Перспективы информационной безопасности

100 вопросов, касающихся формирования комплексного подхода к информационной безопасности, которые нужно обсудить с поставщиками технологий

Джон Саффолк

Старший вице-президент
Руководитель глобальной службы информационной безопасности
Huawei Technologies

Декабрь 2014 г.

HUAWEI

Авторы

Я хотел бы выразить благодарность всем, кто внес вклад в создание этого документа. Вот имена этих людей: Хэрри Лю, Джефф Нэнь, Джупитер Ванг, Дэвид Франсис, Энди Перди, Дебу Найак, Питер Росси, Энди Хопкинс, Джесси Луо, Уэйв Сюэ, Нэнси Ли, Вут ван Вейк, Уильям Пламмер, Людовик Петит, Ульф Фегер, Дэвид Му, Эрик Янг, а также все, кто прямо или косвенно помогал в работе над этим докладом. Прошу меня простить, если я не упомянул чье-то имя, и принять мою искреннюю благодарность за оказанную поддержку.

Джон Саффолк

СОДЕРЖАНИЕ

Декабрь 2014 г.

1. Краткий обзор

В нашем докладе ***«Интеграция информационной безопасности в ДНК компании: комплекс интегрированных процессов, политик и стандартов»***, опубликованном в октябре 2013 г.,[1] мы подробно описали наш комплексный подход к процессам обеспечения информационной безопасности. Мы заявили о нашем намерении составить список из 100 вопросов по информационной безопасности, которые задали нам клиенты. По сути, в нем можно найти вопросы, которые, возможно, каждый хотел задать своему поставщику технологий, когда речь заходила об информационной безопасности. В настоящем докладе эти 100 вопросов рассматриваются подробно, а сам список представляет собой перечень важных аспектов, которые покупателям технологий следует выяснять у своих поставщиков.

Он служит некоторым шаблоном для покупателей, разработанным на основе вопросов, заданных компании Huawei, а также нашей оценки ряда «стандартов» и передового опыта. Участвуя в тендерах, покупатели смогут с помощью этого списка систематически анализировать возможности поставщиков в области информационной безопасности.

Для подробного изучения этих 100 вопросов мы обратились ко многим источникам.

- В первую очередь, мы внимательно прислушивались к нашим клиентам. Каковы их проблемы и заботы? О чем они беспокоятся? Каковы их требования, требования их отрасли или их государства?
- Являясь лидерами отрасли ИКТ и охватывая всю сферу деятельности от крупномасштабной телекоммуникационной инфраструктуры до облачных вычислений, предоставления решений для предприятий и отдельных пользователей, мы обладаем ценным преимуществом в виде знаний наших 150 000 сотрудников, ученых и инженеров. Мы взяли на вооружение их знания и стремление правильно оценить ситуацию.
- Наконец, чтобы достичь определенного уровня последовательности, мы тщательно изучили более 1 200 «стандартов», статей и примеров «лучших практик».

Мы осознаем тот факт, что возрастают правовые и отраслевые требования, касающиеся информационной безопасности. Не редкость наблюдать за тем, как правительства и контролирующие органы начинают передавать обязательства, а также последующую ответственность за нарушения в области информационной безопасности операторам важнейших национальных инфраструктур и поставщикам компьютерных или ИТ-услуг. Все больше компаний будут вынуждены подробно излагать свой подход к информационной безопасности и обозначать, какие анализы и оценки они применяют в отношении поставщиков технологий и услуг.

Проходит то время, когда поставщик услуг мог сказать «я не знал» или «я думал, что они надежные и функциональные». Времена, когда покупатели технологий не прибегали к единообразной системе вопросов по оценке всех своих поставщиков, заканчиваются. В мире глобальных взаимосвязей угрозы могут поступить (и поступают) откуда угодно. Этот список из 100 вопросов может послужить отправной точкой в деле снижения риска при оценке возможностей вашего поставщика в сфере информационной безопасности. И, самое главное, мы считаем, что, чем более взыскательными становятся покупатели и чем более последовательны они в своих требованиях относительно гарантий информационной безопасности, тем выше вероятность того, что поставщики ИКТ будут вкладывать деньги и повышать свои стандарты безопасности.

Основная часть доклада посвящена подробному рассмотрению 100 вопросов, которые, согласно нашим исследованиям, необходимо учитывать при выборе поставщиков технологий. Они подразделены на группы, охватывающие следующие аспекты: стратегия, управление и контроль; стандарты и процессы; законы и нормативно-правовые акты; человеческий фактор; исследования и разработки; проверка; управление сторонними поставщиками; производство; безопасное предоставление услуг; выявление и устранение проблем, дефектов и уязвимостей и, наконец, аудит.

[1] http://pr.huawei.com/en/news/hw-310599-cyber.htm

В каждом разделе представлен ряд требований, которые стоит предъявить вашим поставщикам технологий. Также мы приводим дополнительное разъяснение относительно того, почему это может оказаться важным. Некоторые из этих вопросов могут быть полезны для ваших собственных предприятий с точки зрения предоставления информации о том, на что, вероятно, обратят внимание внутренние аудиторы, что может заинтересовать ваше правление и о чем может спросить совет директоров или аудиторский комитет.

В заключение мы обращаемся с несколькими просьбами к органам стандартизации.

- Во-первых, нам необходимо объединиться и уменьшить частичное совпадение и дублирование различных стандартов.
- Во-вторых, необходимо изменить структуру различных стандартов таким образом, чтобы они были построены на основе единообразных блоков. Например, блок ***«управление и контроль»*** должен быть единым для всех стандартов, в которых необходимо отразить этот аспект, а не присутствовать во многих стандартах в виде несколько отличающегося модуля.
- В-третьих, нам нужно по мере возможности сфокусироваться на выходных показателях, а не на определении входных данных или задачи.

Со своей стороны, мы призываем компании, политических деятелей, поставщиков и покупателей, рассматривать этот перечень ТОП-100 вопросов в качестве «версии 1.0» и вносить предложения о том, как его можно улучшить. В этом контексте, мы рады сообщить, что EastWest Institute (EWI) дал свое согласие, приняв данный Топ-100 за основу и используя свои обширные знания и контакты, курировать эволюцию обновленных и более проработанных версий. Мы с нетерпением ждем, что концепция Top 100 станет неотъемлемой составляющей при формировании покупательских оценок и поможет отрасли ИКТ совершенствовать продукты и услуги в отношении безопасности, новых разработок и размещения.

2. Введение

В нашем докладе ***«Интеграция информационной безопасности в ДНК компании: комплекс интегрированных процессов, политик и стандартов»***, опубликованном в октябре 2013 г.,[2] мы подробно описали наш комплексный подход к процессам обеспечения информационной безопасности. Мы заявили о нашем намерении составить список из 100 вопросов по информационной безопасности, которые задали нам клиенты. По сути, в нем можно найти вопросы, которые, возможно, каждый хотел задать своему поставщику технологий, когда речь заходила об информационной безопасности.

Мы назвали этот список «Предоставление информации в ответ на запросы» (Reverse Request for Information — RFI). В сущности, это список возможных требований к информационной безопасности, которые следует учитывать при выборе поставщика. Иными словами, мы повернули этот процесс в противоположном направлении, когда стали просить клиентов задавать нам вопросы о том, как мы решаем проблемы кибербезопасности.

В данном, третьем по счету, докладе представлены все 100 вопросов, а также подход, который мы выбрали для их решения.

Начнем с обсуждения того, по каким причинам разработка, согласование и реализация набора международных стандартов, норм и практик в области информационной безопасности оказываются настолько трудно выполнимыми задачами. Связано ли это с тем, что выгода от их достижения не стоит затрачиваемых усилий? Очевидно, что это утверждение не может быть справедливым в свете заявлений о значительных убытках, понесенных в результате киберпреступлений. Является ли это следствием того, что данные вопросы не входят в число корпоративных или политических задач? Тоже

[2] http://pr.huawei.com/en/news/hw-310599-cyber.htm

нет, принимая во внимание количество международных правительственных конференций по вопросам преступности в компьютерной сфере и нашумевшие сообщения в прессе об утечках данных, ущербе интеллектуальной собственности и нарушении предоставления онлайн-обслуживания из-за сетевых атак. Возможно, масштаб задачи слишком велик, и мы не знаем, с чего начать, а возможно, существует очень много разных взглядов на «стандарты», «лучшую практику» и «указания». Безусловно мы согласимся с тем, что эта ситуация может послужить сопутствующим фактором и, как мы заявили в предыдущем докладе, «проблема стандартов в том, что они нестандартны».

Наконец, если проанализировать доступные материалы, то окажется, что в основном они нацелены на предприятие или государственное учреждение, иногда — на конечного потребителя и почти нет таких, которые были бы ориентированы на производителя программного или аппаратного обеспечения — поставщика.

В действительности, учитывая размах технологий, мы никогда не придем к «единому стандарту». Однако в наших силах сосредоточиться на требованиях, часто описываемых (возможно, различными словами) во многих стандартах, кодексах и лучших практиках, но рассмотреть их с точки зрения коллективных мер, которые поставщики могут предпринять для повышения безопасности своих продуктов.

В данном докладе мы обратимся к самым распространенным вопросам нетехнического свойства, которые клиенты и другие заинтересованные стороны задают нам, когда речь заходит об информационной безопасности. В этом контексте определение «самые распространенные» также относится к тем вопросам, которые порождают больше всего обсуждений, проверок или уточнений. Мы прибегли к «поэтической вольности», чтобы модифицировать адресованные нам вопросы и придать им обобщенный характер. Кроме того, мы добавили вопросы, которые отражают последние события, например разоблачения Сноудена, а также недостающие вопросы для обеспечения полноты каждого раздела.

Внося свой вклад в текущую дискуссию и работу по определению «что такое хорошо» в сфере информационной безопасности, мы выдвигаем эти вопросы в рамках нашей совместной деятельности по постоянному расширению знаний.

Подробно изучая упомянутые вопросы, мы не пытаемся присвоить им приоритет и включить их в какую бы то ни было систему или методологию. По сути, для каждого ключевого процесса Huawei мы определили, каким образом тот или иной вопрос представлен в рамках этого процесса.

Этот список по определению не может подходить для любой отрасли и принимать во внимание все законы и технические стандарты: цель его создания заключается в другом. Он служит некоторым шаблоном для покупателей, разработанным на основе вопросов, заданных компании Huawei, а также нашей оценки «стандартов» и передового опыта. Участвуя в тендерах, покупатели смогут с помощью этого списка систематически анализировать возможности поставщиков в области информационной безопасности. Они смогут использовать эту информацию для повышения качества своих запросов на получение информации или запросов на предложения (Requests for Proposals — RFPs) в поиске лучших поставщиков для удовлетворения своих текущих и долгосрочных потребностей в технологиях.

Мы абсолютно уверены, что, чем более взыскательными становятся покупатели и чем более последовательны они в своих требованиях относительно гарантий информационной безопасности, тем выше вероятность того, что поставщики ИКТ будут инвестировать и повышать свои стандарты безопасности.

Вместе мы сможем повысить качество мер по обеспечению безопасности в рамках технологических продуктов и услуг и, таким образом, внести больший вклад в обогащение жизни людей посредством использования ИКТ.

3. Методология обнаружения и решения проблем

Для подробного изучения этих 100 вопросов мы обратились ко многим источникам.

