочих процедур.
Политика безопасности (Security Policy)	Набор обязательных принципов, правил и методов регулирования того, как организация управляет, защищает и распространяет критичную информацию.
Пользователи, не являющиеся клиентами	Любые лица, исключая держателей карт, имеющие доступ к системным компонентам, включая, но не ограничиваясь: сотрудники, администраторы и третьи стороны.
Поставщик услуг (Service Provider)	Организация (кроме международных платежных систем, МПС), непосредственно вовлеченная в процесс обработки, хранения или передачи данных о держателях карт. К поставщикам услуг относятся также компании, предоставляющие услуги, которые контролируют или могут влиять на безопасность данных о держателях карт. Примерами таких компаний являются поставщики управляемых услуг (Managed Service Provider – MSP), предоставляющие услуги по межсетевому экранированию, обнаружению вторжений и прочие услуги, а также хостинг-провайдеры и другие организации. К поставщикам услуг не относятся такие организации, как телекоммуникационные компании, предоставляющие только каналы связи без доступа к их прикладному уровню.

Термин	Определение
Приложение (Application)	Любая приобретенная или собственная программа или пакет программ, включая внутренние и внешние приложения (например, веб-приложения).
Проверка с сохранением состояния (Stateful Inspection)	Также называется "динамической фильтрацией пакетов". Это функция межсетевого экрана, которая обеспечивает повышенную безопасность посредством отслеживания коммуникационных пакетов. Только входящие пакеты с надлежащим ответом могут проходить через межсетевой экран.
Протокол (Protocol)	Согласованный метод обмена данными, используемый в сетях. Спецификация, в которой описаны правила и процедуры, которым должны соответствовать программные продукты для выполнения операций в сети.
Протоколы безопасности (Security Protocols)	Сетевые коммуникационные протоколы, разработанные для безопасной передачи данных. Примеры протоколов безопасности включают, но не ограничиваются: SSL/TLS, IPSEC, SSH и другие.
Процедура (Procedure)	Политика в более узком смысле. Процедура — это практические приемы и методы реализации политики.
Разделение знания (Split Knowledge)	Состояние, при котором две или более стороны раздельно владеют компонентами одного ключа, которые по отдельности не дают знания результирующего криптографического ключа.
Разделение полномочий (Separation of Duties)	Практика распределения этапов выполнения какой-либо функции между различными людьми, с целью устранения возможности нарушения процесса одним человеком.
Размагничивание (Degaussing)	Также называется "размагничиванием диска". Процесс или метод размагничивания диска для уничтожения всех данных, которые хранятся на диске.
Резервная копия (Backup)	Копия данных с целью архивации или защиты от повреждения или потери.
Рекламное ПО (Adware)	Тип вредоносного ПО, которое при установке заставляет компьютер автоматически отображать или загружать рекламные объявления.
Реселлер / Интегратор (Reseller / Integrator)	Организация, которая продает и/или интегрирует платежные приложения, но не разрабатывает их.
Руткит (Rootkit)	Тип вредоносного ПО, которое при установке без авторизации может скрыть свое присутствие и получить контроль над системой компьютера.
Сегментация сети (Network Segmentation)	Сегментация сети позволяет изолировать системные компоненты, которые используются для хранения, обработки или передачи данных о держателях карт, от систем, которые не используются для этого. С помощью надлежащей сегментации сети можно уменьшить размер среды данных о держателях карт и область оценки на соответствие стандарту PCI DSS. См. раздел "Сегментация сети" в документе *"Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования и процедуры аудита безопасности"*. Сегментация сети не является требованием стандарта PCI DSS. См. *Системные компоненты.*

