0
Рейтинг

PayOnline

PayOnline 21 июн 2016 в 09:06

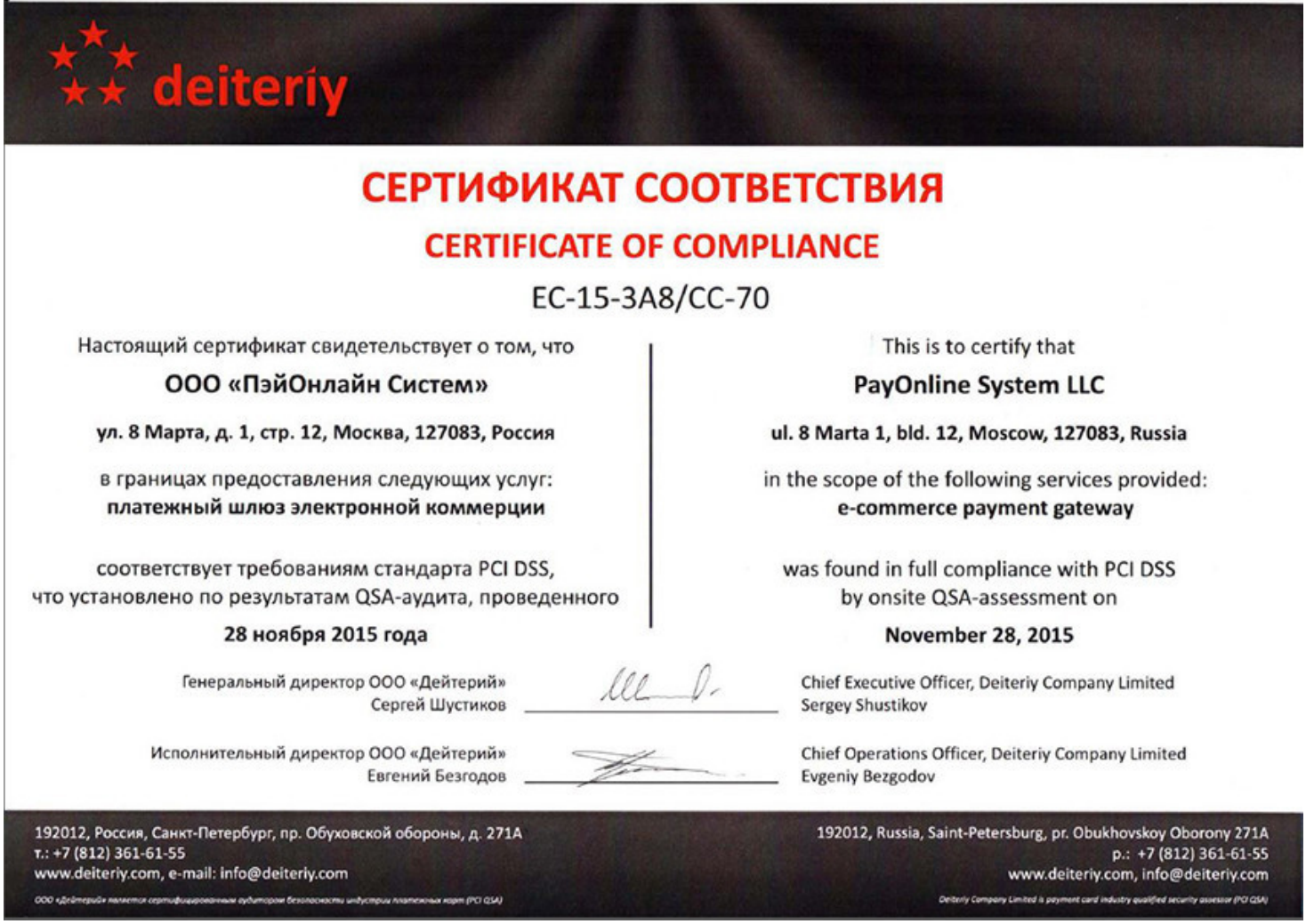
Что такое PCI DSS и как происходит проверка на соответствие стандарту?

9 мин 82K

Блог компании PayOnline, Информационная безопасность*, Платежные системы*

В конце 2015 года система электронных платежей PayOnline уже в восьмой раз доказала, что мерчанты и плательщики находятся под надежной защитой. А в мае 2016 года компания получила физический сертификат соответствия требованиям стандарта PCI DSS версии 3.1, подтверждающий высший мировой уровень безопасности.

