КАК СТАНДАРТ PCI DSS ПОМОГАЕТ ПОДНЯТЬ УРОВЕНЬ БЕЗОПАСНОСТИ В ЦЕНТРЕ ОБРАБОТКИ ДАННЫХ

Значительная часть предприятий и организаций размещает свои информационные системы в крупных data-центрах на условиях аутсорсинга. Размещение на внешней площадке позволяет обеспечить условия для надежной бесперебойной работы IT-оборудования. Применение стандарта информационной безопасности индустрии платежных карт (PCI DSS) помогает добиться гарантированной защищенности данных. В статье отражен опыт внедрения PCI DSS в крупнейшем на Северо-Западе России центре обработки данных ООО «СДН».

КЛЮЧЕВЫЕ СЛОВА: информационная безопасность, управление рисками, платежные системы, центры обработки данных

Золотарев Михаил Юрьевич — начальник отдела управления проектами в ООО «Стек Дата Нетворк» (г. Москва)

П. 7.1.3 ISO 9001-2015 [1] требует, чтобы организация определила, создала и поддерживала инфраструктуру, необходимую для функционирования ее процессов. Учет требований информационной безопасности при размещении серверного оборудования в коммерческом data-центре и получение значимых свидетельств соответствия им являются важной составляющей менеджмента качества практически любого предприятия. Отраслевой стандарт индустрии платежных карт — хорошая база для выстраивания ответственных отношений между оператором и клиентом центра обработки данных (ЦОД), для распределения ответственности и управления рисками.

На современном рынке, насыщенном информацией, аутсорсинг размещения серверного оборудования играет важную роль — центры обработки данных обеспечивают предприятия и организации высоконадежной инфраструктурой при умеренных затратах. В России уже прочно закрепилось его название «колокейшн» (от англ. colocation — кооперативное размещение).

Отраслевые стандарты ЦОД

В настоящее время из специфических стандартов для центров обработки данных наибольшее распространение нашли два, созданные Uptime Institute LLC:

- Tier Standard: Topology;
- Tier Standard: Operation Sustainability.

Первый относится к конфигурации инженерных систем, прежде всего электропитания и охлаждения, и применяется на этапах их проектирования и приемки в эксплуатацию. Второй увязывает рабочие процедуры эксплуатации с тем уровнем надежности, который должна обеспечивать заложенная в проект топология. При этом основное внимание в стандартах уделяется организации технического обслуживания и управления мощностями, а относительно обеспечения безопасности против злоумышленников приведены лишь базовые требования.

В 1990-х гг. рост количества и размеров ЦОД привел к качественному изменению бизнес-модели их операторов. Изначально ЦОД являлись подразделениями компаний — операторов связи, и размещение IT-оборудования предлагалось в качестве дополнения к услугам передачи данных. При этом тарифы и политика подразумевали преимущественное использование каналов связи «своего» провайдера. По мере роста размеров ЦОД, необходимых инвестиций, повышения зрелости рынка услуг такая модель стала сдерживающим фактором. Ответом было появление концепции Carrier Neutral — в ней data-центр позволяет всем операторам связи иметь равный доступ ко всем клиентам. Фактически это ознаменовало формирование самостоятельного рынка услуг ЦОД, независимого от рынка связи и доступа к сети Интернет.

В большом ЦОД удельные затраты на обеспечение бесперебойного питания, охлаждения и каналы связи гораздо ниже, чем в серверной комнате на десяток стоек. Ставший нормой уровень непрерывности, при котором периоды бесперебойности достигают нескольких лет, требует особых компетенций менеджмента и специалистов, и оплачивать эти компетенции для эксплуатации непрофильного актива (собственной серверной) непозволительно дорого.

Реализация концепции Carrier Neutral в России началась с 2004 г., когда группа специалистов под брендом «Стек» открыла первый коммерческий ЦОД в Москве. По сегодняшним меркам его никак нельзя назвать крупным, но тогда он был безусловным лидером. Успех был закреплен в 2007 г. запуском площадки «M1», которая функционирует и развивается и поныне. Третьим серьезным проектом под нашим брендом стал запуск крупнейшего на Северо-Западе РФ модульного ЦОД в Санкт-Петербурге. Этот новый ЦОД «СДН» имеет полную проектную мощность в 1500 стоек, из которых в настоящее время введено в эксплуатацию свыше 1000. Присоединение к электрическим сетям выполнено на 10 МВт, имеется возможность расширения до 14 МВт и далее.

