

## «Перечень классов решений по направлениям для отражения кибератак»

№	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, Криптошлюз)
3	Системы выявления и реагирования на инциденты (SIEM, SOC)
4	Системы управления инцидентами (SOAR, IRP)
5	Системы противодействия сложным и целевым атакам (Sandbox, Anti-APT, NTA, Deception)
6	Системы защищенного файлового обмена (EFSS)
7	Системы аудита и защиты данных (DLP, DCAP, DAM, DBF, маскирование данных)
8	Антивирусные системы и средства защиты конечных устройств (EDR, XDR, MDM)
9	Системы защиты API (API Security Gateway)
10	Система управления уязвимостями и контроля соответствия стандартам (VM)
11	Средства безопасной разработки (SCA, OSA, SAST, DAST, HAST)
12	Системы защиты от DDoS-атак
13	Системы защиты контейнеров для информационных систем с микросервисной архитектурой (Container Security Platform)
14	Защищенные системы аудиоконференции (селекторной связи) и видеоконференцсвязи для предприятий (Secure Collaboration Platform)
15	Программное обеспечение «Речевая аналитика» (U-Speech Analytics)
16	Системы управления доступом и аутентификацией (IAM, PAM, MFA)
17	Межсетевые экраны для веб-приложений (WAF)
18	Системы шифрования, электронная подпись и инфраструктура публичных ключей
19	Антифрод
20	Квантовое шифрование
21	Системы обучения, оценки компетенций и повышения осведомленности