- В первую очередь, мы внимательно прислушивались к нашим клиентам. Каковы их проблемы и заботы? О чем они беспокоятся? Каковы их требования, требования их отрасли или их государства? В этом отношении нам повезло принимать тысячи посетителей в нашем головном офисе в Шэньчжэне, где мы демонстрируем наши ценности, возможности, политики и подход — все это стимулирует появление множества вопросов и идей, и мы благодарим наших гостей за всю ценную информацию.
- Являясь лидерами отрасли ИКТ и охватывая всю сферу деятельности от крупномасштабной телекоммуникационной инфраструктуры до облачных вычислений, предоставления решений для предприятий и отдельных пользователей, мы обладаем ценным преимуществом в виде знаний наших 150 000 сотрудников, ученых и инженеров. Мы взяли на вооружение их знания и стремление правильно понять ситуацию.
- Компания Huawei с энтузиазмом поддерживает основные международные стандарты и принимает активное участие в их формулировке. К концу 2012 года компания Huawei присоединилась более чем к 150 организациям по стандартизации в отрасли, в том числе 3GPP, IETF, ITU (Международный союз электросвязи), OMA, ETSI (Европейский институт стандартов по телекоммуникациям), TMF (Tele Management Forum), ATIS, IEEE, 3GPP и Open Group. Всего компания Huawei подала в эти органы стандартизации более 5 000 предложений. Также мы занимаем 180 должностей в организациях, поддерживающих стремление к согласованным международным стандартам. Что касается стандартов и базовых концепций, то мы внесли свой вклад в разработку недавно появившейся базовой программы Национального института стандартов и технологии США (National Institute of Standards and Technology — NIST), поддержали оптимизацию стандарта ISO27001 и выступаем в роли активного участника в работе и развитии концепции ITU and 3GPP. Составляя список из 100 вопросов, мы часто опирались на этот материал.
- Наконец, чтобы достичь определенного уровня последовательности, мы тщательно изучили более 1 200 «стандартов», статей и примеров «лучших практик».

Как бы то ни было, наш список из 100 вопросов не стоит рассматривать в качестве полного перечня требований, которые вы предъявите вашему поставщику, однако мы надеемся, что многие из вас используют данный документ в качестве справочного материала. Задать вопрос несложно, но требуется определенный навык, чтобы понять ответ, убедиться в его точности, наглядности и доступности для проверки.

В заключение мы обращаемся с несколькими просьбами к органам стандартизации.

- Во-первых, нам необходимо объединиться и уменьшить частичное совпадение и дублирование различных стандартов.
- Во-вторых, необходимо изменить структуру различных стандартов таким образом, чтобы они были построены на основе единообразных блоков. Например, блок «управление и контроль» должен быть единым для всех стандартов, в которых необходимо отразить этот аспект, а не присутствовать во многих стандартах в виде несколько отличающегося модуля.
- В-третьих, нам нужно по мере возможности сфокусироваться на выходных показателях, а не на определении входных данных или задачи.

Со своей стороны, мы будем рады получить ваши отзывы по поводу этого списка из 100 вопросов (что нам следует добавить, исключить или изменить), чтобы в будущем мы смогли разработать новую версию с учетом ваших дополнительных предложений.

4. Вопросы и аспекты, которые необходимо учитывать в процессе разработки устойчивой программы по обеспечению информационной безопасности

Мы осознаем тот факт, что возрастают правовые и отраслевые требования, касающиеся информационной безопасности. Не редкость наблюдать за тем, как правительства и контролирующие органы начинают передавать обязательства, а также последующую ответственность за нарушения в области информационной безопасности операторам важнейших национальных инфраструктур и поставщикам компьютерных или ИТ-услуг. И это представляет определенную трудность, поскольку в случае, например, значительной утери данных или невыполнения обслуживания правительство или контролирующий орган, скорее всего, спросит поставщика услуг о его подходе к информационной безопасности (полагая, что это был инцидент в системе безопасности). Все больше компаний будут вынуждены подробно излагать свой подход к информационной безопасности и обозначать, какие анализы и оценки они применяют в отношении поставщиков технологий и услуг. Трудность усиливается под влиянием того факта, что в самом широком смысле информационная безопасность — это комплекс, охватывающий аспекты от правовой базы до производства, от услуг до человеческого фактора, от управления до исследования и разработки. Немного найдется людей в мире с таким широким кругозором и глубиной знаний, поэтому мало кто имеет представление о том, какие вопросы следует задавать и какие доказательства искать.

Проходит то время, когда поставщик услуг мог сказать «я не знал» или «я думал, что они надежные и функциональные». Времена, когда покупатели технологий не прибегали к единообразной системе вопросов по оценке всех своих поставщиков, заканчиваются. В мире глобальных взаимосвязей угрозы могут поступить (и поступают) откуда угодно. Этот список из 100 вопросов может послужить отправной точкой в деле снижения риска при оценке возможностей вашего поставщика в сфере информационной безопасности.

В данном разделе вы найдете 100 требований, которые, по нашему мнению, стоит учитывать при оценке возможностей ваших поставщиков в отношении безопасности. Не все из них применимы к любым ситуациям. Не все из них применимы ко всем уровням структуры вашей организации. Не все из них применимы к любым приобретениям. Мы надеемся, что с помощью этого списка вы получите более четкое представление о том, на какие аспекты вам следует обращать внимание при выборе поставщиков, и что, дополнив некоторые пункты в этом списке собственными требованиями, вы заставите каждого поставщика технологий еще больше сосредоточиться на безопасности.

Вопросы разделены на те же группы, что и наш второй доклад, опубликованный в 2013 г. В том документе мы представили всестороннее рассмотрение нашего подхода к информационной безопасности.

Изучая список из 100 вопросов, вы можете посчитать, что некоторые вопросы можно было бы объединить. Мы долго и усердно думали над этим и попытались сделать вопросы в достаточной степени конкретными. Чем больше мы будем обобщать, тем выше вероятность отвлечься от главного. Тонкость некоторых вопросов влечет такую ситуацию, когда уточняющий вопрос перемещается на другой этап жизненного цикла или процесса и приобретает несколько другой оттенок. По желанию вы можете свободно видоизменять их, поскольку нашим первоочередным стремлением является повышение качества мер по обеспечению безопасности среди всех поставщиков технологий.

4.1. Стратегия, управление и контроль

Если информационная безопасность не является приоритетом для Совета директоров и высшего руководства компании, она не будет приоритетом и для сотрудников организации. Внедрение и обеспечение информационной безопасности в структуре организации, стратегии правления и структуре внутреннего контроля является отправной точкой проектирования, разработки и поставки качественных технологий кибербезопасности.

Вопрос	Дополнительные аспекты...
1. Есть ли у поставщика официальная стратегия и подход к управлению рисками, информационным рисками и угрозами информационной безопасности?	• Если стратегии нет, маловероятно, что будут выделяться какие-либо средства и ресурсы. • Организация должна осознавать угрозу информационной безопасности, стоящую перед ее операциями (включая миссию, функции, имидж или репутацию), активами и сотрудниками. • Отсутствие стратегии приводит к непоследовательным результатам, снижению устойчивости и воспроизводимости качества и безопасности. • Если стратегия существует, но лишена эффективных подходов, то она просто превратится в пустые обещания.
2. Есть ли у поставщика управленческая, организационная модель, политики и процедуры для поддержки стратегий? Обновляет ли поставщик на регулярной основе свои стратегии, чтобы привести их в соответствие с текущей обстановкой и требованиями в сфере информационной безопасности?	• Если информационная безопасность встроена в схему правления и структуру самого «объекта», то она будет одинаково значима, например, для финансового комитета или комитета по разработке стратегий. • Доступные для учета и наблюдения комитеты Совета директоров, программные документы, стандарты и ключевые контрольные точки аудита свидетельствуют о том, что все они встроены в работу организации и поэтому рассматриваются со всей серьезностью. • Если что-то не имеет значения для Совета директоров и высшего руководства компании, это не будет иметь значения и для рядовых сотрудников, вот почему необходимы разъяснения.
3. Какая управленческая структура в компании поставщика говорит о том, что информационная безопасность является ключевой стратегической и операционной задачей бизнеса? Есть ли у них специализированный комитет Совета директоров по вопросам информационной безопасности, как он работает?	• Специализированный комитет, возглавляемый старшим членом Совета, служит доказательством того, что это направление является приоритетом для компании, а не обычной тактической работой, делегированной техническому персоналу. • Если в комитет входят ведущие члены Совета, то это говорит о высшей степени заинтересованности, поскольку только эти лица способны осуществлять значительные изменения. • Если такой комитет является принимающим решения органом, который задает общее направление стратегии и подхода к информационной безопасности, это подтверждает активную вовлеченность Совета. • Если члены совета проходят подготовку, проводят анализ в случае обнаружения нарушений, принимают участие в антикризисном управлении, это говорит о том, что они близко знакомы с практической стороной деятельности. • Если высшее руководство ясно излагает свои ожидания в отношении стратегических целей и приоритетов, доступных ресурсов и общей рискоустойчивости, а также распределяет обязанности по достижению результатов, это гарантирует всеобщее понимание важности информационной безопасности.
4. Каким образом поставщик обеспечивает решение вопросов информационной безопасности в рамках своего бизнеса. Как члены Совета директоров включаются в процессы, которые происходят в организации, и каким образом они отчитываются о своих действиях?	• Должен существовать отлаженный канал, предоставляющий информацию о том, как высокопоставленный комитет Совета директоров контролирует выполнение намеченной стратегии. • •Поставщики должны продемонстрировать интегрированные связи, ведущие от стратегии ко всем, даже самым отдаленным, точкам бизнес-процесса рядом с клиентом) и в обратном направлении. • Может ли поставщик предоставить доказательства того, что члены совета и вышестоящие руководители несут определенную личную ответственность за принятие решений в сфере информационной безопасности, или они просто заседают в комитете?
5. Какой подход выбрал поставщик для того, чтобы влияние вопросов безопасности учитывалось в каждом подразделении организации? Каким образом этот подход реализуется на постоянной основе?	• Информационная безопасность — это всеобщая задача, и каждый сотрудник должен стать частью ее решения. Способность продемонстрировать такой универсальный для всей компании подход по принятию решений о том, что играет роль, а что — нет, говорит о вхождении безопасности в структуру бизнеса. • Чем больше вопросы информационной безопасности сосредоточены в руках отдельных сотрудников головного офиса, тем в большей степени они становятся лишь их проблемами. Комплексный подход означает привлечение всех ресурсов. • Каким образом другие стороны бизнес-процесса реализуют это корпоративное стратегическое направление и используют информацию в качестве ориентиров в рамках деятельности по управлению рисками и операционного процесса?

Вопрос	Дополнительные аспекты...
6. Каков подход поставщика к выбору мероприятий в сфере информационной безопасности? Осуществляется ли он силами специальной руководящей группы или привлечением всех подразделений, включая региональные ресурсы службы безопасности?	• Кто решает эти проблемы? Если этим занимаюсь не я, и моя деятельность не включает реализацию лучших подходов к безопасности, то я не буду решать эти задачи. Структура организации и то, каким образом поставщик встраивает в нее безопасность, позволяет определить, является ли стратегия универсальной для всей организации или закрепленной лишь за несколькими людьми. • Компании должны суметь продемонстрировать в отношении всех основных функций, каким образом управление рисками и информационная безопасность включены в их деятельность, включая процессы и ресурсы. • Компании должны суметь продемонстрировать, как местные требования по безопасности рассматриваются и реализуются в рамках корпоративных процессов.
7. Каждая компания сталкивается с нарушениями в сфере безопасности, каким образом поставщик извлекает уроки из этих происшествий? Как они анализируются на уровне вышестоящих руководителей, чтобы полученный опыт использовался в обычной деятельности?	• «Слепой» совет — это плохой совет. Часто упоминается о том, что только те, кто занимает самые высокие посты в организации, способны стимулировать крупнейшие изменения в поведении и подходе. Если эти лица не видят нарушений или инцидентов в сфере безопасности, они не осознают то, что очевидно для клиента или не представляют, какие изменения им необходимо внести в свой бизнес. • Компания должна суметь продемонстрировать систему регулярного предоставления в комитет уровня Совета директоров отчетов о зарегистрированных происшествиях, извлеченных уроках и тех исправлениях, которые были внесены после происшествий.
8. Подвергались ли внутренние ИТ-системы поставщика кибератакам и какой опыт он вынес из этих происшествий, чтобы усовершенствовать собственные продукты и услуги?	• Способность компании извлекать опыт из проблем в собственной системе безопасности позволяет ей понять те трудности, с которыми могут столкнуться клиенты и то, как смягчить последствия возникновения рисков. • Компания должна суметь продемонстрировать, каким образом она «залечивает собственные раны», когда речь идет об информационной безопасности.