Термин	Определение
Сервер (Server)	Компьютер, который предоставляет сервисы другим компьютерам, такой как обработка данных, хранение файлов или доступ к принтеру. Серверы включают, но не ограничиваются: веб-серверы, серверы баз данных, серверы приложений, серверы аутентификации, DNS-серверы, почтовые серверы, прокси-серверы и серверы NTP.
Сервисный код (Service Code)	Набор из трех или четырех цифр на магнитной полосе карты, который следует за датой истечения срока действия платежной карты в данных дорожки. Сервисный код используется, например, для определения сервисных атрибутов, различий между национальными и международными комиссиями за проведения операций по карте или для выявления ограничений использования.
Серийный продукт (Off-the-Shelf)	Готовый к использованию и/или доработанный (так называемый коробочный) продукт, не разработанный для конкретного пользователя или заказчика.
Сетевые компоненты (Network Components)	Включают, но не ограничиваются: межсетевые экраны, коммутаторы, маршрутизаторы, беспроводные точки доступа, сетевые программно-аппаратные комплексы и прочее.
Сеть	Два или более компьютеров, которые подключены друг к другу физически или посредством беспроводных технологий.
Системные компоненты (System Components)	Любой компонент сети, сервер или приложение, которые являются частью среды данных о держателях карт или подключены к этой среде.
Системный администратор (SysAdmin)	Человек, обладающий расширенными полномочиями и несущий ответственность за управление компьютерной системой или сетью. Лицо, обладающее расширенными полномочиями и несущее ответственность за управление компьютерной системой или сетью.
Сканирование сети на наличие уязвимостей (Network Security Scan)	Процесс, позволяющий вручную или автоматически выполнять удаленную проверку организации на наличие уязвимостей. Проверка может включать в себя тестирование внешних и внутренних систем и предоставление отчетов об уязвимых службах. Сканирование выявляет уязвимости в операционных системах, службах и устройствах, которыми могут воспользоваться злоумышленники.
Смарт-карта (Smart Card)	Другие названия: чиповая карта или карта с микропроцессором. Тип платежной карты, которая имеет встроенный чип, содержащий данные платежной карты, включая, но не ограничиваясь, данные, эквивалентные данным на магнитной полосе. Чип содержит данные платёжной карты, включая, но не ограничиваясь, данные, , эквивалентные данным на магнитной полосе.
Соль (Salt)	Случайная строка, которая присоединяется к другим данным перед исполнением хеш-функции. См. также *Хеширование.*
Специалист по безопасности (Security Officer)	Человек, несущий основную ответственность за деятельность по обеспечению безопасности организации.

Термин	Определение
Среда данных о держателях карт (Cardholder Data Environment)	Среда данных о держателях карт — это люди, процессы и технологии, которые хранят, обрабатывают или передают данные о держателях карт или критичные аутентификационные данные, включая любые подключенные системные компоненты.
Стойкая криптография (Strong Cryptography)	Криптография, основанная на протестированных и принятых в отрасли алгоритмах, наряду с использованием ключа надлежащего размера и надлежащих методов управления ключами. Криптография — это метод защиты данных, который включает как шифрование (которое обратимо), так и хеширование (которое необратимо, то есть является односторонним). Примерами принятых в отрасли стандартов и алгоритмов шифрования являются AES (128 бит или больше), TDES (ключи как минимум двойной длины), RSA (1024 бита и больше), ECC (160 бит и больше) и ElGamal (1024 бита и больше). Для получения дополнительной информации см. специальное издание NIST 800-57 (http://csrc.nist.gov/publications/).
Съемные электронные носители	Носители, которые содержат цифровые данные и которые можно легко извлечь, и/или переместить с одного компьютера на другой. Например, к таким носителям относятся CD и DVD-диски, USB-накопители и съемные жесткие диски.
Тест на проникновение (Penetration Test)	Тест на проникновение представляет собой попытки использования уязвимостей для определения возможности несанкционированного доступа или других злонамеренных действий. Тестирование на проникновение включает тестирование сети и приложений, а также механизмов контроля и процессов. При этом моделируется проникновение как из-за пределов сети, так и внутри сети.
Торгово-сервисное предприятие (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. Обратите внимание, что торгово-сервисное предприятие, которое принимает платежные карты, может быть также поставщиком услуг, если предоставляемые услуги приводят к хранению, обработке или передаче данных по поручению других торгово-сервисных предприятий или поставщиков услуг. Например, ISP — это торгово-сервисное предприятие, которое принимает платежные карты для ежемесячного выставления счетов, но также является поставщиком услуг, если она обслуживает торгово-сервисные предприятия как клиентов.
Троян (Trojan)	Также называется "программой типа троянский конь". Тип вредоносного ПО, которое при установке разрешает пользователю выполнять обычные функции, в то время как троян выполняет зловредные функции в компьютерной системе без ведома пользователя.
Угроза (Threat)	Условие, при котором данные или ресурсы, обрабатывающие данные, могут быть намеренно или непреднамеренно потеряны, изменены, раскрыты, сделаны недоступными либо использованы другим образом с целью нанесения ущерба организации.

