

Article #: 030030	Date: 15 ноября 2011
Article Name: Вопрос оценки 30. Политика безопасности	AGB Reference: none
Version #: v01	Category: Knowledge Article – Evaluation Questions

[Дополнительные примечания](#)

[Предложения на основе передовых методов](#)

[Текст вопроса](#)

1. ДОПОЛНИТЕЛЬНЫЕ ПРИМЕЧАНИЯ

15 ноября 2011 г.

1.1 В отношении вопроса 30(a):

- Уровни безопасности определяются кандидатом. Кандидат должен составить список обязательств, которые он планирует взять на себя перед своими будущими владельцами регистраций, исходя из определенных уровней безопасности. Кроме того, следует предоставить также краткое описание каждого обязательства.
- Отчет о результатах независимой оценки должен продемонстрировать эффективные механизмы безопасности инфраструктуры ИТ, которая будет использоваться для выполнения операций реестра. В ответе кандидата должно быть уделено внимание всем областям, которые нуждаются в улучшении согласно отчету о результатах независимой оценки. Следует иметь в виду, что ICANN не станет публиковать отчет независимой оценки для всеобщего доступа.

1.2 В том, что касается вопроса 30(b): необходимо предоставить политику и процедуры обеспечения безопасности, посвященные исключительно операциям реестра кандидата. Поскольку данная информация по своей природе является конфиденциальной, ICANN не станет публиковать политику обеспечения безопасности кандидата для всеобщего доступа.

2. ПРЕДЛОЖЕНИЯ НА ОСНОВЕ ПЕРЕДОВЫХ МЕТОДОВ:

15 ноября 2011 г.

2.1 Кандидатам следует ознакомиться с каждым вопросом оценки полностью, включая все примечания, критерии и пояснения по начислению баллов. Ответ должен учитывать все указанные критерии и включать подробное обоснование, демонстрирующее глубокое понимание данных критериев (примеры из работы и т. п.).

2.2 Если используются сокращения, то при первом упоминании сокращения оно должно быть расшифровано, даже если это общепринятое сокращение определенного термина, продукта или услуги.

2.3 Кандидаты, которые предлагают поручить выполнение отдельной функции или ряда функций, относящихся к операциям реестра, независимым поставщикам услуг, должны учесть все критерии, указанные для каждого вопроса, и предоставить подробное обоснование, демонстрирующее глубокое понимание критериев (примеры из работы и т. п.).

2.4 Если кандидат ограничится предоставлением краткого резюме, это не будет засчитано как демонстрация технических и операционных возможностей или доказательство наличия необходимых ресурсов. Кандидат должен предоставить подробное пояснение плана обеспечения ресурсами и уделить внимание таким вопросам, как ресурсы, которые требуются для управления и эксплуатации той или иной функции, необходимая квалификация и опыт, график посменной работы и т. п. В дополнение к такому плану обеспечения ресурсами можно использовать и резюме.

2.5 Если ответ содержит ссылку на политику или процедуру, кандидат должен предоставить краткие сведения о данной политике или процедуре. Кандидат не должен прилагать копии с текстом упоминаемых политик и процедур, за исключением случаев, когда его об этом попросят.

2.6 Если кандидат предлагает использовать нестандартное программное обеспечение, он должен уточнить масштаб и объем отклонения от стандартных процедур, в том числе описать процесс разработки нестандартного программного обеспечения. Подобное пояснение необходимо для того, чтобы оценочная комиссия могла представить степень соответствия данного программного обеспечения стандартным процедурам и правилам.

3. ТЕКСТ ВОПРОСА

- (а) Представьте краткую информацию о политике безопасности для предлагаемого реестра, включающую следующее:
- указание на какие-либо независимые оценки возможностей системы безопасности и планы периодического проведения независимой оценки для тестирования возможностей системы безопасности;
 - описание расширенных уровней безопасности или возможностей, соответствующих природе строки рДВУ, в том числе указание на существующие международные или отраслевые стандарты безопасности, которым кандидат намерен следовать (необходимо представить адрес соответствующего сайта);
 - список договорных обязательств перед владельцами регистраций в отношении уровней безопасности.

Чтобы набрать 2 балла, ответы должны также содержать:

- Данные о независимой оценке, демонстрирующие наличие эффективных средств обеспечения безопасности (например, ISO 27001).



Краткое описание вышеуказанного не должно превышать 20 страниц. Обратите внимание, что полное описание политики обеспечения безопасности реестра необходимо представить в соответствии с вопросом 30(b).

- (b) Опишите всеобъемлющие политики и процедуры обеспечения безопасности для предлагаемого реестра, в том числе следующее:
- контроль системного (данные, сервер, приложение/услуги) и сетевого доступа, обеспечение безопасного управления системами, включая информацию о том, как они отслеживаются, как производится вход в систему и восстановление;
 - ресурсы для обеспечения безопасной интеграции обновлений между системами реестров и серверами имен, а также между серверами имен, если таковые имеются;
 - отчеты о независимой оценке, демонстрирующие возможности системы безопасности (представляются в виде приложений), если таковые имеются;
 - меры предосторожности, которые уменьшают риски, вызываемые атаками типа «отказ в обслуживании»;
 - политики, планы и процедуры реакций на проблемы, связанные с вычислительным оборудованием и сетью;
 - планы по минимизации рисков, связанных с несанкционированным доступом к системам или нанесением ущерба данным реестра;
 - механизмы обнаружения вторжений, анализ угроз для предлагаемого реестра, средства защиты, которые будут использоваться для противодействия этим угрозам, и обеспечение регулярного анализа угроз;
 - сведения о возможностях проверки всех видов доступа к сети;
 - подход с учетом физической безопасности;
 - указание отдела или группы, ответственных за организацию системы безопасности реестра;
 - проверки данных персонала службы безопасности;
 - описание выявленных главных угроз безопасности реестра;
 - планы выделения ресурсов для первичной реализации и последующей поддержки этого аспекта критериев (количество и описание ролей персонала, выделенного для данной области).

ОТКАЗ ОТ ОБЯЗАТЕЛЬСТВ: Настоящий материал подготовлен исключительно в информационных целях и не отражает всех требований и критериев, которым должен соответствовать кандидат. ICANN не приводит в нем правовых, финансовых, деловых или иных рекомендаций. Данный материал не вносит изменений в Руководство кандидата или условия и положения программы ввода новых рДВУ. Данный материал также не является отказом от каких-либо политик, процедур или соглашений ICANN. Если любые сведения, приведенные в настоящем материале, противоречат или не соответствуют информации, опубликованной ICANN в других источниках, не руководствуйтесь настоящим электронным письмом, не получив подтверждения или разъяснения со стороны ICANN.