4.2. Стандарты и процессы

Чтобы получать продукт неизменно высокого качества, необходимы процессы и стандарты такого же уровня. Более того, ваши сотрудники и поставщики также должны следовать этому подходу. То же относится и к информационной безопасности: если ваши процессы, стандарты или подходы к информационной безопасности меняются от продукта к продукту, то качество, защищенность и безопасность конечного продукта также будут каждый раз отличаться.

Вопрос	Дополнительные аспекты
9. Принимает ли и поддерживает ли поставщик какие-либо международные стандарты в рамках широкого определения информационной безопасности? Каких стандартов придерживается компания и в каких органах стандартизации ее сотрудники занимают руководящие должности или принимают активное участие?	• Если предприятие при любой возможности практикует принятие международных стандартов и готово к интеграции передового опыта в собственные бизнес-процессы, вероятнее всего, оно идет в ногу с самыми последними представлениями об информационной безопасности. • Компания, которая входит в объединение по стандартизации, поддерживающее разработку и принятие стандартов в сфере информационной безопасности, демонстрирует свою готовность перенимать передовой опыт и стандарты. • Способен ли поставщик продемонстрировать поддержку и принятие технических стандартов, применимых к деятельности вашей компании? • Чтобы повысить надежность независимого тестирования программного обеспечения, у вас может возникнуть желание выяснить, каким образом поставщик перенимает передовой опыт тестирования в отрасли (напр., Общие критерии) и стремится ли он к стандартизации с целью расширения возможностей и повышения качества тестирования внутренней системы информационной безопасности.

Вопрос	Дополнительные аспекты
10. Каким образом поставщик определяет, какому передовому опыту и стандартам (законам) необходимо следовать? Какие процессы прошла компания для определения и разрешения противоречий между законами и стандартами и каким образом она обеспечивает обновление данных?	• Проблема стандартов и передового опыта состоит в том, что добро существует только в глазах наблюдающего. Наличие механизма по обновлению говорит клиентам о том, что они получают продукт, отвечающий новейшим требованиям. Для компании применение широкого спектра подходов, стандартов и идей означает необходимость постоянной оценки того, как другие предприятия справляются с проблемой, и внедрения новых усовершенствованных представлений и требований в собственные операции. • Компания должна суметь продемонстрировать комплексный подход к изучению лучших мировых практик, стандартов, кодексов и т. д. и преобразованию этого материала в набор корпоративных политик, процедур и критериев.
11. Какие рабочие группы или возможности привлекает поставщик для поддержки широкого спектра стандартов по административному управлению и технических стандартов, включая криптографию, при попытке соответствовать ряду технических норм?	• Вы можете расширить этот список требований и конкретизировать ряд стандартов по административному управлению или технологическому процессу, таких как серия ISO 27000, и набор технических стандартов для вашей отрасли, например X.805, PCI и OWASP. • Для вас может оказаться важным, что поставщик способен выполнять существующие стандарты и готов изменять свою технологию по мере пересмотра действующих и разработки новых стандартов. • Криптография (шифрование) — это специализированная область, которая зачастую регулируется местным законодательством. У вас может возникнуть желание удостовериться, что поставщик обладает ресурсами для обеспечения криптографии (шифрования) и знаком как с правовыми, так и с техническими требованиями.

4.3. Законы и нормативно-правовые акты

Законы сложны и постоянно меняются. К примеру, если в государстве принят закон, это вовсе не означает, что он исполняется, а если он исполняется, то способы его исполнения могут существенно различаться или один и тот же закон или кодекс может иметь различные интерпретации. Законодательство, кодексы, стандарты и средства международного контроля создают дополнительные сложности и риски для поставщиков и бизнеса.

Вопрос	Дополнительные аспекты
12. Каким образом поставщик оценивает и пытается усвоить законы и требования по информационной безопасности и конфиденциальности в тех странах, где он осуществляет свою деятельность? Как эта информация используется в ходе проектирования, разработки, эксплуатации и обслуживания его продуктов и услуг?	• Помимо того, что непоследовательность законодательства в различных странах, где работает международная компания, представляет очевидную трудность, проблема законов и кодексов в том, что они могут иметь различные интерпретации. Для компании важно иметь механизм по обновлению и давать оценку законам и кодексам, чтобы клиенты были уверены в том, что они получают продукты, соответствующие новейшим требованиям. Для компании рассмотрение широкого спектра подходов, стандартов и идей означает необходимость постоянной оценки того, как другие предприятия справляются с проблемой, и внедрения новых представлений и требований в собственные операции. • Компания должна суметь продемонстрировать комплексный подход к изучению передового опыта, стандартов, кодексов и т. д. во всем мире и преобразованию этого материала для обеспечения постоянного улучшения корпоративных политик, процедур и критериев и т. д. • Учитывая изменчивую и требовательную природу законов, компания должна постоянно демонстрировать свое умение обращаться с нечеткими или противоречивыми законами в области разработки продуктов и услуг. • Закон так же важен, как и технический стандарт или требование. Поставщик должен суметь показать, каким образом он исполняет правовые требования страны или региона, особенно в сферах неприкосновенности личной жизни и защиты данных. • Повседневные деловые операции следуют за процессами. Поэтому способность продемонстрировать, что технические требования соблюдаются на стадии разработки продуктов и услуг, свидетельствует о целостном подходе к любым требованиям.

Вопрос	Дополнительные аспекты
13. Каким образом поставщик обеспечивает соответствие своих процессов местным законам и требованиям? Каковы его действия в случае противоречия между местным законом и политиками, стандартами или процессами компании? Как члены Совета директоров включаются в процессы, которые происходят в организации, и каким образом они отчитываются о своих действиях?	• Закон есть закон, и важно, чтобы поставщик смог доказать, что его оборудование и услуги законны. • Каждая компания, которая ведет деятельность за границей, сталкивается с задачей по обеспечению связи между местными рабочими группами и головным офисом. Поставщики должны суметь продемонстрировать, каким образом мнения регионов учитываются при обсуждении на уровне головного офиса и процессе разработки продукта. • Компания должна суметь продемонстрировать свое умение обращаться с противоречивыми законами и требованиями с учетом прецедентного права местного законодательства. • Поставщик должен прямо заявлять о своей обязанности предоставлять информацию (данные) иностранному правительству. • С учетом недавних разоблачений у вас может возникнуть необходимость найти официальное заявление поставщика о его взаимоотношениях с государством, резидентом которого он является (или с каким-либо другим), касающихся информационной безопасности, предоставления «лазеек», ослабления криптографической защиты или обеспечения секретности. • Поставщик должен прямо заявлять о месте хранения данных и о том, под какой юрисдикцией они находятся.
14. Каким образом поставщик обеспечивает соответствие своих процессов и процедур экспортному контролю и действующим законам (включая криптографию) страны, в которой они реализуются?	• Компания должна суметь продемонстрировать интегрированные систему управления, политики и процедуры, которые охватывают процессы продаж, обслуживания, заключения контрактов и разработки продуктов, подстраивающиеся под конкретные правовые требования, будь то требования торговой политики, управление лицензиями, экспортный контроль и т. д. • Компания также должна суметь продемонстрировать соответствующие точки контроля, которые подтверждают выполнение ключевых требований. • Если это не осуществимо, покупатель подвергает себя риску вынужденной замены оборудования и услуг, которые нарушают законы.
15. Что представляет собой корпоративная политика поставщика в сфере прав на интеллектуальную собственность в тех странах, где отсутствует соответствующее законодательство?	• Компания должна суметь выделить ряд политик, процедур и подходов, которые отражают ее ответственность в таких сферах, как лицензирование, права на интеллектуальную собственность и межкультурные различия. Этические и правовые задачи возникают во многих странах, но их решение должно быть последовательным и встроенным в подход компании по ведению бизнеса. Вам следует удостовериться в наличии у поставщика внутреннего кодекса поведения или политики делового поведения.
16. Каким образом поставщик гарантирует, что его отдел продаж продает только те продукты и услуги, которые соответствуют местным законам и нормативным актам, включая экспортный контроль и торговые санкции?	• Отдел продаж создается для того, чтобы продавать, это главная мотивация сотрудников и залог процветания бизнеса. Но иногда они могут посчитать, что правила и нормы встают на пути у продаж. Кроме того, покупатель может обладать мощными снабженческими ресурсами, и поэтому поставщик должен быть готов продемонстрировать, каким образом его процессы защищают покупателя. • Важно, чтобы поставщик смог предоставить набор интегрированных процессов, которые объединяют продажи, правовую сферу и поставку или поддержку, а также отвечают внутренним и внешним требованиям покупателя.
17. Каким образом поставщик проверяет контракты и обеспечивает точность информации о своих возможностях с точки зрения информационной безопасности?	• Зачастую проекты и контракты бывают очень сложными, долгосрочными по своей природе и могут содержать данные, полученные от нескольких подразделений многочисленных компаний. Поставщик должен суметь доказать, что договоренности, прописанные в контракте, отвечают целям покупателя, а также законам и нормативно-правовым актам.
18. Учитывая, что все крупные компании, деятельность которых основана на технологиях, используют технологии других поставщиков, ваш поставщик должен суметь описать	• У вас может возникнуть необходимость удостовериться в том, что компоненты сторонних организаций, которые использует поставщик, должным образом лицензированы. Это позволит избежать возможных последующих споров, результатом которых может стать замена программного или аппаратного обеспечения, влекущая за собой дорогостоящие сбои.

4.4. Человеческий фактор

Многие компании заявляют, что их сотрудники являются их самым ценным активом, и это действительно так. Однако с точки зрения безопасности они могут стать самым слабым звеном в структуре. То, каким образом сотрудников нанимают, обучают, мотивируют и как управляют их производительностью, во многом определяет успех или провал компании. Это утверждение истинно не только для информационной безопасности, но и для реализации общей стратегии компании.

