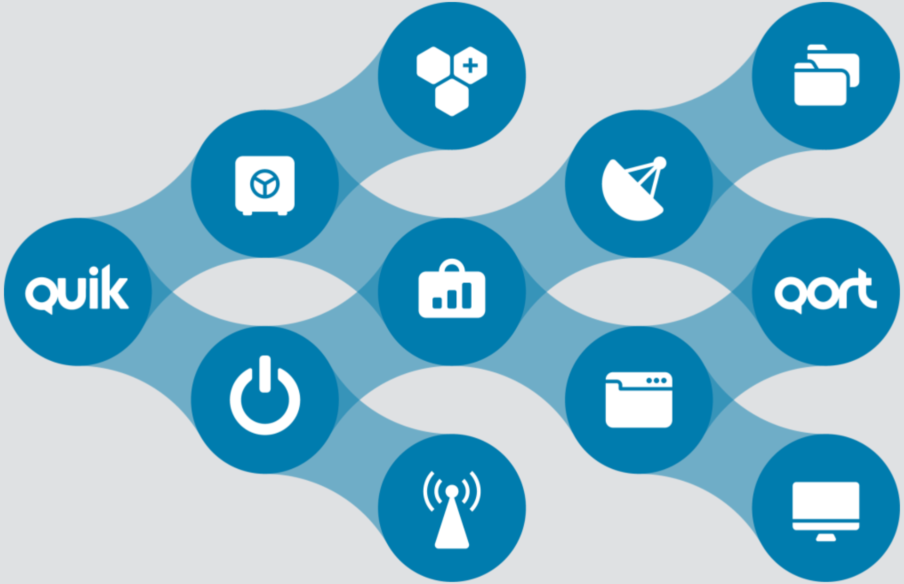
Взаимодействие вендора и профучастника

в процессе реализации требований Положения 757-П Банка России в части оценки соответствия ОУД-4



Владимир Курляндчик

Директор по развитию ARQA Technologies

2021

Главная новелла 757-П

анализ уязвимости

оценка соответствия

Дилемма «правильного ПО»

Сертификация ФСТЭК

(сроки, сложность, оперативность)

Оценка соответствия ОУД-4

Оценка профучастником соответствия ПО требованиям

Самостоятельная оценка профучастником ПО на соответствие:

- договоренность с вендором о предоставлении текстов ПО
- выделение ресурса профучастника на ПО каждого вендора
- возникновение длительных регламентов оценки новых версий ПО каждого вендора

Вендоры идут навстречу интересам профучастников:

- проведение вендором оценки соответствия ОУД-4 с привлечением сертифицированных оценщиков на основе общей методики

Общая методика

- **Политики Безопасности профучастников должны быть унифицированы**
- **Профиль защиты ЦБ**

Статус самостоятельного анализа уязвимости и оценки соответствия самим вендором

В соответствии с абзацем 4 п.1.8 Положения 757-П «…оценка соответствия …проводится самостоятельно или с привлечением проверяющей организации».

Некоторые это трактуют так, что проверяющей организацией может быть вендор ПО, но здесь возникает два момента:

- может ли вендор проверять сам себя, как заинтересованное лицо,
- проверка на соответствие требованиям ГОСТ Р ИСО/МЭК 15408-3-2013 относится к лицензируемым ФСТЭК видам деятельности — «услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации»

Мы придерживаемся мнения, что профучастник может пользоваться результатами проверки, проведенной вендором ПО, но только с привлечением независимой лицензированной ФСТЭК организации

Кодировка участков обработки информации

В соответствии с абзацем 5 п.1.8 Положения 757-П НФО должны регистрировать «код, соответствующий технологическому участку».

- Ряд профучастников считает, что этот код должен регистрироваться непосредственно в журналах прикладных систем (например, QUIK).

- Однако, наше мнение состоит в том, что разбиение на технологические участки у профучастников могут быть очень разнообразны, и стандартизировать это разбиение путем внесения в алгоритмы ПО брокерской системы неестественно.

Проверка целостности сообщений

В соответствии с п.1.9 Положения 757-П «Некредитные финансовые организации, …должны обеспечить целостность электронных сообщений и подтвердить их составление уполномоченным на это лицом».

В качестве механизма обеспечения данного требования, с учетом упомянутого в абзаце 2 п.1.9 Положения «…иных, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения», по нашему мнению вполне применима уже широко используемая комбинация протоколов передачи данных SSL с дополнительной аутентификацией посредством СМС

Регуляторный арбитраж

Российские вендоры под давлением Банка России через профучастников

Иностранные вендоры вне регуляции

Спасибо за внимание!