На фоне этого события мы бы хотели подробнее рассказать, что такое PCI DSS, по каким критериям осуществляется проверка на соответствие стандарту и как, не имея собственного сертификата, интернет-магазин может обеспечить безопасность финансовых данных пользователей.



deiteriy

СЕРТИФИКАТ СООТВЕТСТВИЯ

CERTIFICATE OF COMPLIANCE

EC-15-3A8/CC-70

Настоящий сертификат свидетельствует о том, что

ООО «ПэйОнлайн Систем»

ул. 8 Марта, д. 1, стр. 12, Москва, 127083, Россия

в границах предоставления следующих услуг:
платежный шлюз электронной коммерции

соответствует требованиям стандарта PCI DSS,
что установлено по результатам QSA-аудита, проведенного

28 ноября 2015 года

This is to certify that

PayOnline System LLC

ul. 8 Marta 1, bld. 12, Moscow, 127083, Russia

in the scope of the following services provided:
e-commerce payment gateway

was found in full compliance with PCI DSS
by onsite QSA-assessment on

November 28, 2015

Генеральный директор ООО «Дейтерий»
Сергей Шустиков

Chief Executive Officer, Deiteriy Company Limited
Sergey Shustikov

Исполнительный директор ООО «Дейтерий»
Евгений Безгодов

Chief Operations Officer, Deiteriy Company Limited
Evgeniy Bezgodov

192012, Россия, Санкт-Петербург, пр. Обуховской обороны, д. 271А
т.: +7 (812) 361-61-55
www.deiteriy.com, e-mail: info@deiteriy.com

192012, Russia, Saint-Petersburg, pr. Obukhovskoy Oborony 271A
p.: +7 (812) 361-61-55
www.deiteriy.com, info@deiteriy.com

Если попробовать забить аббревиатуру PCI DSS в Google или поискать по ней на Хабре, то можно обнаружить достаточно много статей, описывающих этот стандарт. Тут же выяснится, что целевой аудиторией всех этих материалов будут те, кто так или иначе связан с электронной коммерцией. Главным образом это платёжные агрегаторы и процессинговые центры, а уже потом разработчики интернет-магазинов.

Любой вид электронной коммерции так или иначе основан на том, что покупатели, желающие приобрести товар, должны будут расплатиться за него. Несмотря на то, что возможность расплатиться архаичным способом (отдать деньги курьеру при встрече) наиболее популярна в России, есть большая вероятность, что покупатель предпочтет воспользоваться своей платёжной картой. Тут разработчикам магазина придётся иметь дело с такой деликатной материей как личные данные пользователей, которые ещё и связаны с их финансами. Вряд ли кто-то из клиентов магазина захочет, чтобы все это стало достоянием общественности, поэтому здесь приходится прибегать к продуманным и многократно проверенным решениям.

Создание целого интернет-магазина с нуля — мягко говоря, задача непростая. Поэтому на рынке довольно много фреймворков, помогающих разработчикам с этим (у всех на слуху Magento, к примеру). Задачу приема платежей, как одну из самых важных, потому что она связана с деньгами, включают в себя все решения для электронной коммерции. Разработчики, имевшие с этим дело, знают, что это достаточно простая последовательность шагов, которая часто выглядит как «качаем код библиотеки для платёжного шлюза XYZ», «настраиваем его» (все обычно сводится к получению и использованию специального ключа, позволяющего шлюзу понять с каким магазином он имеет дело), «немного допиливаем» и «выгружаем на продакшн».

Как правило, это не вызывает существенных проблем. Правда, после того, как пользователь вашего магазина перешел на страницу оплаты выбранного платежного шлюза, ввел данные своей платежной карты и нажал на кнопку «Оплатить», вмешаться в процесс уже не получится — разве только обработать ответ шлюза на своей стороне и показать пользователю красивую страничку с благодарностью (если всё прошло нормально) или извиниться (если что-то пошло не так).

Квалифицированный пользователь знает, к примеру, что https лучше http и проверяет это, многие браузеры будут показывать в адресной строке данные сертификата сайта. Однако когда платёжный шлюз начнёт свои «внутренние» транзакции с банком-эмитентом (тот, который выдал карту) и с банком-эквайером (тот, который должен получить оплату), то может возникнуть вполне закономерный вопрос — а насколько это всё вообще безопасно? Ведь передача данных по протоколу https — еще не гарантия безопасности, а лишь один из сотен параметров, обеспечивающих защиту информации.