Вопрос	Дополнительные аспекты
19. Вовлечена ли группа управления в процесс обучения всех сотрудников культуре информационной безопасности? Если да, то каким образом? Проходят ли вышестоящие руководители и члены Совета директоров постоянное обучение по вопросам соблюдения законодательства?	• Важно, чтобы группа управления, в том числе менеджеры среднего звена, были заметно заинтересованы обучением, иначе рядовые сотрудники не будут придавать ему должного значения. Поэтому руководители должны подчеркивать важность этой работы и подтверждать свою позицию на деле, участвуя в обучении для всех сотрудников. • Способность поставщика продемонстрировать всеобщую заинтересованность и осознание ответственности каждым сотрудником обеспечивает более высокие шансы на успех. • Понимание лицами, принимающими решения и контролирующими повседневные операции, сферы нормативно-правового соответствия способствует устойчивой и непрерывной работе компании. Они должны знать законы об информационной безопасности.
20. Не все должности несут одинаковый риск с точки зрения внутренней угрозы. Выделяет ли поставщик «чувствительные» или «важнейшие» должности, когда речь идет об информационной безопасности?	• Необходимо убедиться, что важнейшие должностные лица, которые предоставляют услуги заказчикам, являются доверенными и обеспечены необходимыми защитными мерами. • Учрежденные механизмы выявления важнейших должностей и сосредоточенность на возможных угрозах, которая подразумевает эффективное управление должностями, свидетельствуют о развитости поставщика. • Например, должности, которые имеют непосредственный доступ к вашим ключевым ИКТ и возможность внесения изменений в программные продукты, могут представлять более серьезную угрозу для продуктов и услуг.
21. Какой подход использует поставщик для найма и испытания сотрудников на «чувствительных» или «важнейших» должностях? Практикует ли поставщик проверку биографических данных, проверку на предмет вывода из штата и подписание соответствующих пунктов договора?	• Это показатели последовательного подхода к компетенции и репутации персонала. Компания осознает риск возникновения внутренних угроз и демонстрирует подход к снижению такого риска. • Способность поставщика продемонстрировать эти аспекты свидетельствует о выборе комплексного подхода к информационной безопасности.
22. Какие процессы и механизмы имеются в распоряжении поставщика для обеспечения регулярного оповещения и специального обучения в отношении информационной безопасности с учетом обязательств, политик, процедур и других требований к сотрудникам и подрядчикам? Каким образом регистрируется факт прохождения обучения?	• Как поставщику удается обеспечить для информационной безопасности статус основной ценности, включенной в культуру поведения, принятую всеми сотрудниками? Какие базовые системы и процедуры утверждает поставщик с этой целью? • Информационная безопасность — это перспективное требование, которое подразумевает частое обновление знаний. Если актуальность уровня знаний поставщика не поддерживается, это может означать потерю ориентира и недостаток готовности. • Выбирая поставщика, стоит узнать о наличии у него системы регулярного обучения и оповещения, опыта использования различных средств обеспечения осведомленности на глобальном и местном уровнях и проведения дополнительной работы в функциональных областях, т. е. более углубленного обучения по конкретным направлениям. По сути, у вас может возникнуть необходимость удостовериться в том, что сотрудники и партнеры организации хорошо обучены для выполнения своих функций и обязанностей в сфере информационной безопасности с учетом соблюдения связанных политик, процедур и соглашений.
23. Есть ли у поставщика политики, направленные на повышение компетенции и осведомленности лиц, занимающих «чувствительные» или «важнейшие» должности?	• Подразумевается, что признание должности в качестве «чувствительной» или «важнейшей» влечет применение других, более жестких требований. Компания должна суметь показать заказчику, что не только осведомлена о рисках, но и имеет опыт и понимает ценности, такие как целостность.

Вопрос	Дополнительные аспекты
24. Во многих странах существуют антикоррупционные законы. Каким образом поставщик применяет их по отношению к своим сотрудникам?	• Поставщик должен суметь продемонстрировать, каким образом он знакомит своих сотрудников с национальным законодательством и с международно признанным передовым опытом в рамках мероприятий по борьбе с взяточничеством и коррупцией. • Каким образом поставщик популяризирует ценности компании и представления о том «что такое хорошо и что такое плохо» и прививает их своим сотрудникам на постоянной основе?
25. Имеется ли в распоряжении поставщика механизм, благодаря которому сотрудники могут уведомить руководство (подобающим образом) о подозрениях, связанных с нарушением политик, законов или нормативно-правовых актов?	• Часто рядовые сотрудники компании замечают то, что не видят руководители. Утверждение соответствующих механизмов уведомления обеспечивает компании возможность обнаружить проблему на начальной стадии и принять меры по исправлению ситуации. Самообучающаяся, закрытая система рационализации должна показывать, каким образом компания рассматривает аспекты, которые не вписываются в рамки ее процессов, а сотрудникам часто требуется использовать такие механизмы, чтобы сигнализировать о том, что они считают неправильным.
26. Какова стратегия поставщика по выводу сотрудников из штата предприятия и как он использует знания, полученные в рамках этого процесса для совершенствования политик, процедур и культуры?	• Сотрудники уходят по разным причинам, некоторым из них не нравится то, что происходит вокруг. Такие отзывы могут указывать на проблемы в сфере безопасности. Поставщики должны суметь продемонстрировать, что они принимают к сведению все данные (в том числе и поступающие от сотрудников, покидающих компанию) в отношении стиля управления компании, политик и процедур, используемых для решения проблем и повышения эффективности бизнеса.
27. Имеется ли у поставщика официальное руководство по дисциплинарным мерам в сфере информационной безопасности?	• Поставщику необходимо продемонстрировать средства достижения равновесия стимулов и сдерживающих факторов, которые создают здоровую атмосферу безопасности для клиента, компании и сотрудников. • Если сотрудники сознательно действуют вопреки политике информационной безопасности, должно быть четкое представление о тех стратегиях и процессах, которые будут приняты, и тех потенциальных дисциплинарных мерах, которые могут быть применимы против них.
28. Если к сотруднику применяются меры дисциплинарного характера, то как поставщик учитывает возможные нарушения со стороны менеджера или руководителя, т. е. как он решает проблемы, связанные с руководящим составом?	• Компании важно продемонстрировать, что менеджеры несут ответственность за работу и поведение команды. Они не могут просто обвинять кого-то за действия и рабочие показатели своей команды. Компания должна показать, каким образом ей удается обеспечивать ответственность и соразмерность стимулов и дисциплинарных подходов с точки зрения отдельного сотрудника, менеджера (-ов) и команд (-ы).

4.5. Исследования и разработки

Компании не хотят использовать свои ограниченные средства на покупку высокотехнологичных продуктов у поставщиков, которые не ведут исследования и разработки на серьезном уровне и, соответственно, не получают от них постоянных результатов в виде высококачественных безопасных продуктов. Также они не желают наблюдать, как поставщики, принимая решение об инвестициях, думают, что выбрать: вложения в новый продукт или в защиту и безопасность всех имеющихся продуктов. Информационную безопасность, подобно качеству, невозможно «прикрутить» к продукту. Компании должны демонстрировать заинтересованность в долгосрочных исследованиях, чтобы иметь возможность осуществлять проектирование, разработку и развертывание систем информационной безопасности, а также инвестировать в следующее поколение продуктов.

Вопрос	Дополнительные аспекты
29. Имеется ли в распоряжении поставщика формальный набор процессов по исследованию и разработке, в которые встроены требования по информационной безопасности, и что лежит в его основе: отраслевой стандарт или передовой опыт?	• Если компания не способна продемонстрировать готовый набор процессов и подходов, у нее нет прочной основы для внедрения системы качества и информационной безопасности. Случайные процессы равносильны случайному качеству, случайным результатам в сфере безопасности и повышенному риску. • Не существует совершенной модели или одного глобального стандарта по безопасности, поэтому компании необходимо продемонстрировать порядок использования знаний и передового опыта из многочисленных источников.
30. Каким образом процессы по исследованию и разработке обеспечивают и определяют эффективность требований в отношении безопасности, в том числе в условиях изменяющихся угроз? Какие механизмы используются для определения того, что является обязательным, а что — лишь успешным опытом?	• В то время как многие расценивают информационную безопасность как часть показателя качества, что справедливо, она характеризуется различными аспектами, а именно: динамикой угрозы или разнообразием точек входа для атаки. Поставщики должны суметь продемонстрировать всесторонний подход к внедрению требований по обеспечению безопасности в сферу исследования и разработки, осуществляя поиск новых факторов или сведений и проверяя эффективность результатов. Если они окажутся неэффективными, требования необходимо заменить, а затем вернуться на этап внедрения новых или скорректированных знаний или опыта для укрепления системы информационной безопасности.
31. Клиенты во всем мире предъявляют различные, иногда даже противоречивые, требования по безопасности и функциональные требования. Имеется ли в распоряжении поставщика набор интегрированных процессов, который позволяет учитывать требования клиента на всех этапах вплоть до окончания взаимоотношений, а также оценить, что может и должно происходить?	• Различные законы и нормативно-правовые акты, социальные культуры и предпочтения пользователей в разных странах формируют разные требования клиентов. Набор постоянных и негибких процессов не может удовлетворить необходимость в соблюдении требований со стороны клиента или специфических для конкретной юрисдикции условий. Отсутствие эффективного управления может привести к такому результату, когда клиент получает продукт, который не оправдывает его ожиданий или даже несовместим с нужной ему функцией. Поставщикам необходимо показать умение эффективно управлять различными или противоречивыми требованиями.
32. Есть ли у поставщика стратегия жизненного цикла товара, которая гарантирует обеспечение безопасной составляющей на протяжении всего срока его существования? Какую информацию она дает и как используется?	• У вас, как у потенциального клиента, может возникнуть желание удостовериться в том, что продукты, которые вы приобретаете, имеют срок использования, достаточный для того, чтобы их приобретение окупилось (напр., 3—5 лет). Поставщик должен суметь объяснить порядок управления жизненным циклом продукта или набора связанных продуктов. По сути, он должен удостоверить вас в том, что приобретаемые вами продукты не устареют в краткосрочном периоде и допускают модернизацию. • Если требования по безопасности вступают в противоречие с другими требованиями, такими как функциональность, надежность, работоспособность и т. д., каким образом поставщик принимает решение о превосходстве какого-либо требования?
33. Поставщик должен описать ход процесса разработки основного продукта, а также порядок его анализа и непрерывного совершенствования с точки зрения технических характеристик и качества. Необходимо предоставить сведения о том, какие проверки, контрольные точки и точки принятия решений о годности или негодности включены в процесс.	• Большинство технологий имеют сложную структуру, поэтому понимание того, каким образом поставщик встраивает многочисленные технические экспертизы, обзоры финансово-хозяйственной деятельности, проверки безопасности и качества, а также контрольные точки в свой процесс, обеспечивает уверенность клиента в том, что поставщик никогда не теряет из вида задачи и успешные результаты.

Вопрос	Дополнительные аспекты
34. Современное программное обеспечение очень сложное. Обычно оно содержит миллионы строк компьютерного кода и тысячи компонентов от разных поставщиков. Какую процедуру и какую технологию использует ваш поставщик, чтобы обеспечить использование нужных компонентов в нужное время?	• Процесс разработки может быть четко определен. Тем не менее отсутствие эффективной платформы управления ИТ для поддержки этого процесса может затруднить реализацию нормативных актов компании и требований клиента. Если различные элементы, которые составляют компьютерную систему, не включены в «конфигурационное управление» или не контролируются должным образом, то работа системы может быть неустойчивой и вы не сможете отслеживать, что и где используется.
35. Конфигурационное управление — это процесс проектирования системы и вспомогательная технология для обеспечения и сохранения устойчивой работы продукта, функциональных и физических характеристик, которые необходимы на протяжении всего срока его службы. В сложной технологической среде этот механизм является краеугольным камнем для устойчивого, высококачественного, безопасного кода. Каков подход вашего поставщика?	• Компания должна суметь продемонстрировать последовательное «конфигурационное управление» или системы контроля, которые предотвращают злоумышленную подделку элементов или использование неподобающих элементов на стадии разработки и компиляции продукта. • Сюда же необходимо отнести управление версиями, изменениями, сторонние инструменты и компоненты.
36. Разделение обязанностей необходимо для ограничения угроз и риска повреждения. Каким образом поставщик реализует это условие в процессе исследования и разработки, особенно в среде разработчиков программного обеспечения?	• Важно понимать, каким образом смягчаются внутренние угрозы. Разделение обязанностей является важной частью этого процесса. Поставщики должны быть способны распределить роли в процессе исследования и разработки и запланировать, на каких этапах этого процесса может быть задействована каждая роль. С точки зрения безопасности умение сотрудника ограничивать фазы, действия, продукты и программные коды, к которым у него есть доступ, может ограничить риск.
37. Многие технологические компании внедряют стороннее программное обеспечение и программное обеспечение из открытых источников в собственные компьютерные коды. Каким образом поставщик отслеживает и контролирует состав каждого продукта?	• В то время как код и компьютерная технология поставщика могут быть построены по высоким стандартам, уязвимость может заключаться в сторонней технологии, которую он использует. Информация о месте нахождения проблемы и о том, чье программное и аппаратное обеспечение задействовано, является ключевым аспектом оценки риска и проведения восстановительных мероприятий.
38. Стороннее программное обеспечение и программное обеспечение из открытых источников часто находятся на различных сайтах. Каким образом поставщик определяет, что загружаемая программа является легальной и не содержит вредоносных компонентов или лазеек?	• Если поставщик не осуществляет строгий контроль за тем, какие программные компоненты используются и из какого источника они поступили, он демонстрирует недостаток контроля качества. Наличие скрупулезных процессов для обеспечения заимствования исходных кодов только с авторитетных сайтов может служить снижающим риск фактором. • Некоторые мошеннические сайты могут содержать поддельные открытые исходные коды и встроенные вредоносные программы, поэтому поставщики должны проявлять бдительность.

