**Приложение № 3**

**Перечень программного обеспечения и оборудования**

|  |  |
| --- | --- |
| **№** | **Класс решений** |
| 1. | Защищенные среды виртуализации для реализации ЗОКИИ, АСУ ТП, ИСПДн (Secure Virtualization Platform) |
| 2. | Системы защиты периметра и предотвращения вторжения (NGFW, IDS, IPS, SWG, VPN) |
| 3. | Системы выявления и реагирования на инциденты (SIEM, SOAR, SOC, Sandbox, Anti-APT, TIP) |
| 4. | Системы защищенного файлового обмена (EFSS) |
| 5. | Системы аудита и защиты данных (DLP, DCAP, DAM, DBF, маскирование данных) |
| 6. | Антивирусные системы и средства защиты конечных устройств (EDR, XDR, MDM) |
| 7. | Системы защиты API (API Security Gateway) |
| 8. | Система управления уязвимостями и контроля соответствия стандартам |
| 9. | Средства безопасной разработки (SCA, OSA, SAST, DAST, HAST) |
| 10. | Системы защиты от DDoS-атак |
| 11. | Системы защиты контейнеров для информационных систем с микросервисной архитектурой (Container Security Platform) |
| 12. | Защищенные системы аудиоконференции (селекторной связи) и видеоконференцсвязи для предприятий (Secure Collaboration Platform) |
| 13. | Програмное обеспечение «Речевая аналитика» (U-Speech Analytics) |
| 14. | Системы управления доступом и аутентификацией (IAM, PAM, MFA) |
| 15. | Межсетевые экраны для веб-приложений (WAF) |
| 16. | Системы шифрования, электронная подпись и инфраструктура публичных ключей |
| 17. | Система защиты критической инфраструктуры (ГосСОПКА, безопасность АСУТП, безопасность IoT) |