Термин	Определение
Удаленная лабораторная среда	Лаборатория, которая не находится в ведении организации, имеющей статус PA-QSA.
Удаленный доступ (Remote Access)	Доступ к компьютерным сетям из удаленного местоположения, обычно осуществляемый из-за пределов сети. Примером технологии для удаленного доступа может быть *VPN*.
Управление ключами (Key Management)	В криптографии это набор процессов и механизмов, которые поддерживают использование ключей, включая замену старых ключей новыми при необходимости.
Усечение (Truncation)	Метод приведения номера PAN к нечитаемому виду посредством удаления сегмента данных PAN. Усечение относится к защите номера PAN при *хранении* в файлах, базах данных и т. д. См. *Маскирование* для получения информации о защите номера PAN *при его отображении* на экранах и печати на бумажных квитанциях.
Услуги выпуска (Issuing services)	Примеры услуг выпуска включают, но не ограничиваются: авторизация, персонализация карт.
Учетная запись по умолчанию (Default Accounts)	Учетная запись для входа, установленная в системе, приложении или устройстве и разрешающая первоначальный доступ к системе при ее начальном запуске. В процессе установки система может сгенерировать дополнительные учетные записи.
Учетные данные для аутентификации	Сочетание идентификатора пользователя или учетной записи и аутентификационных факторов, которые используются для проверки подлинности человека (персоны), устройства или процесса.
Уязвимость (Vulnerability)	Недостаток или слабое место, которое, будучи использованным, может привести к умышленной или неумышленной компрометации системы.
Фильтрация входящего трафика (Ingress Filtering)	Метод фильтрации входящего сетевого трафика, при котором только явно разрешенный трафик может проникать в сеть.
Фильтрация исходящего трафика (Egress Filtering)	Метод фильтрации исходящего сетевого трафика, при котором только явно разрешенный трафик может выходить за пределы сети.
Хеширование (Hashing)	Процесс представления данных о держателях карт в нечитаемом виде посредством преобразования данных в сообщение фиксированной длины с использованием *стойкой криптографии.* Хеширование — это математическая функция, при использовании которой несекретный алгоритм преобразует сообщение любой длины в сообщение фиксированной длины (обычно это называется «хеш-код» или «дайджест-сообщение»). 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 PAN, чтобы хеш-код невозможно было прочитать. Рекомендуется, чтобы хешированные данные о держателях карт включали в себя соль как вводное значение для функции хеширования (см. *Соль*).

Термин	Определение
Хост (Host)	Основное аппаратное обеспечение компьютера, на котором хранится и/или исполняется программное обеспечение.
Хостинг-провайдер (Hosting Provider)	Организация, которая предлагает различные услуги торгово-сервисным предприятиям и другим поставщикам услуг. Диапазон услуг достаточно широк: от простых до сложных; от предоставления общедоступного места на сервере до полного спектра возможностей торговой корзины ("shopping cart"); от платежных приложений до подключения к платежным шлюзам и процессинговым центрам; а также для получения услуг хостинга, позволяющих одному клиенту размещать информацию на выделенном сервере. Хостинг-провайдером может быть поставщик услуг с общей средой, который размещает несколько организаций на одном сервере.
Частная сеть (Private Network)	Сеть организации, которая использует частное адресное пространство. 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.
Шифрование (Encryption)	Процесс преобразования информации в форму, нечитаемую всеми, за исключением владельца специального криптографического ключа. Использование алгоритмов шифрования позволяет защитить информацию от несанкционированного раскрытия после процесса шифрования и до процесса расшифрования. См. *Стойкая криптография.*
Шифрование базы данных на уровне столбцов (Column-Level Database Encryption)	Метод или технология (либо программная, либо аппаратная) для шифрования содержимого определенного столбца в базе данных, а не всего содержимого базы данных. См. также *Шифрование диска* или *Шифрование на уровне файла.*
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). Кроме того, могут использоваться такие методы, как *Шифрование на уровне файла* или *Шифрование базы данных на уровне столбцов*, для шифрования содержимого определенных файлов или столбцов базы данных.
Шифрование на уровне файла (File-Level Encryption)	Метод или технология (программная или аппаратная) для шифрования полного содержимого определенных файлов. См. также *Шифрование диска* или *Шифрование базы данных на уровне столбцов.*
Шпионское ПО (Spyware)	Тип вредоносного ПО, которое при установке перехватывает или получает частичный контроль над компьютером пользователя без согласия пользователя.
Эквайер (Acquirer)	Также называется "банком-эквайером" или "финансовой организацией-эквайером". Организация, которая устанавливает и поддерживает взаимодействие с торгово-сервисными предприятиями, принимающими платежные карты.

