

????????? ??????? ?? ??

??????????

- Нормативные акты в РФ по отраслям и меры защиты: <https://regulhub.kaspersky.ru/>

KUMA

- Онлайн-справка по KUMA: <https://support.kaspersky.com/help/KUMA/2.1/ru-RU/217694.htm>
- Группа в Telegram: <https://t.me/kumasiem>
- База знаний: <https://kb.kuma-community.ru/>
- Коллекция API на Postman: <https://www.postman.com/kl-ru-presales/workspace/kaspersky-products-apis-ru/overview>

Windows

- Рекомендации по аудиту событий Windows: <https://github.com/JSCU-NL/logging-essentials>
- Рекомендации от Kaspersky MDR: <https://support.kaspersky.com/MDR/ru-RU/204200.htm>
- Скрипты для **быстрой настройки политики аудита по рекомендациям MDR**: <https://box.kaspersky.com/d/48e696a683c04340926e/>
- **✓ Рекомендуется** ID событий отправляемые в MS Sentinel: <https://learn.microsoft.com/en-us/azure/sentinel/windows-security-event-id-reference> (Строка с Common)
 - **✓ Рекомендуется** Дополнительные полезные ID событий (пресейл рекомендация дополнение к MS Sentinel): <https://box.kaspersky.com/f/8c71107f71054d3981c3/>
- Рекомендации от ManageEngine: <https://www.manageengine.com/products/active-directory-audit/guide-to-configure-group-policy-object-auditing-in-adauditplus.html>
- Рекомендации от MS:
 - <https://learn.microsoft.com/ru-ru/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>
 - <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor>

- Написание регулярных выражений: <https://regex101.com/>

Revision #21

Created 2023-08-10 08:10:16 UTC by Koala

Updated 2026-05-27 11:56:05 UTC by Ierat