Может быть ребята из этого шлюза и смогли настроить себе https, купили сертификат и даже большими буквами написали на своём сайте, что всё очень хорошо и всё очень защищено. Но единственным по-настоящему надёжным способом убедиться в этом является выполнение каких-то процедур, удостоверяющих безопасность внутреннего кода платежного шлюза. И, конечно, желательно, чтобы пройти такую проверку было бы сложнее, чем написать на своём сайте немного красивого HTML — «100% гарантия безопасности».

Мы опишем такую процедуру и попробуем понять, почему она является стандартом в индустрии электронной коммерции. Всё это будет скрываться под аббревиатурой PCI DSS, и именно наличие этого сертификата у платёжного шлюза вполне может означать, что данные платёжной карты (да что там, проще говоря, деньги плательщика) дойдут до адресата без проблем.

Что такое PCI DSS?

PCI DSS (Payment Card Industry Data Security Standard) — стандарт безопасности данных индустрии платежных карт. Другими словами, это документация со списком критериев, которому должен удовлетворять сервис, если он как-то управляет такими вещами, как номер карты, срок её действия и CVV-код.

Платёжных карт можно насчитать довольно много (все знают Visa и MasterCard), а поскольку речь идёт о стандарте индустрии, то было бы нелишним всем компаниям договориться между собой о том, что они будут считать безопасным. Для этого существует Совет PCI SSC (Payment Card Industry Security Standards Council) — Совет по стандартам безопасности индустрии платежных карт, образованный пятью крупнейшими платёжными системами. Именно он создаёт правила «безопасной игры», и именно его правилам должны следовать компании, желающие получить заветный шильдик «Сертифицировано PCI-DSS». Проходить сертификацию необходимо каждый год.

Что именно проверяют?

На самом деле описать все критерии проверки будет сложно — их 288. Сама процедура довольно длительная, потому что затрагивает проверку ряда сложных технических моментов. Полностью список критериев, разбитый на 12 групп, выглядит следующим образом:

- Защита вычислительной сети.
- Конфигурация компонентов информационной инфраструктуры.
- Защита хранимых данных о держателях карт.
- Защита передаваемых данных о держателях карт.
- Антивирусная защита информационной инфраструктуры.
- Разработка и поддержка информационных систем.
- Управление доступом к данным о держателях карт.
- Механизмы аутентификации.
- Физическая защита информационной инфраструктуры.
- Протоколирование событий и действий.
- Контроль защищенности информационной инфраструктуры.
- Управление информационной безопасностью.

Тут хорошо заметно, что речь идёт и о программной части, и о «физическом компоненте» — проще говоря, проверяется всё. При этом под словом «проверка» понимается буквальное присутствие того, кто эту проверку выполняет, в офисе той компании, которую проверяют. Уполномоченный аудитор, обладающий статусом QSA (Qualified Security Assessor — а этот статут подтверждается Советом PCI SSC) имеет право пообщаться с сотрудником платежного шлюза (для этого есть специальная процедура интервью), изучить настройки компонентов системы, сделать скриншоты и просто посмотреть «как это работает». Аудитором PayOnline в последние годы выступает компания Deiteriy. Её заключения признаются международными платёжными системами Visa, MasterCard, МИР, American Express, Discover и JCB.

Сам программный код библиотек проверяется выборочно, наибольшее внимание уделяют ядру, непосредственно обрабатывающему данные платёжных карт, при этом внимание обращают на соответствие внешнему стандарту безопасности OWASP, который описывает основные требования к поиску и исключению в коде уязвимостей. Также в бизнес-процессе разработки присутствует звено Code Review, на котором, собственно, проходит дополнительная проверка другим разработчиком, не участвующим в самом написании кода.

Все взаимоотношения и ответственность в рамках требований PCI DSS между сервис-провайдерами, а именно между процессинговым центром и датацентром, а также банками-эквайерами, фиксируются в так называемых матрицах ответственности. Наличие подписанных матриц ответственности между сервис-провайдерами стало обязательным требованием с версии 3.1 стандарта PCI DSS. Помимо прочего, разумеется, у датацентра должен быть также

актуальный сертификат соответствия PCI DSS на компоненты инфраструктуры, которые использует в работе процессинговый центр — виртуализация, сервисы, физическое оборудование и так далее.

