КОД ИБ

ИТОГИ

ЧТО УСТРАНЯТЬ ИЛИ КАК НЕ УТОНУТЬ В УЯЗВИМОСТЯХ

ДМИТРИЙ ТОПОРКОВ
Начальник отдела контроля защищённости
АО Альфа-Банк

КОД ИБ

ИТОГИ

О себе

Дмитрий Топорков

- Начальник отдела контроля защищённости
- Спикер и автор курса по управлению уязвимостями на обучающей платформе Inseca

КОД ИБ

ИТОГИ

Почему мы “тонем” в уязвимостях?

- **С каждым годом регистрируется всё больше CVE**

Сканеры находят намного больше, чем раньше.

- **CVSS не помогает выбрать главное**

Высокий CVSS ≠ высокий риск.

- **Команды не понимают с чего начать**

Какие уязвимости устранять в первую очередь.
Backlog растёт быстрее, чем скорость исправления

КОД ИБ

ИТОГИ

Все ругают CVSS

- Не учитывает наличие эксплоита
- Не учитывает ценность актива
- Не учитывает контекст

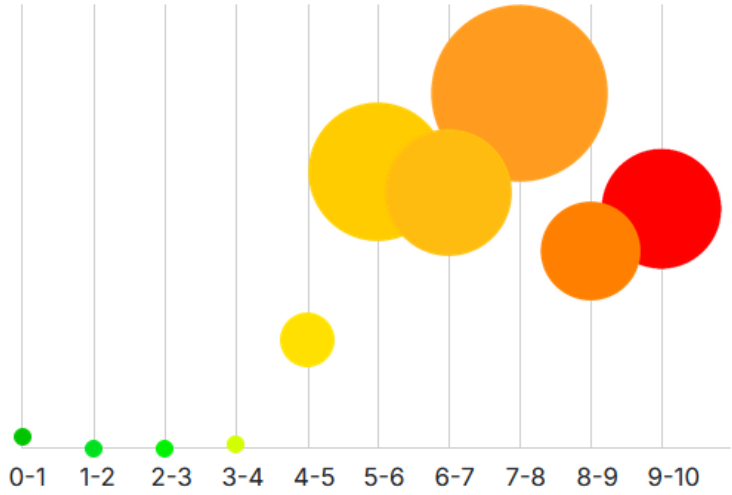
CVSS
COMMON VULNERABILITY SCORING SYSTEM

КОД ИБ

ИТОГИ

CVSS Score Range	Vulnerabilities
0-1	2117
1-2	49
2-3	656
3-4	1477
4-5	10105
5-6	25695
6-7	23849
7-8	33009
8-9	18390
9+	22302
Total	137649

Weighted Average CVSS Score: 7.5



Распределения критичности уязвимостей по CVSSv3.1 за 2022-2025 гг.

КОД ИБ

ИТОГИ

Какие альтернативы?

КОД ИБ

ИТОГИ

Синк по определениям

CISA KEV — это каталог известных эксплуатируемых уязвимостей (Known Exploited Vulnerabilities), который ведется Агентством по кибербезопасности и защите инфраструктуры (CISA).

EPSS (Exploit Prediction Scoring System) — это метрика, которая отражает вероятность того, что конкретная уязвимость будет проэксплуатирована.

