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 РТС-Тендер № 705826, в ЕИС № 31907657509)

Цель закупки: Поставка специализированного ПО (лицензий) и сертификатов на техническую поддержку для программно-аппаратных комплексов систем обеспечения информационной безопасности организации.

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, необходимым для осуществления управления неструктурированными данными (ПО Varonis DatAdvantage, DatAlert):

- В рамках одного программного интерфейса и единой базы поддерживаются: Windows, NAS, SharePoint, Exchange, Active Directory;
- Единая платформа, включающая в себя: отображение прав доступа, контекстную классификация данных, аудит действий пользователей, отчетность и оповещения в реальном времени, поведенческий анализ пользователей и выявление аномалий использования данных;
- Возможность моделирования и изменения прав доступа непосредственно из интерфейса системы;
- Простота администрирования, широкий ассортимент типов собираемых событий, возможность комбинированного анализа всех потоков метаданных (права, логи, контент);
- Отсутствие дополнительной нагрузки на контролируемые ресурсы, так как их штатный функционал аудита не используется;
- Отсутствие необходимости в автоматическом обновлении программного обеспечения (возможно вручную под контролем системного администратора), не требуется выход за пределы периметра организации для нормального функционирования;
- Интеграция с другими системами информационной безопасности, такими как DLP, IDM, SIEM и др.;
- Низкая трудоемкость и временные затраты, связанных с получением матрицы доступа сотрудников к информации, а также при проведении служебных расследований;
- Поддержка ролевой модели с делегированием различных полномочий при эксплуатации системы.

Подготовил: _____ А.А. Жилинов