Сами серверы, так же как и все остальные компоненты инфраструктуры, например, сетевое оборудование, также подлежат обязательной проверке. Основным требованием здесь является актуальность статуса PCI-DSS, который ставится в прямую зависимость от частоты изменений программного обеспечения, конфигураций оборудования или/и виртуальных машин и, что не менее важно, от ставших известными уязвимостей, таких как печально известный HeartBleed. Администраторы инфраструктуры обязаны проводить аудит системы на предмет поиска внутренних/внешних уязвимостей и приводить компоненты инфраструктуры в соответствие стандарту PCI DSS.

Аудит безопасности выполняется дважды. Первый раз используется автоматический сканер на известные уязвимости, который предоставляет сертифицированная организация ASV (Approved Scanning Vendor). В случае успешного прохождения этого теста, система проверяется на безопасность второй раз экспертами, что называется, вручную, с вынесением официального заключения.

Возможные трудности

Здесь хотелось бы привести пример из личного опыта. Во время последней сертификации PCI-DSS наши специалисты организовали специальную службу мониторинга, которая следила за тем, чтобы транзакции между нашим дата-центром и банками выполнялись непрерывно. Источником потенциальных проблем было то, что некоторые банки сообщают о том, что их сертификат TLS 1.0 был обновлён до версии 1.2 уже постфактум. Потенциально могло произойти так, что мы пытаемся общаться с банком, имея старый сертификат, тогда как на их стороне он уже обновлён. Благодаря тому, что теперь у нас отдельная служба мониторинга непрерывности транзакций, такая проблема больше невозможна.

Вообще можно привести несколько примеров, как работает проверка, и как мы приводили нашу инфраструктуру в соответствие с требованиями. Как известно, согласно PCI-DSS, платёжная система не должна хранить у себя так называемые Критичные аутентификационные данные (КАД), к которым относят, к примеру, CVV или PIN-код (последний обычно поступает из POS-терминалов супермаркетов). Реализовано это таким образом:

Когда транзакция получает от процессингового центра специальный статус, говорящий о том, что она завершена (независимо от того успешно или нет), то в системе инициируется специальный программный код, решающий две задачи. Если во время транзакции по какой-либо причине её данные были записаны на диск, то специальная операция, удаляющая эту запись, получает максимальный приоритет и выполняется специальным воркером. Если обращения к диску не было, то всё еще проще: процесс транзакции удаляется из памяти сервера и таким образом фиксации КАД не происходит. Единственные данные, которые можно хранить — это номер карты PAN (Primary Account Number), и то исключительно в зашифрованном виде.

Еще один пример напрямую связан с одним из наших пользователей (хотя на самом деле таких историй много, просто эта последняя по времени), который покупал товар в интернет-магазине. После того, как что-то «пошло не так», он не стал читать достаточно подробные сообщения об ошибке, а просто сфотографировал свою платёжную карту с обеих сторон (наверно, потому, что в форме платежа ему объяснили, что надо вводить три последние цифры после магнитной полосы на оборотной стороне) и прислал её нам в службу поддержки. По мнению покупателя, это должно было помочь нам выяснить статус его платежа — «снялись деньги» или нет. Надо сказать, что даже такие курьёзные и одновременно печальные случаи оговорены стандартом PCI-DSS.

В случае компрометации данных пользователя платёжная система обязана уведомить его самого и банк-эмитент, выпустивший «засвеченную» карту. Кроме того, необходимо было удалить письмо с вложениями-картинками из клиентской почтовой программы оператора службы поддержки, а также на почтовом сервере. Всё это делалось для того, чтобы следовать золотому правилу обеспечения безопасности индустрии платёжных карт — «Если тебе не нужна эта информация, то не храни её».

Интеграция PayOnline с интернет-магазином

Как уже упоминалось выше, задачу интеграции конкретного интернет-магазина с платёжной системой вряд ли можно назвать сложной. В интернете можно найти множество примеров для многих шлюзов. Всё обычно сводится к установке на сервер специально написанной библиотеки (у нас их много и под разные платформы) и написанию какого-то клиентского кода, который будет собирать информацию пользовательской формы и отправлять её платёжному шлюзу. Единственным моментом, на который хотелось бы обратить внимание, должно быть месторасположение самой платёжной формы — будет она находиться на стороне интернет-магазина или будет работать на стороне PayOnline. Несмотря на то, что многие решения вполне могут позволить принимать платежи прямо на своём сайте, в случае отсутствия у мерчанта собственного сертификата PCI-DSS, необходимо будет организовать всё так, чтобы платежи выполнялись на стороне платёжного шлюза. Обоснование тут одно — это безопасность финансовых данных пользователя. При этом платёжную форму можно кастомизировать под компанию, так что отторжения у конечного пользователя не возникнет.