Вопрос	Дополнительные аспекты
39. Прежде чем использовать стороннее программное обеспечение, через какие процессы проходит поставщик для устранения известных уязвимостей перед утверждением его использования и после внедрения?	• Хорошее правило для покупателей и продавцов: ничего не предполагай, никому не доверяй и все проверяй. Вам необходимо узнать, подтверждает ли поставщик, что все известные уязвимости в стороннем программном обеспечении, встроенном в ваш продукт, устранены до его отправки покупателю. Это длительный процесс, поскольку новые уязвимости могут быть обнаружены уже после запуска продукта. • Если поставщик встраивает сторонние компоненты в свой продукт, вам необходимо уточнить у него, охватывается ли стороннее программное обеспечение процессом управления жизненным циклом?
40. Каким образом поставщик гарантирует устранение дефекта в стороннем программном обеспечении, компоненте из открытого источника или даже стандартной системной программе, независимо от места использования кода?	• Зачастую сторонние компоненты используются во многих продуктах поставщика или даже на нескольких позициях в рамках одного продукта. Поэтому для устранения уязвимостей стороннего происхождения поставщику необходимо знать каждый продукт, в котором использовался данный компонент. В противном случае уязвимости не будут устранены во всех продуктах.
41. Использует ли поставщик несколько языков и инструментов разработки в своих продуктах? Если да, то вносит ли он эти инструменты в каталог, поддерживаются ли они и отвечают ли современным требованиям?	• Поставщик может использовать целый ряд инструментов, программ и кодов сторонних разработчиков и уязвим в связи с тем, что компании сливаются, становятся банкротами или меняют свои стратегии. По этой причине вам необходимо удостовериться в том, что в распоряжении у вашего поставщика есть формальные процессы проверки, одобрения и блокирования сторонних продуктов и компонентов на основании их качества, архитектуры и дорожных карт разработки. • Поставщик должен суметь продемонстрировать стратегию и набор механизмов, которые обеспечивают внедрение в продукты только поддерживаемых и безопасных сторонних инструментов и компонентов.
42. Поставщик должен описать свой подход к отслеживанию сквозного процесса исследования и разработки, а также используемых программных инструментов по каждому стороннему программному обеспечению и программному обеспечению из открытых источников.	• Нарушения могут возникнуть в любой момент, люди могут совершать плохие поступки. Если в результате какого-либо происшествия в вашей компании системы вышли из строя или подверглись любого рода угрозе, сколько времени вы отведете поставщику на поиск проблемы? День, неделю, месяц? Сложные технологии могут содержать тысячи компонентов и много миллионов строк компьютерного кода. Вы должны быть уверены в том, что поставщик способен отслеживать все компоненты, использованные во всех продуктах, проданных всем компаниям, а вы можете отслеживать все приобретенные продукты. Кроме того, поставщику необходима возможность отслеживать всех вовлеченных людей: что они делали и когда, а также все разрешения на эти виды работ.
43. Сложные продукты подразумевают создание миллионов строк компьютерного кода. Есть ли у поставщика средства для автоматического сканирования кодов, позволяющие выполнить автоматическую проверку кодирования в рамках процесса исследования и разработки.	• Эффективная разработка нацелена на автоматизацию как можно большего числа задач, поскольку это позволяет «гарантировать» качество и развивать последовательность. У поставщика должно быть несколько автоматических инструментов и методов для динамического сканирования ваших продуктов с целью обнаружения широкого спектра неполадок. В идеале результаты должны автоматически отсылаться в систему управления качеством поставщика. • Автоматизация не позволяет решить все проблемы и обозначить все слабые места, поэтому необходимо использовать сочетание подходов и избегать ситуации, когда компания чрезмерно полагается на проверку с помощью технических средств.
44. Поставщик должен описать механизмы определения готовности продукта для выпуска на рынок и процесс авторизации.	• Удостоверьтесь в надежности процесса одобрения. Вы могли слышать от многих представителей ИКТ-групп, возможно, даже в рамках своей компании, что что-либо закончено на 95 %. Ваш поставщик должен доказать, что продукт закончен на 100 % по всем параметрам, и его готовность должна быть проверена сотрудниками, не входящими в группу по работе над проектом. • Необходимым доказательством служат многочисленные технические экспертизы и проверки обеспечения качества или безопасности, а окончательное решение об авторизации не должно выноситься инженером программного обеспечения — не стоит ставить оценку за свою собственную домашнюю работу.

Вопрос	Дополнительные аспекты
45. Дефекты выявляются в течение всего цикла разработки продукта, а также срока его службы. Каким образом поставщик отслеживает дефекты и обеспечивает их устранение в каждом продукте, в котором может использоваться соответствующий компонент?	• Как клиент, вы не хотите снова и снова сталкиваться с одной и той же проблемой. Не хотите также, чтобы аналогичная проблема возникала в разных продуктах. Поэтому вам нужно выяснить, каким образом поставщик отслеживает дефекты и сбои и как этот процесс интегрируется в сферу исследований и разработки, обучения и др.
46. Поставщик должен объяснить, каким образом он максимизирует рост своей компетенции в сфере информационной безопасности. Есть ли в компании центры повышения квалификации и центр обучения сотрудников по вопросам информационной безопасности? Как работают эти структуры?	• Не все сотрудники в вашей компании могут быть экспертами во всех областях. То же касается и предприятия по разработке широкомасштабных комплексных технологий. Поэтому поставщику необходимо умение оценивать обширность и глубину своих возможностей в сфере безопасности и обеспечивать соответствующим группам доступ к важным навыкам и компетенциям, а вам нужно выяснить, как это осуществляется.
47. Угрозы постоянно эволюционируют. Каким образом поставщик следит за этим процессом и учитывает все изменения на этапах проектирования, разработки и развертывания?	• На примере управления автомобилем можно сказать, что если поставщик постоянно смотрит в зеркало заднего вида, он рискует врезаться в кирпичную стену. У вас может возникнуть необходимость удостовериться в том, что поставщик смотрит вперед, предвидит появление новых обстоятельств и учитывает их при проектировании и разработке продукции. • Поставщики должны продемонстрировать, что они принимают в расчет каждый источник угроз или атак, а также то, каким образом этот принцип закладывается в проектные решения и другие требования.
48. Поставщик должен объяснить, каким образом его процессы поддерживаются соответствующей технологией. Например, как он использует базу данных угроз в своем тестировании? Или создал ли он библиотеку сценариев тестирования?	• Поставщик может представить увлекательный рассказ о своих процессах и стандартах, но для эффективной и результативной работы компании нужна базовая поддерживаемая и интегрированная технология. Следует ли этому принципу ваш поставщик? • Набор интегрированных технологических платформ должен использоваться в рамках каждого процесса и подразделения поставщика для поддержания работы и бизнес-целей.
49. Поставщик должен объяснить свой подход к управлению версиями. Некоторые поставщики предлагают единую кодовую базу всем клиентам во всех странах, у некоторых кодовая база характеризуется ответвлениями для определенных регионов, стран или клиентов. Оба ключевых метода имеют сильные и слабые стороны. Какой подход использует ваш поставщик?	• Не существует идеальной модели для одного продукта во всем мире либо одного продукта в определенной стране или у определенного клиента. Если вы используете один продукт по всему миру, то можете потерять гибкость, а у поставщика может отсутствовать желание принимать ваши требования. Если сотни различных продуктов выполняют, грубо говоря, одну функцию, затраты поставщика возрастут, а результативность снизится. Важно понять, каким образом поставщик старается поддерживать нужный баланс и справляется с задачами в рамках метода, который он выбрал.

4.6. Проверка: ничего не предполагай, никому не верь и все проверяй

Несмотря на то, что непрерывные исследования и разработки жизненно важны для качества, защищенности и безопасности продуктов, от участников этого процесса могут требовать выпускать новые продукты быстро и без надлежащих испытаний и проверок. Использование многоуровневого всестороннего подхода к независимым проверкам снижает риск распространения небезопасных продуктов. Непрерывный процесс сдерживания и уравновешивания является гарантией качества продукта и безопасности капиталовложений клиентов.

Вопрос	Дополнительные аспекты
50. Есть ли у поставщика лаборатория информационной безопасности, которая в дополнение к процессам на этапе исследования и разработки проводит независимые проверки продукта (т. е. проверки или испытания силами сотрудников, не причастных к разработке продукта) перед его выпуском на рынок?	• Группы по исследованиям и разработке имеют свои бизнес-цели. Они стремятся найти равновесие между прогрессом, затратами и безопасностью. Деятельность независимой от отдела исследований и разработки лаборатории может быть направлена на достижение целей безопасности за рамками сферы влияния групп по исследованиям и разработке. Такой подход согласуется с принципом защиты, который обеспечивается разделением обязанностей. • Важно, чтобы поставщик показал, что он оценивает продукты непосредственно перед выпуском на рынок.
51. Могут ли отделы исследований и разработки или маркетинга игнорировать результаты, полученные в такой лаборатории?	• С точки зрения качества и добропорядочности важно, чтобы участвующие в проекте сотрудники обеспечивали соответствие продукта всем требованиям качества и безопасности. На этих сотрудников не должно оказываться влияние со стороны других подразделений предприятия, и они должны иметь право вето. • Если снова вернуться к модели управления, предусмотрено ли предоставление отчетов вышестоящему руководству о каких-либо проблемах, обнаруженных силами внутренней лаборатории?
52. Проводит ли внутренняя лаборатория, которую может иметь в своем распоряжении поставщик, испытания на проникновение, статическое и динамическое сканирование кодов для обеспечения соответствия архитектуре системы информационной безопасности и требованиям к кодированию? Используется ли оценочный отчет, чтобы подтолкнуть группы разработки продуктов к внесению улучшений?	• Цель такой лаборатории — сосредоточить внимание на безопасности во всех ее проявлениях, поэтому, попросив поставщика продемонстрировать обширность и глубину знаний соответствующей группы, вы удостоверитесь в прочности подхода к безопасности. • Тем не менее, чтобы поднять уровень качества, компании необходимо продемонстрировать, каким образом аспекты, обнаруженные в ходе таких проверок или испытаний, используются для улучшения не только тестируемого продукта, но и всей структуры процесса исследований и разработки.
53. Подвергает ли поставщик свои продукты какой-либо другой независимой проверке безопасности за пределами зоны контроля головного офиса? Если да, то что это за проверка и как она осуществляется?	• Небольшая конкуренция между командами тестирования и разнообразие инструментов, методов и подходов может повысить полноту и строгость процессов тестирования безопасности. То, насколько большие и значительные инвестиции поставщик делает в эти процессы, говорит о его стратегическом замысле достичь долгосрочной безопасности и качества.