Термин	Определение
Экспертиза (Forensics)	Также называется "компьютерной экспертизой". В области информационной безопасности применение средств и методов анализа для сбора доказательств из компьютерных ресурсов с целью определения причины компрометации данных.
Эмитент (Issuer)	Организация, которая выпускает платежные карты и/или выполняет, содействует или поддерживает услуги выпуска карт, включая, но не ограничиваясь: банки-эмитенты и эмиссионные процессинговые центры. Также называется "банком-эмитентом" или "финансовой организацией-эмитентом".
AAA	Аббревиатура от "аутентификация, авторизация и учет". Набор протоколов, состоящий из аутентификации пользователя на основе его учетных данных, авторизации пользователя на основе его прав и учета использования пользователем сетевых ресурсов.
AES	Аббревиатура — Advanced Encryption Standard (Улучшенный стандарт шифрования). Алгоритм блочного шифрования, используемый в симметричной криптографии, утвержденный Национальным институтом стандартов и технологий (США) в ноябре 2001 года. Этот алгоритм был принят как стандарт FIPS PUB 197 (или FIPS 197)я.
ANSI	Аббревиатура — Американский национальный институт стандартов. Частная некоммерческая организация, которая управляет и координирует деятельность американской добровольной системы стандартизации и оценки соответствия требованиям.
ASV	Аббревиатура — Approved Scanning Vendor (Авторизованный поставщик услуг сканирования). Компания, которой Совет PCI SSC предоставил право проведения внешнего сканирования на наличие уязвимостей.
Bluetooth	Протокол беспроводной связи, который использует технологию связи ближнего действия для передачи данных на короткие расстояния.
CERT	Аббревиатура — Computer Emergency Response Team (Группа реагирования на компьютерные происшествия Университета Карнеги-Меллона). Программа CERT продвигает использование различных методов управления технологиями и системами для противостояния атакам на подключенные к сети системы с целью минимизации ущерба и для обеспечения непрерывности работы.
CIS	Аббревиатура — Center for Internet Security (Центр интернет-безопасности). Некоммерческая организация, целью которой является содействие компаниям в снижении риска нарушения ведения основной деятельности или ведения электронной коммерции из-за неадекватных технических мер по обеспечению безопасности.

Термин	Определение
DMZ	Аббревиатура — demilitarized zone (демилитаризованная зона). Физическая или логическая подсеть, которая обеспечивает дополнительный уровень защиты для внутренней частной сети организации. Демилитаризованная зона создает дополнительный уровень защиты сети между сетью Интернет и внутренней сетью организации, чтобы внешние стороны могли подключаться напрямую только к устройствам в этой зоне, а не ко всей внутренней сети.
DNS	Аббревиатуа — Domain Name System (система доменных имен) или domain name server (сервер доменных имен). Система, которая хранит в распределенной базе данных в сети, такой как Интернет, информацию, связанную с доменными именами.
DSS	Аббревиатура — Data Security Standard (Стандарт безопасности данных), также обозначается как PCI DSS.
ECC	Аббревиатура — Шифрование на основе эллиптических кривых. Метод, применяемый в криптографии с открытым ключом, использующий эллиптические кривые в конечных полях. См. *Стойкая криптография.*
FIPS	Аббревиатура — Federal Information Processing Standards (Федеральные стандарты обработки информации). Стандарты, которые признаны Федеральным правительством США; также для использования неправительственными учреждениями и подрядчиками.
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.
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.
HTTP	Аббревиатура — hypertext transfer protocol (протокол передачи гипертекста). Открытый интернет-протокол для передачи данных в сети Интернет.