У нас есть библиотеки для организации платежей для десктопных и мобильных решений, включая и Windows Phone (хотя позиции этой платформы с точки зрения популярности у пользователей гораздо слабее, чем у тех же Android или iOS). Говорить о библиотеке для PHP мы даже не будем — это практически подразумевается само собой. У нас также есть SDK для .NET-решений. Часто спрашивают, почему для Android выбран не традиционный подход — библиотека на Java — а используется Node.js. Такое решение было принято некоторое время назад — интегрировать такой код чуть проще, чем написанный на Java, равно как и отвечать требованиям субстандарта PCI PA-DSS. Что касается будущих интеграций, то мы сейчас располагаем адаптивными платежными формами, которые великолепно работают в нативных мобильных приложениях, интегрированных в приложение через WebView, и отвечают всем требованиям PCI PA-DSS.

Что получает интернет-магазин

Среди основных преимуществ системы электронных платежей PayOnline мы можем выделить особо наши технические возможности, нацеленные на увеличение конверсии в успешные платежи. В первую очередь, конечно, это тонкая работа с 3-D Secure, позволяющая сохранить высокий уровень защиты от мошеннических операций и одновременно увеличить платежную конверсию.

Мы внимательно изучаем поведение плательщиков, которое из года в год меняется вслед за технологическим прогрессом. Благодаря возможности измерять конверсию и поведение человека на платёжной странице в момент заполнения данных и совершения платежа, мы технологически позволяем своим клиентам шаг за шагом отследить путь покупателя, представить себя на его месте и максимально упростить его пользовательский опыт на основе полученной статистики. В случае же, если при совершении платежа у покупателя по какой-то причине не получается провести оплату, магазин получает от процессингового центра точную причину отклонения, далее магазин транслирует причину отклонения плательщику в любом кастомизированном виде. Таким образом, клиент сразу понимает, почему платеж не прошел и что ему необходимо сделать, чтобы приобрести товар или услугу.

Если вас заинтересовала такая возможность, обращайтесь, наши специалисты предоставят дополнительную информацию и, в случае необходимости, помогут настроить прием платежей на сайте и в мобильном приложении по защищенному шлюзу, отвечающему требованиям стандарта PCI DSS 3.1.

Теги: PCI DSS, безопасность, хранение данных, платежные транзакции, реквизиты карты, криптография, сертификат, PayOnline

Хабы: Блог компании PayOnline, Информационная безопасность, Платежные системы

PayOnline
Система электронных платежей

Сайт Facebook Twitter ВКонтакте Google+

13 Карма 0 Рейтинг

PayOnline @PayOnline
Система электронных платежей

Комментарии 15

grossws 21 июн 2016 в 10:19

Offtopic для "хранения данных" и "инфраструктуры", поправьте список хабов.

Ответить

PayOnline 21 июн 2016 в 11:44

Да, спасибо, убрали их

Ответить

akubintsev 21 июн 2016 в 11:38

Да, сертификация PCI DSS — титанический труд, как не помнить такое :)

Вот тут в конце упомянули про библиотеку под Android. Как-то то ли на Тостере, то ли у знакомого всплывал вопрос на тему её использования. Ничего толкового нагуглить не удалось. В лучшем случае были отсылки на экзотические способы установки node.js на рутованые девайсы. Так как же на самом деле обстоят дела?

Ответить

mihmig 21 июн 2016 в 12:37

>>или PIN-код (последний обычно поступает из POS-терминалов супермаркетов)
Эмм, а пин-код точно уходит дальше терминала?

Ответить

artemy_m 21 июн 2016 в 13:51

онлайн-пин уходит конечно же

Ответить

Sleuthhound 21 июн 2016 в 21:09

Не порите чушь, пин-код никогда не покидает пределы пинпада терминала (если пинпад идет к терминалу внешним устройством) или пин-пада в банкомате. Наружу уходит свёртка пин-кода и она даже шифруется приватным ключом, по ней нельзя восстановить сам пинкод.

Да есть конечно варианты настроек терминалов где все гуляет чуть ли не а открытом виде или используется DES вместо 3DES, но это все от людской глупости и лени сотрудников банков и т.п.

Ответить

tbicr 21 июн 2016 в 14:25

> Как известно, согласно PCI-DSS, платёжная система не должна хранить у себя так называемые Критичные аутентификационные данные (КАД), к которым относят, к примеру, CVV или PIN-код (последний обычно поступает из POS-терминалов супермаркетов).

