Обоснование невозможности соблюдения ограничения на допуск программного обеспечения, происходящего из иностранных государств

В соответствии с требованиями Директивы правительства от 11.07.2016 №4972п-П13 ООО «УК «РОСНАНО» представляет обоснование невозможности соблюдения ограничения на допуск программного обеспечения, происходящего из иностранных государств:

Процедура закупки: открытый запрос предложений (на ЭТП B2B-rusnano № 897058, в ЕИС № 31705577625)

Цель закупки: Предоставление права использования программного обеспечения, а также поставка сертификата технической поддержки системы обнаружения сложного специализированного вредоносного программного обеспечения.

Класс (классы) программного обеспечения: «Средства обеспечения информационной безопасности» Классификатора программ для электронных вычислительных машин и баз данных, утвержденного приказом Министерства связи и массовых коммуникаций Российской Федерации от 31.12.2015 № 621 «Об утверждении классификатора программ для электронных вычислительных машин и баз данных».

Требования к функциональным, техническим и эксплуатационным характеристикам объекта закупки, которым не соответствуют программное обеспечение, базы данных, сведения о которых включены в Единый реестр российских программ для электронных вычислительных машин и баз данных:

- Возможность отслеживания трафика на всех сетевых портах по более чем 100 протоколам, что обеспечивает максимально возможную степень защиты;
- Наличие специализированных модулей обнаружения и настраиваемых изолированных сред, позволяющих выявлять и анализировать вредоносные программы, сеансы обмена данными с командными центрами, скрытые действия злоумышленников;
- Возможность обнаружения атак в широком спектре защищаемых систем - ОС Windows, Mac OS X, Android, Linux и др.;
- Наличие глобальной системы оповещения об угрозах, используемой системами обнаружения для анализа атак, обмена данными о признаках взлома и заражения;
- Возможность анализа вложений в сообщениях электронной почты с использованием специальных модулей обнаружения и изолированной среды - исполняемых файлов Windows, документов Microsoft Office, PDF- и ZIP-файлы, вложенных URL-адресов, проверка паролей;
- Возможность работы с интегрированными «песочницами» с поддержкой ОС WinXP/Win7/Win8/Win10/Win2003/Win2012, а также настраиваемыми типами «песочниц»;
- Интеграция с другими системами информационной безопасности, такими как DLP, IDM, SIEM и др.;
- Возможность получения подробной отчетности о результатах анализа атак, включая сведения о действиях вредоносных образцов и обмене данными с командными центрами через централизованную систему информационных панелей и отчетности.

Рук. направления ИБ А.А.Жиганов