www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

ГАДАНИЕ НА ВЗЛОМАХ. ПРЕДСКАЗАТЕЛЬНАЯ СИЛА EPSS

Сергей Гордейчик –
генеральный директор СайберОК

В конце года принято подводить итоги и делать предсказания. Давайте совместим оба ритуала и посмотрим, насколько лучше эксперты СайберОК могли бы контролировать поверхность атак, если бы слепо верили в магию EPSS. Спойлер: контролировали бы не очень. И вот почему.

Что мы сделали

Мы взяли все CVE, которые CISA добавила в KEV за 2025 год (то есть «уже ломают так, что заметили федералы»).

Всего KEV-уязвимостей: 245.
EPSS «на дату добавления в KEV» удалось получить только для 203 (≈83%). То есть, в 17% случаев EPSS как сигнал «на момент решения» просто отсутствовал.

Напоминалка: что такое EPSS и почему там 2 числа

- *epss — вероятность (0…1), что уязвимость будут эксплуатировать в ближайшие 30 дней. 0.01 = 1%*
- *percentile — «место в очереди« (0…1). Например, 0.94 означает: уязвимость «горячее», чем 94% CVE в этот день (то есть, она вТОП-6% по «эксплуатируемости»)*

Теперь практика: «сколько KEV вы поймаете порогами EPSS»

Если патчить только то, что выше порога, то среди реально эксплуатируемых (KEV) вы поймаете:

- 0.1% (EPSS ≥ 0.001): 132 из 203 (65%)
- 1% (EPSS ≥ 0.01): 78 из 203 (38%)
- 10% (EPSS ≥ 0.1): 55 из 203 (27%)

Но! Если EPSS используется в реальном процессе, отсутствие EPSS — это тоже означает «не поймал». Тогда фактический recall на полном наборе KEV ещё ниже:

- EPSS ≥ 0.001: 132 / 245 = 53.9%
- EPSS ≥ 0.01: 78 / 245 = 31.8%
- EPSS ≥ 0.1: 55 / 245 = 22.4%

Иными словами, даже там, где EPSS был, пороги ≥1% и ≥10% ловят лишь 38% и 27%.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

А на полном наборе KEV — 31.8% и 22.4%. Грусть-тоска-печаль.

Перевод на человеческий

(для тех, кто, как и я, прогуливал матан в школе)

Если вы используете EPSS как «проходной балл» и берёте только ≥1% — вы пропускаете примерно 68.2% того, что уже реально эксплуатируют. Так что EPSS — **отличный «ускоритель сортировки», но плохой «турникет на входе».**

Что это значит на практике

Плохой пример (или почему «низкий EPSS» не спасает):

«кровоточащая Монга» — CVE-2025-14847 / MongoBleed

- EPSS на дату добавления в KEV: 0.00041 (то есть 0.041%).
- Percentile: 0.122 (примерно «где-то внизу списка»).
- И при этом — KEV. То есть, эксплуатация подтверждена.

Вы же уже пропатчились? Пропатчились, верно?

Потому что вот вам главный урок: **низкий EPSS не означает «не эксплуатируют».**

Он может означать:

- эксплуатируют точечно;
- нишево;
- по internet-facing инсталляциям;
- с нетипичным шумом;
- без красивой массовой телеметрии, которую любит статистика.

Хороший пример (EPSS действительно помогает поднять приоритет):

React2Shell — CVE-2025-55182 (React Server Components RCE)

- EPSS на дату добавления в KEV: 0.13814 (13.8%).
- К 2025-12-29 вырос до 0.48714.

Вот здесь EPSS работает как задумано: **«Оно горячее, оно рядом, оно будет стрелять».**

Самый коварный класс: «сначала тихо, потом пожар»

Есть кейсы, где EPSS на дату добавления был почти ноль (<0.1%), а потом стал огромным:

- CVE-2025-0108: 0.00043 → 0.94007
- CVE-2025-30066 (tj-actions): 0.00036 → 0.87601

То есть, если вы в моменте смотрите и говорите: «0.04%? Ну, расслабились» — статистика может догнать уже после того, как рынок горит и пахнет жареным.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

А ещё хуже становится, когда мы выходим за пределы CVE вообще, и особенно когда смотрим на российские системы.