Термин	Определение
HTTPS	Аббревиатура — hypertext transfer protocol over secure socket layer (протокол передачи гипертекста со средствами шифрования) Защищенный (безопасный) протокол HTTP, который обеспечивает аутентификацию и шифрование соединения с целью защиты веб-взаимодействия, например, при входе в систему через веб-интерфейс.
IDS	Аббревиатуоа — intrusion detection system (система обнаружения вторжения). Программное обеспечение или оборудование, которое используется для обнаружения попыток вторжения в сеть или систему и оповещения о таких попытках. Включает в себя датчики, генерирующие события безопасности, консоль для отслеживания событий и оповещений и управления датчиками, а также центральный механизм, записывающий события, зафиксированные датчиками, в базу данных. Использует систему правил для генерации оповещений при обнаружении событий безопасности.
IETF	Аббревиатура — Internet Engineering Task Force (Специальная комиссия инженерии сети Интернет). Открытое международное сообщество проектировщиков, сетевых операторов, провайдеров и ученых, которые занимаются развитием архитектуры сети Интернет и обеспечением безопасной работы в ней. В это сообщество может вступить любой желающий.
IP	Аббревиатура — internet protocol (межсетевой протокол). Протокол сетевого уровня, содержащий данные об адресе и определенную управляющую информацию, необходимую для маршрутизации пакетов. IP — основной протокол сетевого уровня, входящий в пакет протоколов сети Интернет.
IPS	Аббревиатура — intrusion prevention system (система предотвращения вторжений). Система предотвращения вторжений дополняет систему обнаружения вторжений механизмом блокирования попыток проникновения в сеть или систему.
IPSEC	Аббревиатура — Internet Protocol Security (протокол безопасности сети Интернет). Стандарт для защиты соединений по протоколу IP посредством шифрования и/или аутентификации всех IP-пакетов. IPSEC обеспечивает безопасность на уровне сети.
IP-адрес (IP Address)	Также называется "адресом межсетевого протокола". Числовой код, который уникально идентифицирует конкретный компьютер в сети Интернет.
ISO	International Organization for Standardization (Международная организация по стандартизации). Неправительственная организация, состоящая из сети национальных организаций по стандартизации более чем из 150 стран (по одному члену из каждой страны). Центральный секретариат находится в городе Женева (Швейцария).
LAN	Аббревиатура — local area network (локальная сеть). Это группа компьютеров и/или других устройств, совместно использующих единые каналы связи, часто расположенных в пределах одного или нескольких зданий.

Термин	Определение
LDAP	Аббревиатура — Lightweight Directory Access Protocol (Облегченный протокол доступа к каталогу). Хранилище данных аутентификации и авторизации, используемых для определения очередности и изменения полномочий пользователей и предоставления доступа к защищенным ресурсам.
LPAR	Аббревиатура — logical partition (логический раздел). Система разделения ресурсов компьютера — процессоров, памяти и хранилища — на более мелкие блоки, которые можно запускать с их собственной копией операционной системы и приложений. Логическое разделение обычно применяется для обеспечения возможности использования различных операционных систем и приложений на одном устройстве. Разделы можно настроить таким образом, чтобы они могли взаимодействовать друг с другом или совместно использовать ресурсы сервера, например сетевые интерфейсы.
MAC	Аббревиатура — message authentication code (код аутентификации сообщения). В криптографии это небольшая часть информации, используемая для аутентификации сообщения. См. *Стойкая криптография.*
MAC-адрес (MAC Address)	Аббревиатура — media access control address (адрес управления доступом к среде). Уникальный идентификатор, который присваивается разработчиками сетевым адаптерам и сетевым интерфейсным картам.
MPLS	Аббревиатура — multi protocol label switching (мультипротокольная коммутация по меткам) Сеть или телекоммуникационный механизм для объединения группы сетей с пакетной коммутацией.
NAT	Аббревиатура — network address translation (механизм преобразования сетевых адресов). Другие названия: сетевое преобразование, преобразование IP. Замена IP-адреса, используемого в одной сети, другими IP-адресами, известными в другой сети.
NIST	Аббревиатура — National Institute of Standards and Technology (Национальный институт стандартов и технологий). Управление по технологиям США одного из агентств Департамента торговли США. Миссия Института — продвигать инновационную и индустриальную конкурентоспособность США путем развития наук об измерениях, стандартизации и технологий с целью повышения экономической безопасности и улучшения качества жизни.
NMAP	ПО для сканирования на наличие проблем безопасности, которое сопоставляет сети и выявляет открытые порты в сетевых ресурсах.
NTP	Аббревиатура — Network Time Protocol (сетевой протокол службы времени). Сетевой протокол для синхронизации часов компьютера, сетевых устройств и других системных компонентов.
OWASP	Аббревиатура — Open Web Application Security Project (Открытый проект безопасности веб-приложений). Некоммерческая организация, задача которой заключается в повышении безопасности прикладного ПО. OWASP предоставляет список критических уязвимостей для веб-приложений. (См. http://www.owasp.org).