КОД ИБ

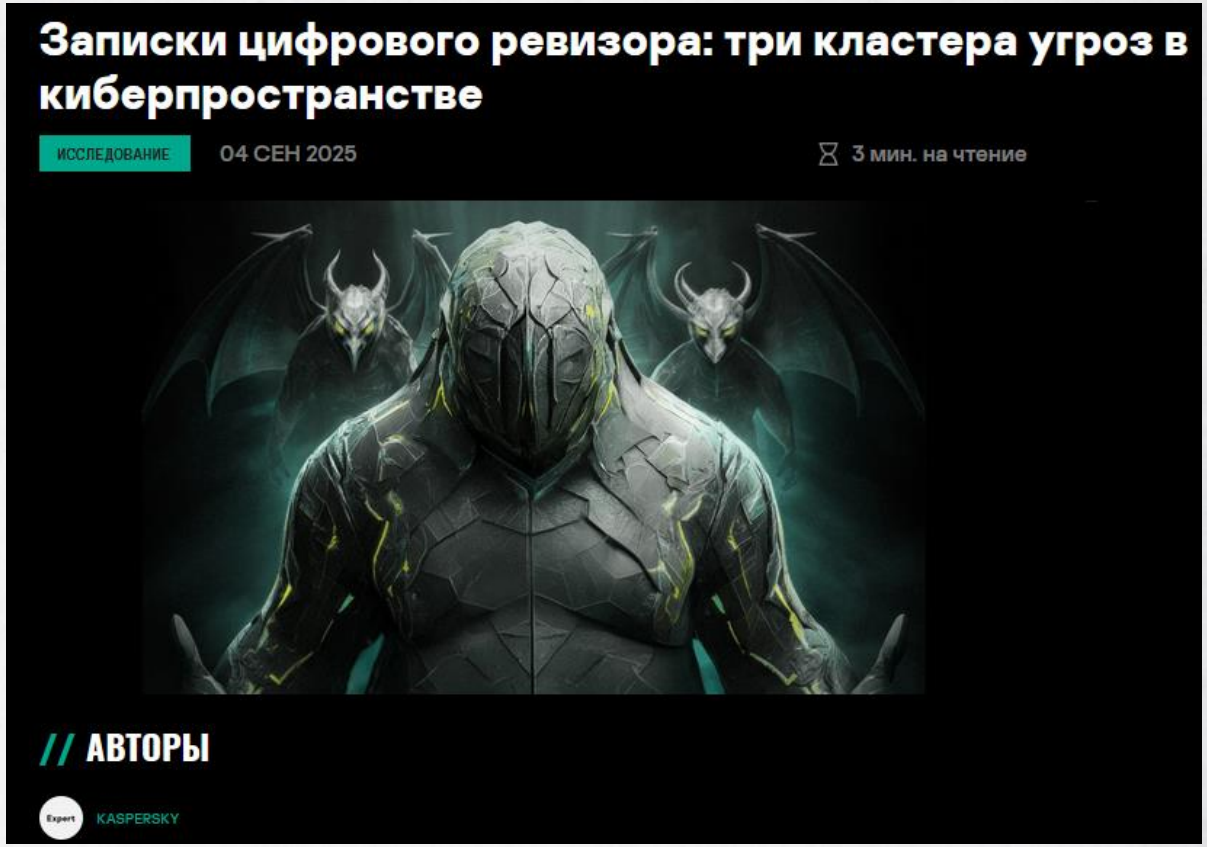
ИТОГИ

Что нам показывают практические кейс

В сентябре 2025 компания Kaspersky опубликовала исследования по актуальным киберугрозам для российских организаций.

В отчёте представлено:

- Какие техники используют злоумышленники;
- Какие используют инструменты;
- **Какие уязвимости эксплуатируют**



КОД ИБ

ИТОГИ

Эксплуатируемые уязвимости согласно

CVE ID	Вендор	Продукт	EPSS	CVSSv3	CISA KEV
BDU:2024-05252	1C	Bitrix	-	9,8	✗
CVE-2012-0158	Microsoft	MSCOMCTL.OCX	0,9431	8,8	✓
CVE-2017-11882	Microsoft	Office	0,9438	7,8	✓
CVE-2018-0802	Microsoft	Office	0,9410	7,8	✓

КОД ИБ

ИТОГИ

Эксплуатируемые уязвимости согласно

CVE ID	Вендор	Продукт	EPSS	CVSSv3	CISA KEV
CVE-2021-26855	Microsoft	Exchange Server	0,9435	9,1	✔
CVE-2021-26857	Microsoft	Exchange Server	0,3454	7,8	✔
CVE-2021-26858	Microsoft	Exchange Server	0,5506	7,8	✔
CVE-2021-27065	Microsoft	Exchange Server	0,9430	7,8	✔
CVE-2021					

КОД ИБ

ИТОГИ

Какие сохраняются тенденции?

- Атакующие эксплуатируют старые уязвимости, которым >1 года
- Большая часть уязвимостей **находятся в CISA KEV**
- Имеют высокий EPSS

КОД ИБ

ИТОГИ

Динамика CISA KEV

КОД ИБ

ИТОГИ

Недостатки CISA KEV

- Показывает факт эксплуатации, но не предупреждает заранее не
- Есть лаг между выявлением эксплуатации и добавлением в список
- Неприменимо для отечественного ПО

КОД ИБ

ИТОГИ

Не знаете с чего начать?

- Соберите список всех обнаруженных уязвимостей в вашей инфраструктуре
- При необходимости обогатите данными по CISA KEV
- Сфокусируйте ресурсы на устранении этих уязвимостей
- Не забывайте следить за **трендовыми** уязвимостями для проактивного реагирования.

КОД ИБ

ИТОГИ

СПАСИБО ЗА ВНИМАНИЕ!