Например, уязвимости в TrueConf Server:

- BDU:2025-10116
- BDU:2025-10115
- BDU:2025-10114

А также пачки багов, найденные экспертами СайберОК:

- BDU:2025-13736
- BDU:2025-13737
- BDU:2025-13738

У них нет CVE → нет EPSS → нет магии. Видишь взломы? А они есть.

EPSS и патч-менеджмент: сколько реально придётся патчить (и сколько пальцев стереть об клавиатуру)

Окей, с KEV разобрались. Но давайте зададим более приземлённый вопрос: если поставить порог EPSS — сколько вообще придётся патчить ВСЕГО, а не только KEV? CISO живёт не в мире процентов, а в мире людей, часов и «когда мы это всё успеем».

Мы взяли все CVE-2025 и EPSS-снэпшот на 29 декабря 2025.

Всего уязвимостей: **37 907.**

Порог EPSS ≥ 0.1% (0.001)

- В патч-лист попадает: 8 663 уязвимости.
- Это 22.85% всех CVE-2025.

Трудозатраты:

- 15 минут на уязвимость → 2 166 часов (≈ 54 человеко-недели).
- 30 минут → 4 332 часа (≈ 108 человеко-недель).
- 60 минут → 8 663 часа (≈ 217 человеко-недель).

Получается уже не «спринт», а ксеноморфная многорукая форма жизни.

Порог EPSS ≥ 1% (0.01)

- В патч-лист попадает: 1 078 уязвимостей.
- Это 2.84% всех CVE-2025.

Трудозатраты:

- 15 минут → 270 часов (≈ 6.7 человеко-недель).
- 30 минут → 539 часов (≈ 13.5 человеко-недель).
- 60 минут → 1 078 часов (≈ 27 человеко-недель).

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Вот это уже похоже на реалистичную нагрузку для команды и именно поэтому этот порог так любят.

Порог EPSS ≥ 10% (0.1)

- В патч-лист попадает: 360 уязвимостей.
- Это всего 0.95% всех CVE-2025.

Трудозатраты:

- 15 минут → 90 часов (≈ 2.2 человеко-недели).
- 30 минут → 180 часов (≈ 4.5 человеко-недели).
- 60 минут → 360 часов (≈ 9 человеко-недель)

Очень комфортно, очень красиво в отчётах, но при этом вы пропускаете половину KEV. Как раз ту, которую «уже эксплуатируют».

Перевод на человеческий язык

- 0.1% EPSS — вы почти не пропускаете KEV, но платите за это сотнями человеко-недель.
- 1% EPSS — разумный компромисс по нагрузке, но вы сознательно принимаете риск пропустить часть реально эксплуатируемого.
- 10% EPSS — дешево, быстро, красиво… и крайне опасно, если использовать как единственный фильтр.

Понятно, что один патч может закрывать несколько уязвимостей, но для понимания масштаба бедствия этих цифр достаточно.

И вот тут вспоминаем MongoBleed:

CVE-2025-14847 / MongoBleed

EPSS = 0.00041:

- Не проходит ни один из этих порогов.
- Не попадает в «разумную» очередь.
- Зато прекрасно попадает под реальную эксплуатацию.

Финальный вывод

EPSS — это полезный сигнал для того, чтобы упорядочить хаос, когда патчить нужно много. Но верить только EPSS нельзя.

- KEV и сигналы от СайберОК — нужно безусловно чинить.
- EPSS — сортировать и фокусироваться.
- Порог EPSS = это всегда обмен риска на трудозатраты.
- А каждый дополнительный «процент EPSS» — это стертые об клавиатуру пальцы.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Магия заканчивается там, где начинается планирование ресурсов. К гадалке не ходи (а в нашу телегу заходи).

Для самых дотошных — репа с расчетами: https://github.com/scadastrangelove/kev_vs_epss.