Термин	Определение
PAN	Аббревиатура — primary account number (номер платежной карты), другое название: "номер карточного счета". Уникальный номер платежной карты (кредитной или дебетовой), который идентифицирует эмитента и персональный счет держателя карты.
PA-QSA	Аббревиатура — Payment Application Qualified Security Assessor, компания, которой Совет PCI SSC предоставил право проведения оценки платежных приложений на соответствие стандарту PA-DSS.
PAT	Аббревиатура — port address translation (преобразование адресов портов), другое название: преобразование сетевых адресов на уровне портов. Тип технологии *NAT*, которая используется для преобразования номеров порта.
PCI	Аббревиатура — Payment Card Industry (индустрия платежных карт).
PDA	Сокращение — personal data assistant или personal digital assistant (карманный компьютер). Карманные мобильные устройства, которые можно использовать для совершения и приема телефонных звонков, работы с электронной почтой и просмотра веб-страниц.
PED	Устройство ввода PIN-кода
PIN	Аббревиатура — personal identification number (личный опознавательный номер). Секретный пароль из цифр, известный только пользователю и системе и используемый для аутентификации пользователя в системе. Пользователю предоставляется доступ, только если PIN, указанный пользователем, соответствует PIN-коду в системе. Обычно PIN-коды используются для получения наличных денег по банковской карте через банкомат. Другой тип PIN-кода используется в картах с чипом EMV, где PIN заменяет подпись держателя карты.
PIN-блок	Блок данных, используемый для инкапсуляции PIN-кода во время обработки. Формат PIN-блока определяет содержимое PIN-блока и того, как оно обрабатывается для получения PIN-кода. PIN-блок состоит из PIN-кода, длины PIN и может содержать поднабор PAN.
POI	Аббревиатура — Point of Interaction, начальная точка, где данные считываются с карты. POI состоит из оборудования и программного обеспечения и размещается в оборудовании для приема, позволяя держателю карты выполнять операции с использованием карты. Работа с POI может выполняться как с участием, так и без участия пользователя. Транзакции POI обычно представляют собой платежные транзакции с применением карты со встроенным чипом или магнитной полосой.
POS	Аббревиатура — point of sale. Оборудование и/или программное обеспечение, которое используется для обработки транзакций с использованием платежных карт на территории торгово-сервисного предприятия.
PTS	Аббревиатура — PIN Transaction Security PTS — это набор требований для оценки, разработанных Советом по стандартам безопасности данных индустрии платежных карт для POI-терминалов, операции через которые проводятся с использованием PIN-кода. Более подробная информация доступна на сайте www.pcisecuritystandards.org.

Термин	Определение
PVV	Аббревиатура — PIN verification value (значение проверки PIN-кода). Значение, закодированное в магнитной полосе платежной карты.
QSA	Аббревиатура — Qualified Security Assessor, компания, которой Совет PCI SSC предоставил право проведения оценки на соответствие стандарту PCI DSS.
RADIUS	Аббревиатура — Remote Authentication Dial-In User (Удаленная аутентификация пользователя, устанавливающего соединение по телефонной линии). Система аутентификации и учета. Проверяет правильность информации, такой как имя пользователя или 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.
RBAC	Аббревиатура — role-based access control (контроль доступа на основе ролей). Механизмы контроля для ограничения доступа по принципу служебной необходимости.
RFC 1918	Стандарт, разработанный Специальной комиссией инженерии сети Интернет, который определяет порядок использования диапазонов адресов для частных сетей.
RSA	Криптографический алгоритм с открытым ключом, разработанный в 1977 г. Рональдом Райвестом (Ron Rivest), Ади Шамиром (Adi Shamir) и Леонардом Адлеманом (Len Adleman) из Массачусетского технологического института (MBT). Аббревиатура RSA — это начальные буквы их фамилий.
SANS	Аббревиатура — SysAdmin, Audit, Networking and Security (Институт системного администрирования, аудита, сетевых технологий и проблем безопасности), институт, который предоставляет услуги обучения в области компьютерной безопасности и профессиональной сертификации. (См. www.sans.org.)
SAQ	Аббревиатура — Опросный лист для самооценки (Self-Assessment Questionnaire). Средство, используемое организацией для проверки соответствия стандарту PCI DSS.
SDLC	Аббревиатура — system development life cycle (жизненный цикл разработки системы). Этапы разработки программного обеспечения или компьютерной системы, которые включают планирование, анализ, проектирование, тестирование и внедрение.
SHA-1/SHA-2	Аббревиатура — Secure Hash Algorithm (Безопасный алгоритм хеширования). Представляет собой семейство или набор алгоритмов криптографического хеширования. См. *Стойкая криптография.*
SNMP	Аббревиатура — Simple Network Management Protocol (Простой протокол управления сетью). Поддерживает мониторинг устройств, подключенных к сети, на предмет появления состояний, требующих внимания администратора.