Вопрос	Дополнительные аспекты
54. Позволяет ли поставщик клиентам и правительственным органам тестировать свои продукты в их внутренних или внешних лабораториях силами их собственных сотрудников или при участии экспертов по безопасности?	• Степень открытости, которую поставщик демонстрирует по отношению к внешним сторонам, проверяющим качество его продуктов, свидетельствует как о его уверенности в собственном подходе, так и о способности оказывать доверие. Если вы видите перед собой постоянно закрытую дверь, это заставляет сомневаться в качестве и безопасности.
55. Если клиент или правительство захотят воспользоваться услугами независимой лаборатории по безопасности под руководством сторонней организации или применить Общие критерии (либо подобный подход), пойдет ли поставщик им навстречу?	• Готовность поставщика принять различные методы независимой оценки, даже с участием внешних сторон, свидетельствует об исполнении обязательств в отношении безопасности. • Вашей компании может потребоваться гибкость в сфере выбора методов оценки на основании рисков, связанных с вашим проектом, и величины контракта.
56. Контролирует ли головной офис (или бизнес-группы) поставщика внутренние или внешние лаборатории и посягает ли на их независимость? Есть ли право у членов головного офиса поставщика или его компании просматривать и корректировать какой-либо отчет или оценку до того, как они поступят в распоряжение клиента или правительства?	• Иногда поставщику приходится запускать продукт под давлением или в связи с желанием создать определенный имидж в рамках условий контракта. Если поставщик заявляет о проведении независимого тестирования его продуктов, он должен суметь доказать, что результаты проверки ни коим образом не подвергались воздействию или фальсификации в связи с запуском или другими факторами, оказывающими давление. • Никакие отчеты, сформированные в процессе оценки, не должны корректироваться компанией до момента отправки клиенту или другому заинтересованному лицу, кроме тех случаев, когда требуется защита от ненамеренного разглашения информации о потенциальных уязвимостях.
57. Имеет ли отдел исследований и разработки головного офиса поставщика доступ к каким-либо инструментам, процессам или сценариям, которые используют внешние лаборатории? Могли ли сотрудники головного офиса поставщика «предвосхитить» тестирование и повлиять на его результаты?	• Если сотрудникам головного офиса поставщика известно, каким образом лаборатория подтверждает доброкачественность продукта, есть ли у них возможность прибегнуть к маскировке продукта, чтобы инструменты лаборатории дали положительную оценку? Строгий подход к соблюдению конфиденциальности говорит о том, что целью любой лаборатории тестирования является повышение качества и безопасности, а не что-то иное.
58. Если одна из лабораторий или один из центров верификации поставщика обнаружит дефект или потенциальную уязвимость, какие процессы позволяют гарантировать решение проблемы силами отдела исследований и разработки и исключить повторное появление этой проблемы в будущих продуктах?	• Все мы видели такие примеры, когда после сообщения о наличии каких-либо отклонений ситуация не менялась. Поставщики должны суметь показать, каким образом они работают с каждой проблемой или дефектом в рамках систематического подхода. Они должны продемонстрировать, какие конкретные проблемы были обнаружены и какие меры были приняты для их решения. Вместе с тем, поставщикам важно показать свое понимание истинной причины возникновения проблемы и то, какие действия предпринимались для корректировки процессов, содержания обучения, шаблонов и т. д., чтобы исключить повторение ситуации.
59. Есть ли у лаборатории или центра верификации поставщика возможность проводить повторное тестирование после исправления программного обеспечения, чтобы подтвердить решение прошлой проблемы и отсутствие новых?	• Для обеспечения качества и безопасности однократного тестирования недостаточно. Технологии, угрозы и способы использования продуктов меняются. У лабораторий и сторонних организаций должна быть возможность повторно тестировать изменения после их внесения в продукты и устранения неполадок.

Вопрос	Дополнительные аспекты
60. Каким образом поставщик систематически интегрирует опыт, полученный на базе центров верификации, в свои бизнес-процессы?	• В ходе внутреннего, внешнего тестирования поставщика и тестирования силами клиента, помимо конкретных проблем, связанных с продуктом, могут быть обнаружены проблемы системного характера. Если поставщик использует комплексные, интегрированные подходы, он должен суметь продемонстрировать, каким образом учитываются полученные знания и решаются базовые проблемы.

4.7. Управление сторонними поставщиками

Многие крупные высокотехнологичные компании работают со сторонними производителями, используя их аппаратные и программные компоненты, а также поддержку при поставках и установке. Если в безопасности сторонних технологий или процессов имеются слабые места, это значительно снижает безопасность продуктов и услуг поставщика, поскольку такие технологии и процессы интегрируются в продукт, получаемый клиентом. Комплексная информационная безопасность означает, что производитель должен работать со своими поставщиками, внедряя наиболее эффективные приемы обеспечения кибербезопасности.

Вопрос	Дополнительные аспекты
61. Каким образом компания осуществляет управление безопасностью в отношении поставщиков? Установила ли она соответствующие критерии безопасности и передала ли их поставщикам? Как часто компания обновляет свои критерии, чтобы обеспечить их соответствие новейшим представлениям?	• Управление безопасностью является неотъемлемой частью отношений с поставщиками. Производитель должен передать поставщикам собственные требования, а также требования своих клиентов по информационной безопасности, в противном случае существует вероятность получения комплектующих с характерными недостатками с точки зрения безопасности. • Производитель должен суметь продемонстрировать, каким образом он следует отраслевым стандартам по безопасности или устанавливает критерии безопасности и передает соответствующие стандарты поставщикам. Необходимо сохранять актуальность установленных критериев, чтобы обеспечить охват новейших представлений и знаний в сфере безопасности. • Каким образом компания оценивает, предоставляют ли поставщики надлежащие ресурсы и обладают ли достаточным опытом для проведения мероприятий по обеспечению информационной безопасности? Требует ли она от поставщиков создания специальных групп по вопросам информационной безопасности? • Есть ли у компании специальные должности, структуры или процессы, подразумевающие ответственность за передачу требований, стандартов и знаний по информационной безопасности поставщикам и исключающие возможность упущения?
62. Какие требования к процессу закупки поставщики компании предъявляют своим поставщикам?	• Маловероятно, что каждый поставщик способен соответствовать всем требованиям по безопасности. Необходимы «аттестация» в области безопасности и оценка поставщиков, чтобы ограничить риск привлечения слабых с точки зрения безопасности поставщиков. • Критерий по «аттестации» поставщиков в области безопасности поможет им расширить свои возможности в отношении безопасности, чтобы соответствовать стандарту производителя, который оценивает их как квалифицированных поставщиков в рамках программы, требующей от поставщиков совместной работы по решению проблем информационной безопасности. • Компания должна суметь продемонстрировать строгий, нацеленный на безопасность процесс выбора поставщиков, который включает порядок оценки, повышения эффективности деятельности и контроля за ней.
63. Подписывает ли компания с ключевыми поставщиками условия договора или соглашения по вопросам безопасности, которые обеспечивают комплексный и учитывающий различные риски набор обязательных требований к поставщикам?	• Поставщики должны знать, что производитель требует от них с точки зрения безопасности. Соглашение по вопросам безопасности — хороший метод передачи поставщикам требований по безопасности и правовых обязательств. Соглашения по вопросам безопасности могут включать требования по усилению контроля в сфере безопасности и заставляют поставщиков нести ответственность за безопасность предоставляемых ими продуктов на договорной основе. • Компания должна суметь продемонстрировать, каким образом договоры и соглашения применяются для обеспечения соответствия всех комплектующих, используемых во всех продуктах и полученных из любых источников, процедуре и требованиям по безопасности.

Вопрос	Дополнительные аспекты
64. Какие процессы, установленные в компании, позволяют оценивать соответствие ее поставщиков каким-либо условиям или соглашениям по обеспечению безопасности? Использует ли компания оценочные листы или другие механизмы по усилению ответственности и повышению эффективности?	• Поставщики могут меняться, а проблемы в области безопасности — периодически снова возникать. Компания должна суметь продемонстрировать, каким образом в сотрудничестве с поставщиками оценивает эффективность работы и как они выстраивают совместную работу по решению проблем? Это может быть реализовано с помощью оценочных листов, аудитов и проверок.
65. Требует ли компания от своих поставщиков уведомлять ее о случаях обнаружения уязвимостей в их продуктах? Как компания использует эту информацию? Налажен ли процесс управления уязвимостями?	• Уязвимости могут быть обнаружены в любом продукте или компоненте. Ответственная компания должна последовательно и своевременно раскрывать уязвимости в своих продуктах. • Ваш поставщик должен уметь распоряжаться информацией об уязвимостях и, соответственно, демонстрировать сквозной процесс управления уязвимостями, независимо от того, кто направил уведомление о проблеме.
66. Какой подход реализует компания, если один из ее поставщиков не соблюдает, не может или не намерен соблюдать требования по безопасности?	• Существуют определенные издержки, связанные с соблюдением требований по безопасности, при этом выгоды могут быть не настолько прямыми и очевидными. • Если поставщик компании не соблюдает требования по информационной безопасности, какие меры принимаются для его убеждения в необходимости сотрудничества и совместного решения проблем безопасности? Каковы действия компании в случае отказа?
67. Соблюдает ли ваш поставщик ведущие международные стандарты, такие как стандарты Таможенно-торгового партнерства против терроризма (Trade Partnership Against Terrorism — C-TPAT) и Ассоциации защиты перевозимых грузов (Transported Asset Protection Association — TAPA)? Имеет ли он соответствующие сертификаты?	• В мире могут существовать различные мнения по поводу того, какой стандарт является самым лучшим, но поставщик должен продемонстрировать соответствие и сертификацию на основе общепризнанных стандартов. • Можно допустить, что стандарт может быть несовершенным, но поставщики должны продемонстрировать, по каким параметрам они способны превзойти стандарт, чтобы обеспечить дополнительные защитные процедуры и меры.
68. Проводит ли компания выездные аудиторские проверки системы безопасности своих поставщиков? Какова сфера охвата этих поверок? Компания должна объяснить, каким образом она работает с поставщиками для решения проблем, обнаруженных в ходе аудита.	• Каждому производителю и каждому поставщику необходимо сосредоточиться на потребностях клиентов. Аудиты и проверки помогают поставщику сохранить осведомленность и одновременно обеспечивают выполнение требований. Совместный подход по изучению потребностей друг друга помогает задать правильное направление деятельности.

4.8. Производство

Производители продуктов закупают комплектующие у целого ряда поставщиков, и они должны проследить, чтобы на всех этапах производственного процесса соблюдалась безопасность.