Интересно как работают рекурентные платежи, если CVV не должен храниться?

Ответить

isden 21 июн 2016 в 16:58

Либо через механизм токенизации, либо через встроенную фичу платежки (емнип, в PayPal/Payflow такое было).

Ответить

realcnbs 21 июн 2016 в 23:02

Обычно шлюзы их не требуют для повторных платежей, но тут конечно, всё индивидуально.

Ответить

Belya-Dj 22 июн 2016 в 12:21

Ну если со стороны API — то как-то вот так
developer.authorize.net/api/reference/features/customer_profiles.html

Ответить

hamsterr 21 июн 2016 в 18:03

читаю ваш блог и в процессе появилось несколько вопросов: что собственно представляет процесс токенизации, если платежная система (учитывая PCI DSS) имеет право хранить только номер карты в зашифрованном виде, то как происходит сборка данных о карте при связке с банком-эквайром?

Ответить

akubintsev 22 июн 2016 в 17:16

Токен выдает банк-эквайр.

Ответить

hamsterr 22 июн 2016 в 17:24

выходит, что если человек согласен привязать карту, то при повторном платеже, в банк нужно будет отправлять зашифрованный номер карты + токен и этого достаточно для проведения платежа (+3D secure)?

Ответить

akubintsev 22 июн 2016 в 17:30

Обычно отправляется токен, сумма для списания. Дальше при необходимости уже 3D secure дергается со стороны банка эквайера. Номер карты передавать уже не нужно.

Ответить

tstyopin 21 июн 2016 в 23:02

О самой сертификации ни слова :)
Труд не титанический, проходим в шестой раз.
Из пунктов приёма карт — 90+ гипермаркетов и 100+ супермаркетов двух торговых сетей, сайт, скоро будет мобильное приложение.
Расскажите лучше большой обзорной статьёй об инновационных методах платежа, которые используете.
Стандарты хорошо применимы и БЕЗ платежей, в обычной сети, т.к. вводят нормальные точки контроля
Ну и да, www.pcidss.ru (Обратите внимание, не httpS) — все актуальные документы.

Ответить

Только полноправные пользователи могут оставлять комментарии. Войдите, пожалуйста.

Публикации

ЛУЧШИЕ ЗА СУТКИ ПОХОЖИЕ

a_chibisov 21 дек в 20:29

Мой заржавелый мозг кипел. Я думал, что в 40+ лет нет смысла даже пытаться. Зачем предпринимателю идти в IT

Простой 9 мин 31K

Из песочницы Хабр IT-гид

+41 79 16 +16

BabayMazay 12 часов назад

Ручная работа со стеклом. Соединение деталей в плоские и объёмные конструкции

Средний 7 мин 1.2K

Обзор

+32 15 4 +4

OlegSivchenko 21 дек в 23:16

Несвоевременная технология подземных лодок и геоходов

8 мин 4.5K

+31 16 45 +45

nmgtech 8 часов назад

Я счастлив, что больше не веб-разработчик

5 мин 6.6K

Мнение Перевод

+22 15 13 +13

ru_vds 8 часов назад

OpenAPI станет проще: готовится версия 4.0

Простой 7 мин 1.5K

Обзор

+22 15 0

PatientZero 11 часов назад

Простой саботаж в мире ПО

6 мин 3.9K

Мнение Перевод

+17 37 10 +10

Pavel_Agafonov 21 дек в 23:45

Есть ли Undefined Behavior в Rust?

Средний 3 мин 3.3K

Из песочницы

+16 21 10 +10

Milfgard 14 часов назад

Чьи права на то, что сделала нейросеть

12 мин 2.7K

+15 24 23 +23

IgnatChuker 7 часов назад

Интервью с руководителем отдела анализа защищённости Angara Security Михаилом Суховым о пентесте

Простой 7 мин 304

Интервью

+14 0 2 +2

RSHB_INTECH 12 часов назад

Прокрастинация как инструмент для развития карьеры

Простой 7 мин 1.5K

Мнение

+13 15 0

Показать еще

ИНФОРМАЦИЯ

Настройка языка

Техническая поддержка

4K 0

1 авг 2017 в 12:57

Мобильная коммерция с социальным подтекстом

3.8K 0

19 июл 2017 в 12:02

«Сири, станет ли HomePod большим хитом»

6.7K 18 +18