Считается, что в нашей стране капитальные затраты на одну стойку в крупном современном ЦОД находятся в пределах $40–60 тыс. При таком уровне гарантируется неограниченная по времени автономность при авариях городской электрической сети, а любое обслуживание или ремонт оборудования инженерных систем происходит без отключения IT-оборудования клиентов. Достигнуть подобного уровня для отдельной серверной комнаты в офисном здании практически нереально даже при затратах, в несколько раз бо́льших. К тому же data-центр как крупный промышленный объект подключен непосредственно к подстанции 110/10 кВ, а статистика сбоев в сетях высокого напряжения как минимум на порядок лучше, чем для потребителей низкого напряжения.

Однако, несмотря на общепризнанные преимущества размещения в коммерческом data-центре, на профессиональных форумах по IT и безопасности продолжается обсуждение того, допустимо ли использование colocation для систем, обрабатывающих, например, платежные транзакции и другие банковские данные. Скептики апеллируют к общепринятым подходам и даже регуляторным требованиям, хотя последние не содержат фактических запретов.

На первый взгляд может показаться, что безопасность проще обеспечить, если и офис, где

работают финансисты, и серверы находятся под одной крышей, в одном периметре безопасности. Однако опыт подсказывает, что ключевым фактором обеспечения надежной защиты информации являются грамотные организационные решения, и безопасность на аутсорсинге зачастую намного выше, чем при использовании собственных ресурсов.

В любом реальном процессе обработки платежных данных участвует целая цепочка организаций, и общепринятые подходы к обеспечению безопасности работают именно в сети, распределенной территориально и между организациями. Недавний опыт сертификации data-центра по стандарту PCI DSS позволяет наглядно показать, как в коммерческом data-центре может быть установлен гарантированный проверяемый уровень информационной безопасности.

Стандарт безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard) [2] разработан в целях повсеместного внедрения единообразных мер по защите данных платежных карт (в терминологии стандарта — «данных держателей платежных карт»). Его требования применимы ко всем участникам хранения, обработки и передачи таких данных, от кассового терминала в торговом центре до процессинговых центров, банков эмитентов и эквайеров. Стандартом вводится понятие информационной среды держателей карт как совокупности людей, процессов и технологий, задействованных в этой деятельности.

Как и в большинстве отраслевых стандартов качества, соотношение организационных и технических требований в PCI DSS примерно 70% к 30%. В него включена концепция непрерывного улучшения. Стандарт устанавливает:

- типы данных и их сочетания, которые можно хранить в открытом виде, в зашифрованном виде, а также не подлежащие хранению (например, PIN-код);
- разграничение доступа (видимость данных должна строго ограничиваться областью, необходимой для выполнения конкретных обязанностей каждого участника);
- меры по защите от несанкционированного доступа и выявлению программных и аппаратных «закладок» (злонамеренно созданных уязвимостей);
- правила сегментации сети, применения брандмауэров, шифрования каналов и т.п.;
- перечень мероприятий, касающихся человеческого фактора, от повышения осведомленности до управления инцидентами.

Исторически каждая из пяти основных мировых платежных систем внедряла свою политику безопасности:

- Visa Cardholder Information Security Program;
- MasterCard Site Data Protection;
- American Express Data Security Operating Policy;
- Discover Information Security and Compliance;
- JCB Data Security Program.

Для унификации 15 декабря 2004 г. была выпущена первая версия стандарта безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard — PCI DSS). Стандарт состоит из 12-ти детализированных требований, покрывающих все аспекты противодействия преднамеренным и непреднамеренным утечкам информации, от шифрования до организации прохода в помещения. Продвижение стандарта проводится самими платежными системами. Например, в 2006 г. международной платежной системой Visa он введен как обязательный в Центральной и Восточной Европе. Это означает, что процессинговые центры, платежные шлюзы и другие поставщики услуг, работающие напрямую с VisaNet, должны подтвердить соответствие его требованиям. К настоящему времени требования стандарта закреплены законодательно тремя штатами США — Миннесотой, Невадой и Вашингтоном. В сентябре 2007 г. был создан совет (Payment Card Industry Security Standards Council — PCI SSC), под эгидой которого происходит постоянное обновление стандарта в рамках трехлетнего цикла: первый год — внедрение версии, второй год — сбор обратной связи, третий год — подготовка новой версии. Для этого ежегодно проводятся конференции — PCI SSC Community Meeting, состоящие из американской и европейской сессий. На сегодняшний день последней является версия 3.2, принятая в апреле 2016 г.

Организация, должным образом подтвердившая (с использованием внешнего аудита, внутреннего аудита или самооценки, в зависимости от ее

роли в обработке данных и объема транзакций) свою способность обеспечивать и постоянно улучшать уровень информационной безопасности, получает лучшие условия при взаимодействии с другими участниками индустрии платежных карт, в том числе по комиссиям и страховым отчислениям.

В стандарте специально оговорено, что организация, поставляющая услуги в режиме аутсорсинга, может проходить проверки в рамках аудита каждого из своих клиентов или самостоятельно пройти оценку и предоставлять ее результаты своим клиентам.