Вопрос	Дополнительные аспекты
69. Каким международным стандартам и передовому опыту следует поставщик в рамках производственной деятельности?	• В производственных центрах существует много сложных процессов и задач. Они охватываются множеством стандартов: от стандарта качества до стандарта охраны окружающей среды. Поставщик должен продемонстрировать комплексный подход к процессу производства, который вмещает в себя ведущие международные стандарты и подходы.
70. Поставщик должен описать ход своего производственного процесса и объяснить, каким образом проводится оценка процесса по всем его направлениям с целью выявления ненадлежащих или поврежденных продуктов.	• В рамках производственного процесса существует много возможностей для повреждения или порчи комплектующих до того, как деталь поступит в производственный центр поставщика и после того, как продукт будет собран и отправлен клиенту. Поставщик должен суметь объяснить порядок работы по замене запасных частей и возвратам в любой точке мира. Ключевым аспектом является обращение с носителями информации, на которых могут храниться персональные данные клиента.
71. Каким образом поставщик следит за тем, соответствуют ли закупаемые им комплектующие тем комплектующим, которые поступают в производственные центры, и обладают ли они нужными характеристиками?	• Поставщику необходимо учитывать, что любой высокотехнологичный компонент, который может быть поврежден или испорчен, находится под угрозой — вместо модели «всему доверяй» следует использовать модель «все проверяй». Каким образом действует поставщик?
72. Каким образом поставщик следит за тем, чтобы компоненты не подвергались несанкционированному обращению его собственными сотрудниками в производственном центре?	• Проблема внутренней угрозы реальна. Поставщику нужно проверять и гарантировать целостность поступающих материалов, но, помимо этого, он должен продемонстрировать процессы и средства контроля, которые позволяют проследить за тем, чтобы покидающие производственный центр продукты не подвергались несанкционированному обращению со стороны его собственного персонала.
73. Каким образом поставщик защищает свои продукты от несанкционированного обращения на этапе сборки до момента отгрузки?	• Готовые, но еще не отправленные продукты являются идеальными объектами для взлома. Каким образом поставщик обеспечивает соответствующую защиту на своих заводах и складах.
74. Каким образом поставщик следит за тем, чтобы продукты, которые получает клиент, соответствовали тем продуктам, которые покинули производственный центр?	• Еще одним фактором, который необходимо учитывать поставщику, является риск того, что продукт, который покидает территорию завода, находясь в целости и сохранности, может подвергнуться несанкционированному обращению до момента передачи клиенту. При выборе логистических компаний необходимо оценивать и учитывать комплексные процессы, связанные с организацией логистики.
75. Каким образом поставщик планирует свою потребность в комплектующих, чтобы ему как можно чаще можно было использовать новейшие компоненты?	• С учетом того, что в любое время могут быть обнаружены уязвимости, избыточное снабжение может привести к ситуации, когда в запасе вы будете иметь компоненты с уязвимостями — производство «строго по графику» снижает этот риск. Для эффективного использования этого принципа комплексное перспективное планирование объемов продаж должно быть автоматически связано с производством.
76. Если на готовое оборудование загружается специфическое программное обеспечение клиента, каким образом поставщик следит за тем, что оно является тем самым программным обеспечением, которое было авторизовано отделом исследований и разработки, и не было взломано?	• Вам бы хотелось, чтобы поставщик продемонстрировал сквозную интеграцию и смог показать, что аппаратное и программное обеспечение задействованы в одном процессе на одной производственной площадке и переходят в другой процесс на другой площадке, что исключает наличие пробелов и возможностей для несанкционированного обращения.

Вопрос	Дополнительные аспекты
77. Каким образом поставщик следит за тем, чтобы в производственном центре никто не имел возможности загрузить вредоносную программу на продукт?	• С точки зрения производственного персонала защита программного обеспечения очень важна. Поставщик должен быть способен продемонстрировать, каким образом регламентируется процесс производства, а также пояснить, классифицируется ли данная роль как ключевая и подлежит ли дополнительному контролю для исключения возможности внутренней угрозы.
78. Каким образом в производственном центре поставщика следят за тем, чтобы все тестовые порты были по умолчанию закрыты, когда продукт покидает территорию, и чтобы не было возможности доступа к ним после этого?	• На этапе производства часто требуется доступ к тестовым портам продукта. Если не обеспечен тщательный контроль и порты часто остаются открытыми по окончании производства, это позволяет злоумышленникам эксплуатировать их во время установки. Поставщик должен суметь продемонстрировать, каким образом порты автоматически закрываются в рамках системного производственного процесса.
79. Каким образом поставщик следит за тем, чтобы ходе производственного процесса неуполномоченные лица не знали о предназначении оборудования клиента и, соответственно, не могли внести в него несанкционированные изменения?	• С учетом того, что в производственном центре риску подвергается определенный продукт или продукты, необходимо принять все меры для исключения случаев подкупа и преступных действий, целью которых выступает конкретное оборудование клиента. Поставщик должен ограничивать круг лиц, которым известно, какое конкретное оборудование предназначено для конкретного клиента. Вместо использования имени клиента следует прибегать к таким методам, как стандарт кодирования.
80. Каким образом в случае возврата клиентом продуктов в связи с тем, что он сделал слишком большой заказ или аннулировал договор, поставщик отслеживает, не был ли осуществлен несанкционированный доступ к продукту до момента его возврата?	• Поставщик должен продемонстрировать, что модель «все проверяй» реализуется даже в случае возврата продукта. В рамках своих процедур и процессов поставщик должен расценивать данный продукт как поврежденный или испорченный и повторно подтверждать его целостность.
81. Какие процессы предусмотрел поставщик в случае возврата неисправного продукта, чтобы убедиться в отсутствии данных клиента на дисках или в памяти до того, как продукт будет отправлен в один из приемных центров?	• В технологическое оборудование обычно встроены запоминающие устройства. Поэтому продукты, возвращаемые в связи со сбоем или неисправностью, могут содержать данные клиента. Поставщики должны быть знакомы с местными законами о защите данных. • Поставщики должны суметь продемонстрировать, каким образом проходят их процессы по возврату и обработке брака и какие меры они принимают, если нет доступа к носителю данных для уничтожения данных на основании судебного решения.
82. Если неисправный продукт отремонтирован в одном из сервисных центров поставщика, каким образом гарантируется использование только оригинальных запасных деталей (т. е. исключается замена на поддельные детали) и отсутствие вредоносного программного обеспечения? Проводят ли поставщики повторное тестирование своих продуктов?	• Представления и процессы поставщика должны опираться на модель «все проверяй». Недостатки могут появиться на многих этапах процесса. Если компоненты ремонтируются и перераспределяются, поставщики должны снижать риск проникновения в цепочку поврежденного компонента, а также использования поддельных частей, вредоносных программ и неверной конфигурации. • Повторная проверка неисправных компонентов может препятствовать поступлению поврежденных, вложенных или поддельных продуктов в цепочку поставок через процесс возврата неисправных частей.
83. Есть ли у поставщика возможности и процессы для отслеживания компонентов? Источником проблем может стать что или кто угодно: программное или аппаратное обеспечение поставщика, сотрудники поставщика или третьи лица. Каким образом в случае возникновения проблемы поставщик сможет выяснить «кто», «зачем», «когда» и «где» ее спровоцировал?	• Точная и быстрая система отслеживания поможет оперативно локализовать источник нарушений и определить их объем, чтобы поставщик смог уведомить соответствующие стороны о необходимости принять меры для предотвращения распространения проблем. • Способность отслеживать процесс на всех его направлениях помогает поставщику найти корень проблемы, определить меры, которые могут исправить ситуацию, а также избежать ее повторения в будущем.

4.9. Безопасное предоставление услуг

Нет особого смысла направлять все усилия на разработку продуктов и при этом делать акцент на их безопасность, если на этапах их внедрения или поддержки безопасность не обеспечивается. Потребители, использующие оборудование для поддержки своего бизнеса, совершенно справедливо хотят получить гарантии безопасности и сохранности данных в ходе его эксплуатации и обслуживания.

Вопрос	Дополнительные аспекты
84. Какой доступ необходим инженерам по обслуживанию поставщика к установленному и функционирующему оборудованию и сервисам клиента? Могут ли они получить доступ к чему захотят и когда захотят?	• Поставщик должен суметь продемонстрировать, что клиент всегда контролирует доступ третьих лиц к своим технологиям и сервисам. В связи с этим поставщику необходимо подтвердить наличие ряда процессов и политик, которые регламентируют действия сотрудников и обеспечивают их подотчетность в отношении того, что они могут, а что не могут делать. • Часто клиенты применяют правило «явного письменного разрешения» и требуют, чтобы средства контроля соответствовали такой политике.
85. Каким образом поставщик защищает стандартные учетные записи или учетные записи, которые клиент предоставляет для получения технической поддержки и обслуживания?	• В рамках своих политик и процедур поставщик должен суметь продемонстрировать, что происходит с этими параметрами доступа, каким образом они защищены и когда они возвращаются, а также доказать, что они подлежат независимой проверке и аудиту.
86. Какие меры контроля устанавливает поставщик в отношении использования портативных компьютеров и технических средств, которые приносят инженеры? Например, могут ли инженеры загружать собственные программные инструменты на портативный компьютер?	• Если портативные компьютеры инженеров взламываются или иным образом заражаются вредоносными программами, злоумышленники могут использовать их, чтобы украсть данные клиента или атаковать его сети. Поэтому поставщик должен подробно изложить те меры, которые принимаются для защиты и контроля портативных компьютеров сотрудников.
87. К каким процессам и средствам контроля прибегает поставщик, чтобы обеспечить использование инженерами только надлежащего программного обеспечения для каждого клиента?	• Зачастую технология поставщика оказывается сложной и включает технические средства от нескольких поставщиков. Иногда для интеграции и эффективной работы этих компонентов требуется набор специфических программ. Поставщик должен быть способен продемонстрировать, что любые изменения и обновления, которые используются для вашей технологии, совместимы с утвержденной для вас, как для клиента, программой, включая правильную версию и сборку.
88. Каким образом поставщик следит за тем, чтобы инженеры по обслуживанию или технической поддержке не могли внести несанкционированные изменения в программное обеспечение, а также установить уязвимую или вредоносную программу?	• Вам, как покупателю, необходимо быть уверенным, что специалист службы поддержки умышленно или случайно не оставит вам то, о чем вы его не просили, поскольку злоумышленники могут заменить компоненты аппаратного обеспечения или загрузить неутвержденное программное обеспечение, чтобы нарушить целостность продукта, внедрить уязвимую или вредоносную программу. • Применяя модель «все проверяй», поставщики демонстрируют, каким образом предотвращается доступ злоумышленников к продуктам или компонентам в процессе развертывания или обновления программного обеспечения.
89. Поставщик должен объяснить свой подход к повышению отказоустойчивости аппаратного обеспечения, использованию проверок программного и аппаратного обеспечения, а также средств обеспечения безопасности (например, брандмауэров) для конкретных клиентов.	• Существует документально подтвержденный передовой опыт, который служит руководством для вашего поставщика и вашей собственной группы ИКТ по «укреплению» (т. е. усилению защиты от атак) оборудования, которое вы приобретаете. Это оборудование также может включать ряд возможностей и функций по обеспечению безопасности. • Для вас может оказаться важным, что любые работы по установке, поддержке или техническому обслуживанию опираются на этот передовой опыт, а также гарантируют правильное включение и отключение соответствующего оборудования.