Термин	Определение
SQL	Аббревиатура — Structured Query Language (язык структурированных запросов). Компьютерный язык, который используется для создания, изменения и извлечения данных из систем управления реляционными базами данных.
SQL-инъекция (SQL Injection)	Тип атаки на веб-сайт, содержащий базу данных. Злоумышленник выполняет несанкционированные команды SQL, применяя их к небезопасному коду в системах, подключенных к сети Интернет. SQL-инъекции используются обычно для кражи информации из базы данных и/или получения доступа к компьютерам организации через компьютер, на котором размещена база данных.
SSH	Аббревиатура — Secure Shell (Безопасная оболочка). Набор протоколов, которые обеспечивают шифрование для сетевых сервисов, таких как удаленный вход в систему или удаленная передача файлов.
SSL	Аббревиатура — Secure Sockets Layer (Уровень защищенных сокетов). Одобренный стандарт шифрования канала связи между браузером и веб-сервером, который обеспечивает конфиденциальность и надежность данных, передаваемых по этому каналу.
TACACS	Аббревиатура — Terminal Access Controller Access Control System (Система управления доступом для контроллера доступа к терминалу). Протокол удаленной аутентификации обычно используется 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). Базовый язык коммуникации или протокол Интернета.
TDES	Аббревиатура — Triple Data Encryption Standard (Тройной стандарт шифрования данных). Также называется 3DES или Triple DES. Представляет собой блочный алгоритм шифрования, созданный на основе алгоритма DES. При применении этого алгоритма над блоком данных три раза производится шифрование с использованием алгоритма DES. См. *Стойкая криптография.*
TELNET	Аббревиатура — telephone network protocol (протокол телефонной сети). Обычно используется для предоставления пользователям сеанса ввода командной строки на компьютерах в сети. Учетные данные пользователя передаются в виде незашифрованного текста.
TLS	Аббревиатура — Transport Layer Security (Безопасность транспортного уровня). Протокол предназначен для защиты и обеспечения целостности данных между двумя взаимодействующими приложениями. TLS является преемником протокола SSL.
VLAN	Аббревиатура — virtual LAN или virtual local area network (виртуальная локальная сеть). Логическая локальная сеть, которая выходит за пределы одной традиционной физической локальной сети.

Термин	Определение
VPN	Аббревиатура — virtual private network (виртуальная частная сеть). Компьютерная сеть, в которой некоторые подключения являются виртуальными цепями в составе более крупных сетей, таких как Интернет, а не прямыми подключениями посредством физических проводов. Конечные точки виртуальной сети туннелируются через более крупную сеть. В общедоступной сети Интернет коммуникации могут осуществляться с использованием механизмов обеспечения безопасности. Сеть VPN может не обладать функциями обеспечения безопасности, такими как аутентификация или шифрование содержимого. VPN может использоваться с токеном, смарт-картой и т. д. для обеспечения двухфакторной аутентификации.
WAN	Аббревиатура — wide area network (глобальная сеть). Компьютерная сеть, охватывающая большую область, часто это региональная компьютерная система или система масштаба компании.
WEP	Аббревиатура — Wired Equivalent Privacy (безопасность, аналогичная защите проводных сетей). Слабый алгоритм шифрования 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.*
WLAN	Аббревиатура — wireless local area network (беспроводная локальная сеть). Локальная сеть, которая связывает два или несколько компьютеров или устройств без использования кабелей.
WPA/WPA2	Аббревиатура — WiFi Protected Access (защищенный доступ WiFi). Протокол безопасности, созданный для защиты беспроводных сетей. WPA является преемником протокола WEP. WPA2 — это следующее поколение технологии WPA.