Требования стандарта затрагивают все аспекты деятельности по хранению и обработке данных: и физическую безопасность, и шифрование, и администрирование сетевых устройств и серверов. Понятно, что оператор ЦОД имеет отношение только к той их части, которая связана с физическим уровнем информационных систем, прежде всего с физическим доступом к IT-оборудованию.

Одним из ключевых моментов для реализации проектов, связанных с организацией обработки данных на аутсорсинге, является соглашение о разделении ответственности между оператором и клиентом ЦОД. В нем указано, какие из требований должны быть реализованы на стороне клиента, а какие берет на себя оператор ЦОД. По некоторым пунктам разделение осуществляется в зависимости от объекта (например, клиент отвечает за журналирование доступа на уровне отдельных носителей информации, а оператор — на уровне серверов) (см. таблицу).

Соглашение оформляется в виде приложения к договору с клиентом, заинтересованным в соответствии PCI DSS. Когда клиент сам проходит аудит, он «закрывает» соответствующую часть требований ссылкой на сертификат оператора.

В нашем случае в зону ответственности оператора ЦОД вошли следующие направления:

- ограничение физического доступа в офисные помещения и сам ЦОД, видеонаблюдение, идентификация и авторизация лиц, посещающих эти помещения;
- ограничение доступа к сетевым разъемам и беспроводным сетям;
- строгий учет вноса-выноса оборудования, который осуществляется только после соответствующего утверждения;
- регулярные проверки отсутствия неавторизованных точек беспроводного доступа, которым в стандарте уделено особое внимание.

Естественно, реализованы и общие для большинства стандартов менеджмента качества требования, обеспечивающие организационную базу для результативной работы, повышения осведомленности персонала, внутренних аудитов, поддержания документированных процедур в актуальном состоянии.

Надо особо отметить: внимание, уделяемое руководством ЦОД вопросам безопасности при реализации требований стандарта, приводит к повышению уровня безопасности для всех клиентов, позволяет избежать типичных ошибок и выстроить работу в соответствии с лучшим мировым опытом.

Не секрет, что деятельность по обеспечению безопасности предприятий чаще всего возглавляют сотрудники правоохранительных органов в отставке, чьи привычные подходы к работе и мышление отличны от характерных для специалистов сферы бизнеса и продаж. Стандарт помогает сочетать опыт этих профессионалов с корпоративной культурой, позволяет гармонизировать всю систему управления, снизить уровень напряженности в отношениях между службой безопасности и другими подразделениями, резко поднять продуктивность работы. Правильность этого подхода подтверждается клиентами data-центра «СДН», значительная доля которых относится к финансовому и банковскому секторам (см. рисунок).

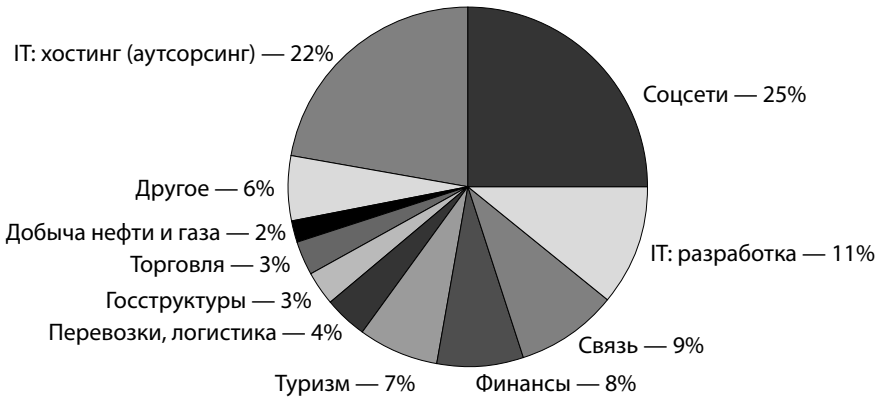
При проектировании ЦОД мы ориентировались помимо СНиПов, ПУЭ и других обязательных регламентов на TIA-942 и Uptime Institute Tier Standard: Topology.

Стандарт TIA-942 покрывает практически все аспекты устройства ЦОД, но требует серьезной адаптации, начиная с перевода размеров

Таблица. Фрагмент соглашения между оператором и клиентом о разделении ответственности

Требования	Ответственная сторона
Вести список авторизованных беспроводных точек доступа с указанием их необходимости для осуществления деятельности	Оператор ЦОД
Внедрить процедуры реагирования на обнаружение неавторизованных беспроводных точек доступа	Оператор ЦОД
Проводить внешнее и внутреннее сканирование сети на наличие уязвимостей не реже одного раза в квартал, а также после внесения значительных изменений (например, установки новых системных компонентов, изменения топологии сети или правил межсетевых экранов, обновления продуктов). Примечание: при проведении ежеквартального сканирования можно объединить несколько отчетов о его результатах для подтверждения того, что все системы были просканированы, а все найденные уязвимости устранены. Может потребоваться дополнительная документация для подтверждения того, что неустраненные уязвимости находятся в процессе ликвидации	Клиент

Рисунок. Распределение клиентов «СДН» по отраслям



в метрическую систему и заканчивая учетом требований пожарной безопасности, которые у нас кардинально отличаются от американских. Применяя его, надо учитывать, что приложения этого стандарта, касающиеся инженерных систем, безопасности и архитектуры, являются справочными. Это не требования, на соответствие которым проводилась бы формальная проверка и сертификация, т.е. это не догма, а руководство к действию.