Вопрос	Дополнительные аспекты
90. Если поставщикам приходится собирать данные для поиска и устранения неисправности, получают ли они официальное разрешение клиента и осуществляют ли сбор данных строго в объеме, предусмотренном данным разрешением?	• Для поиска и устранения неисправностей на технологическом оборудовании может потребоваться доступ к данным на этом оборудовании. Должен быть представлен набор согласованных политик и процедур, который в случае необходимости обеспечивает защиту персональных данных пользователя и коммерческой информации.
91. Если специалист службы поддержки поставщика не может устранить неисправность на месте, а собранные данные необходимо отправить в другую страну для анализа, каким образом контролируется этот процесс для обеспечения соответствия требованиям клиента и местного законодательства?	• Иногда сложные ошибки невозможно устранить на месте силами оперативных специалистов. При этом для поиска и устранения неисправностей необходимо привлечь инженеров отдела исследований и разработки, расположенного в другом месте. • Поставщику и вам, как клиенту, необходимо договориться о правилах обработки данных в том случае, если служба технической поддержки расположена на территории другого государства. Какую степень гибкости проявляет поставщик?
92. Какие процессы применяет поставщик для управления данными, собранными в целях поиска и устранения неисправностей, после того, как они больше не нужны?	• Данные — это активы клиента, которые можно использовать только в пределах разрешенных объемов и сроков. По окончании обслуживания данные необходимо удалять, чтобы предотвратить их использование в целях, не связанных с обслуживанием. Каким образом поставщик реализует этот принцип и следит за его соблюдением?
93. Контрольные журналы играют важную роль для предоставления информации о том, что происходит в системе. Каким образом поставщик удостоверяется в том, что его контрольные журналы содержат всю существенную информацию?	• Поставщик должен суметь продемонстрировать, какой подход он использует к регистрации данных и защите детальных контрольных журналов. • Использование аудиторского программного обеспечения, которое широко признается и применяется в отрасли, может обеспечить более объективные и надежные результаты.
94. Клиенты полагаются на своих поставщиков, особенно в критических ситуациях: во время прерывания обслуживания, стихийного бедствия с точки зрения устойчивости бизнеса. Насколько хорошо оснащен и заинтересован поставщик, чтобы поддержать вас в тяжелые времена? Попросите привести конкретные примеры.	• Наладил ли поставщик постоянные каналы связи со своими клиентами для совместного обсуждения требований по информационной безопасности, составления дорожных карт и планов, чтобы в полной мере соответствовать стратегиям клиентов в сфере информационной безопасности, в том числе и в тяжелые времена? • Риски возникали перед пользователями во все времена, даже в периоды стихийных бедствий, поскольку злоумышленники используют любую возможность. Часто поставщики обладают ценным багажом международного опыта, инструментов и ресурсов, которые помогают защитить клиентов. Например, повторяющиеся атаки типа «отказ в обслуживании» требуют быстрого расширения возможностей оборудования, использования новых или отличающихся технологий, при этом со стороны поставщика вы хотите увидеть готовность оказать помощь и продемонстрировать гибкость. • Стихийное бедствие может произойти в любой момент, а ваши поставщики способны сыграть важную роль в поддержании устойчивости вашего бизнеса. Выявление их заинтересованности в том, чтобы помочь вам в сложные времена, позволяет оценить долгосрочную заинтересованность в успехе вашего бизнеса.

4.10. Устранение проблем, дефектов и уязвимостей

Само собой разумеется, что никто не может дать 100-процентную гарантию безопасности. В результате способность компании оперативно реагировать на проблемы и делать соответствующие выводы об их причинах является критически важной как для клиента, так и для производителя.

Вопрос	Дополнительные аспекты
95. Создал ли поставщик группу по расследованию случаев нарушения безопасности продуктов PSIRT (Product Security Incident Response Team), компьютерную группу по реагированию на чрезвычайные ситуации Vendor CSIRT (Vendor Computer Security Incident Response Team) или их аналоги? Поставщик должен подробно описать их функции и то, каким образом с ними можно связаться. Каким процессам и требованиям обязаны следовать группы PSIRT и Vendor CSIRT?	• Проблемы неизбежны, и вам хотелось бы знать, можно ли в случае их возникновения быстро уведомить поставщика о любого рода реальных или предполагаемых нарушениях безопасности. У вас также может появиться желание удостовериться в наличии механизмов по отслеживанию проблемы в системе безопасности до момента ее решения. • Важно иметь в распоряжении утвержденный набор процессов, которым следуют группы PSIRT и Vendor CSIRT в ходе выполнения своих обязанностей.
96. Какие механизмы утвердил поставщик для того, чтобы взаимодействовать с группами CSIRT или координаторами обслуживания клиента, чтобы они могли сообщать вашей компании о трудностях и совместно работать для быстрого их устранения?	• Ваша компания может быть заинтересована в наличии набора механизмов по налаживанию контактов от одной внутренней центральной точки (PSIRT или Vendor CSIRT) до нескольких подразделений. Поставщик должен продемонстрировать свои возможности и гибкость в применении целого ряда моделей.
97. Разработал ли поставщик подход к работе с исследовательским сообществом в сфере безопасности?	• Организация, которая никого не слушает, ничему не учится. Поставщикам нужно работать с широким кругом разнообразных компаний и частных лиц, которые могут обнаружить недостатки в их продуктах. Каким образом поставщик справляется с этой ситуацией, показывая эффективную и профессиональную работу?
98. Насколько хорошо оснащен поставщик на случай возникновения серьезного инцидента, чтобы обеспечить своим клиентам своевременное оповещение и предоставление необходимых ресурсов для реагирования? Поставщик должен суметь четко описать процесс эскалации.	• Если в вашей организации произошел серьезный инцидент, вы захотите удостовериться в том, что поставщик утвердил механизм быстрого оповещения, а также внутренние процессы по управлению инцидентами, включая эскалацию в рамках его компании. • С учетом того, что у большинства предприятий нет квалифицированных специалистов, сидящих без дела, каким образом поставщик может продемонстрировать, что вышестоящие руководители в обязательном порядке получают информацию о ситуации и могут выделить необходимую помощь для решения проблемы?

4.11. Аудит

Легко вести разговоры и рисовать радужные картины, но делаете ли вы то, что обещали сделать, именно так, как это было согласовано, соблюдая оговоренные временные рамки, требования к расходам, качеству и безопасности? Откуда вы можете это знать? Регулярное проведение комплексных аудитов поможет убедить клиентов и заинтересованных лиц в том, что для достижения соответствующих итоговых показателей используются только надлежащие политики, процедуры и стандарты.

Вопрос	Дополнительные аспекты
99. Какие процессы и механизмы реализует поставщик для проведения внутреннего аудита и составления отчетов в сфере безопасности, чтобы обеспечить понимание Советом директоров реального уровня риска в организации, а также состояния инцидента и его последствий, независимо от того, какие сообщения поступают?	• Наличие формального контроля деятельности в сфере информационной безопасности (внутреннего, внешнего, силами клиента или третьей стороны) говорит о том, что Совет директоров открыт для получения реальных отзывов. • Способность продемонстрировать реализацию этого принципа свидетельствует о том, что стратегии, политики и стандарты являются «живыми» и могут приспосабливаться к новым угрозам и ситуациям. • Если Совет директоров или Комитет получают формальный отчет по действиям, достижениям и показателям в сфере информационной безопасности, это говорит о том, что такая практика является частью обычной деятельности предприятия, а не отдельным «проектом» или «специальным» мероприятием.
100. Утвердил ли поставщик механизм, который позволяет внешним заинтересованным лицам или их уполномоченным организациям проводить аудит?	• Демонстрируя открытость и прозрачность по отношению к ключевым заинтересованным лицам и принимая внешние аудиторские проверки и отчеты, компания заявляет о своем ответственном отношении и культуре непрерывного обучения. • Чем более вы открыты для внешнего анализа, тем больше предложений по оптимизации вы получите.

5. О компании Huawei

Продукты и решения компании Huawei охватывают более 170 стран и регионов, и используются третьей частью населения земного шара. Штат компании насчитывает 150 000 человек, а средний возраст сотрудников — 32 года. В среднем, 79 % составляет местный персонал. К концу 2013 года мы заключили 281 коммерческий контракт в области решений LTE и 162 коммерческих контракта в области решений EPC, в рамках которых развернули 110 коммерческих сетей стандарта LTE и 88 коммерческих сетей стандарта EPC.

Благодаря постоянным инновациям компания Huawei удерживает ведущую роль в отрасли и имеет один из самых внушительных портфелей прав интеллектуальной собственности (IPR) в телекоммуникационной отрасли. Компания Huawei уважает и защищает права интеллектуальной собственности других игроков. Huawei инвестирует более 10 % выручки от продаж в область НИОКР, в которой заняты 45 % сотрудников. В 2013 году компания Huawei инвестировала в НИОКР 30,734 миллиарда RMB, что составляет 12,9 % от общего годового дохода. Общий объем инвестиций в сферу исследований и разработки за последнее десятилетие превысил 151,9 миллиардов RMB.

По данным на 31 декабря 2013 года, компания Huawei подала 44 168 заявок на получение патентов в Китае, 18 791 заявку — на основе Договора о международной патентной кооперации (PCT) и 14 555 заявок — за границей. Путем накопления мы получили 36 511 лицензий на пользование патентами. По сравнению с количеством, компания Huawei придает большее значение коммерческой ценности и качеству IPR. Начиная с 2010 года и до настоящего времени наши 466 ключевых заявок на грант в области 3GPP LTE были одобрены, благодаря чему мы заняли 1 место в отрасли. Компания Huawei занимает лидирующую позицию по количеству патентов в области FTTP (Fibre To The Premises — «волокно в жилище»), OTN (Optical Transport Network — «оптическая транспортная сеть»), G.711.1 (стационарный широкополосный аудиоканал) и т. д. Поэтому защита прав интеллектуальной собственности имеет решающее значение для текущего успешного положения компании, и в связи с этим Huawei является чемпионом в этой области.

Компания открыла 16 научно-исследовательских институтов по всему миру, 28 объединенных инновационных центров и 45 обучающих центров. В целом, 65 % нашего дохода формируется за пределами материкового Китая, а 70 % материалов мы приобретаем у иностранных компаний. США являются крупнейшим поставщиком компонентов; в 2013 году 32 % покупок компании Huawei (на сумму около 7,237 миллиардов долларов США) было совершено у американских компаний.

Мы предоставляем услуги эксплуатационного обслуживания более чем 120 операторам в 75 странах мира и помогаем клиентам в достижении высокой производственной эффективности. Мы получили более 340 контрактов на предоставление управляемых услуг. Компания Huawei построила ИТ-решения на базе облака и организовала совместную работу с 400 партнерами для ускорения коммерческого применения технологий облачных вычислений в различных отраслях. По данным на конец 2013 года, мы открыли для клиентов по всему миру 330 центров сбора и обработки информации, включая 70 центров данных облачных вычислений.

В 2013 году подразделения компании Huawei по обслуживанию клиентов отгрузили 128 миллионов высокотехнологичных устройств во все уголки мира, в том числе около 60 миллионов мобильных телефонов, 44,5 миллиона устройств мобильной широкополосной связи и 24,4 миллиона домашних устройств. Отгрузки смартфонов достигли показателя 52 миллиона — на 60 % больше, чем в 2012 году.

Компания Huawei с энтузиазмом поддерживает основные международные стандарты и принимает активное участие в их разработке. К концу 2013 года компания Huawei присоединилась более чем к 170 организациям по стандартизации и добровольной стандартизации в отрасли, в том числе 3GPP, IETF, ITU (Международный союз электросвязи), OMA, ETSI (Европейский институт стандартов по телекоммуникациям), TMF (Tele Management Forum), ATIS и Open Group. В 2013 году компания Huawei подала в эти органы стандартизации более 5 000 предложений. Также мы занимаем 185 должностей в организациях, поддерживающих стремление к единому подходу в отношении международных стандартов.

По данным на 31 декабря 2013 года, 84 187 сотрудников приобрели пакеты акций компании. План приобретения акций служащими тесно связывает долгосрочное корпоративное развитие Huawei с личным вкладом наших сотрудников и формирует устойчивый механизм преданности и разделения прибыли. Это позволяет нам руководствоваться перспективным подходом, а также обеспечивает возможность балансирования рисков с помощью поощрения и стратегии. Сотрудники знают, что, если мы не будем выгодно отличаться в области обслуживания клиентов или если мы предпримем неприемлемые действия, их собственные акции могут упасть, а пенсии сократиться.