UI Tier Standard: Topology невелик по объему, но требует глубокого понимания при применении. В начале 2000-х гг. в профессиональной среде сложилось много неверных стереотипов, связанных с ним, поскольку шкала Tier была «арендована» разработчиками TIA-942. В результате справочные таблицы и иллюстративные схемы зачастую воспринимались как обязательные требования, а статистика 1990-х гг. по готовности ограниченной выборки реальных ЦОД почему-то превратилась в нормативные значения, особенно для маркетологов и составителей SLA. Окончательно разобраться в этих вопросах нам помогло

живое общение со специалистами российского представительства UI. В сегодняшней редакции стандарта от 2012 г. гораздо меньше возможностей для недопонимания.

UI Tier Standard: Topology устанавливает требования именно к топологии инженерных систем, оставляя пользователям полную свободу в выборе схем и оборудования (нормируется лишь запас по производительности). Если читать стандарт правильно, то обнаружится, что нет никаких оснований не применять его последовательно для каждого ЦОД. Квалифицированный потребитель вполне может по однолинейной схеме составить обоснованное суждение о заложенной в проект надежности.

Однако не следует забывать, что этот стандарт помогает избежать ошибок только на уровне топологии и выбора номиналов производительности. Выбор конкретного производителя с учетом его способности оказать поддержку при проектировании и обеспечить последующее сопровождение на весь срок эксплуатации остается важнейшей задачей инженерной группы проекта. Здесь интересно отметить опыт работы с нашими двумя основными партнерами, отвечающими за бесперебойное питание и охлаждение. Обе компании из Нидерландов. Первая на рынке с 1956 г., у нее очень солидный и обстоятельный стиль работы по любым вопросам. Вторая начала свою деятельность в 2008 г. и работает менее формально, но очень эффективно. Для обеих непрерывность работы ЦОД клиента стоит на первом месте.

Наш опыт показывает, что нельзя недооценивать вопрос выбора площадки. ЦОД — инфраструктурный объект, а значит, инвестиция долговременная. Любые «сюрпризы» в вопросах использования земли или подключения к сетям тут неприемлемы, а любые посредники излишни. За счет присоединения с возможностью прямого выхода на рынок электроэнергии можно сэкономить не меньше, чем за счет энергоэффективных решений внутри ЦОД. Одной из причин открытия первого ЦОД «СДН» именно в Санкт-Петербурге было то, что там благодаря политике руководства города имелись реальные возможности приобрести в собственность «чистый» участок с присоединением к сетям. В Москве сделать это гораздо сложнее.

На рынке ЦОД произошло резкое обострение конкуренции, близкое к ценовой войне. Это связано с падением спроса после 2014 г. и выходом на рынок проектов, начатых в 2011 г. и позже. Сегмент малого бизнеса практически свернулся, средний продлевает срок службы имеющегося оборудования, немногочисленные стартапы ориентируются исключительно на облачные сервисы с минимальными начальными вложениями. Оставшийся спрос сосредоточен в крупных корпорациях, в том числе тех, для которых IT являются основной специализацией (социальные сети и т.п.). Специалисты таких клиентов тщательно вникают во все подробности проектов, организации эксплуатации и обслуживания, безопасности при выборе ЦОД.

Экономическая эффективность проекта ЦОД в целом сильно зависит от деталей финансирования, от того, в какой валюте привлекались средства, по какому курсу покупалось оборудование. Это влияет не только на срок окупаемости, но и на устойчивость организации в целом, но данная тема выходит за рамки разговора о стандартах.

ИСТОЧНИКИ

1. Системы менеджмента качества — требования. — http://pqm-online.com/assets/files/pubs/translations/std/iso-9001-2015-(rus).pdf.
2. Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования и процедуры аудита безопасности. — http://pcidss.ru/files/pub/pdf/1_PCI_DSS_v3.pdf.
3. ЦОД СДН сертифицирован по стандарту PCI DSS. — http://stackdata.net/market-press/news/tsod-sdn-sertifitsirovan-po-standartu-pci-dss/.
4. *PCI Security Standards Council*. — https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss.