CII Cyber Identity Index

F6

Индекс кибербезопасности

Индекс зрелости вашей цифровой защиты

New Новый сервис от F6

Индекс — это не просто цифра

Это аналитическая модель, которая позволяет выявлять закономерности, а не только фиксировать отдельные проблемы.

В отличие от обычных проверок, которые дают список уязвимостей, индекс рассматривает цифровой периметр как систему: находит повторяющиеся риски, связывает их с типом инфраструктуры и отраслью.

Это даёт бизнесу не только картину текущего состояния, но и отправную точку для изменений. Индекс помогает понять, что именно требует внимания, где начинаются системные сбои и как они связаны между собой.

Он не заменяет внутренние аудиты или сканеры уязвимостей — он дополняет их стратегическим взглядом.

Это не технический отчёт, а инструмент для принятия решений: с акцентом на приоритеты, повторяющиеся риски и реальные точки контроля.

Миссия

Наша цель — сформировать культуру зрелого и осознанного управления цифровыми рисками как части корпоративной стратегии.

Индекс помогает компаниям понять, где они уязвимы, сравнить себя с рынком и наметить вектор развития.

Это не просто метрика, а инструмент, который запускает стратегический диалог между бизнесом и ИБ и помогает выстраивать системную работу с киберугрозами.

Из чего состоит Индекс

F6 Cyber Identity Index состоит из глубокой работы аналитиков. Персонализированная оценка основана на трех компонентах:

1 / 3

Детальный анализ компании в рамках индустрии

Оцениваем компанию с учётом её размера, отрасли, географии и типовых угроз в сегменте.

2 / 3

Индивидуальный опросник

Аналитик обрабатывает данные и фиксирует архитектуру, зрелость процессов, бизнес-приоритеты.

3 / 3

Технические данные ASM

Автоматизированный анализ внешней поверхности атаки: IP-адреса, субдомены, открытые порты, протоколы, уязвимости.

Зачем нужен опросник?

Почему без него нельзя

Техническая оценка — это база. Но только опрос позволяет специалистам F6 учесть нюансы именно вашей компании:

- распределение зон ответственности
- контекст бизнес-модели
- зрелость ИБ-процессов
- скрытые векторы риска

Ответы проходят ручной анализ: подбираются индивидуальные веса, добавляются подкатегории, корректируется логика расчёта.

Результат — не усреднённая формула, а персонализированная карта рисков.

Что оценивается — 8 категорий

Графическая паутинка показывает зрелость по восьми направлениям:

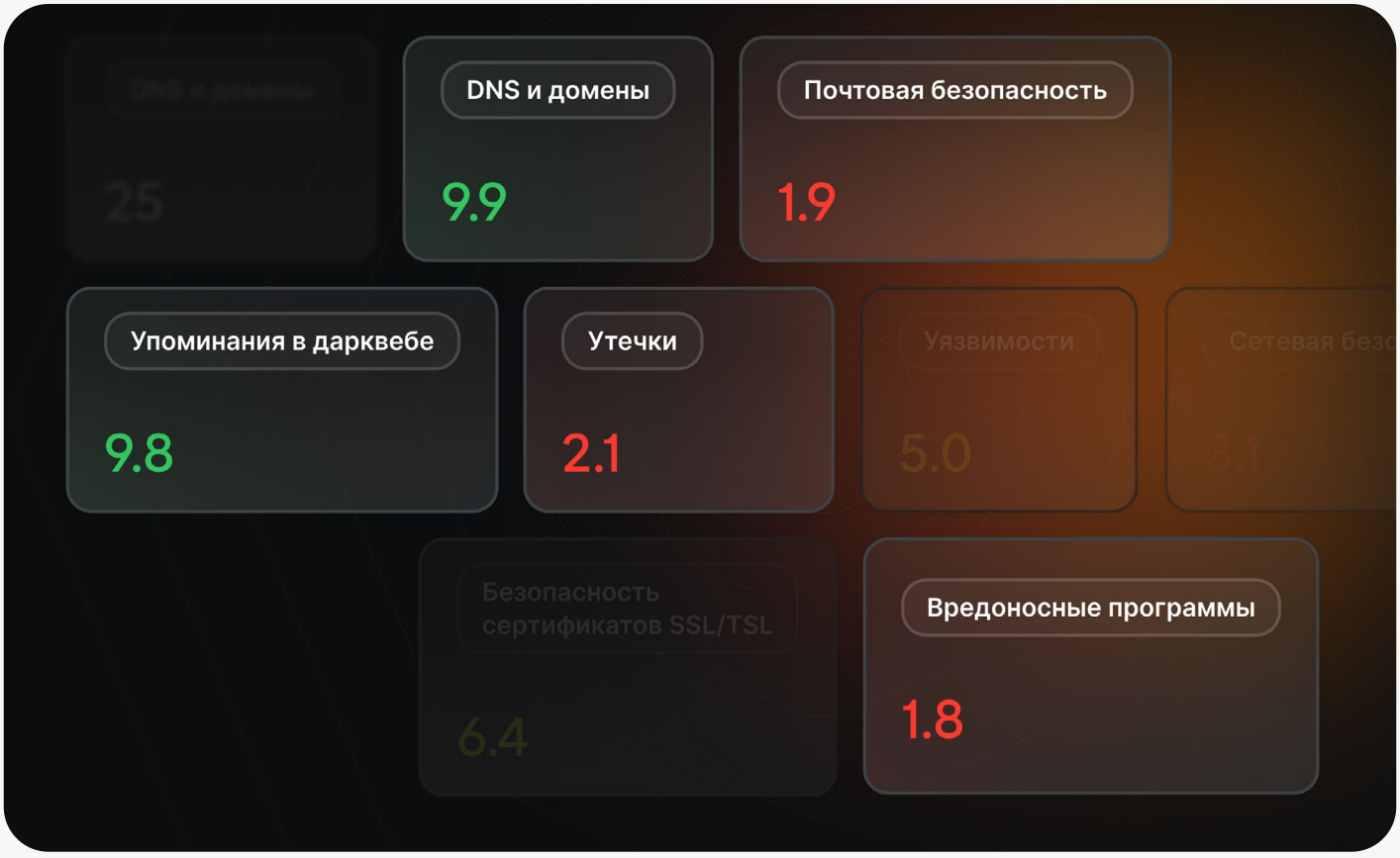
- Уязвимости ОС и ПО
- Сетевая безопасность
- Утечки данных
- Вредоносные программы
- Почтовая безопасность
- SSL/TLS-конфигурация
- DNS и домены
- Упоминания в даркнете

Каждая категория — это реальный вектор атаки.

Каждая метрика — с учётом значимости именно вашей инфраструктуры.

Каждая категория отражает вектор атаки на внешний периметр.

Внутри — конкретные параметры, подкатегории и весовой коэффициент, который учитывает их значимость при расчёте Индекса.



Как формируется техническая оценка

Система формирует целостное представление о внешнем цифровом периметре компании — включая активные IP, субдомены, порты, конфигурации, цифровые следы в даркнете и признаки вредоносной активности.

Сканирование внешнего периметра

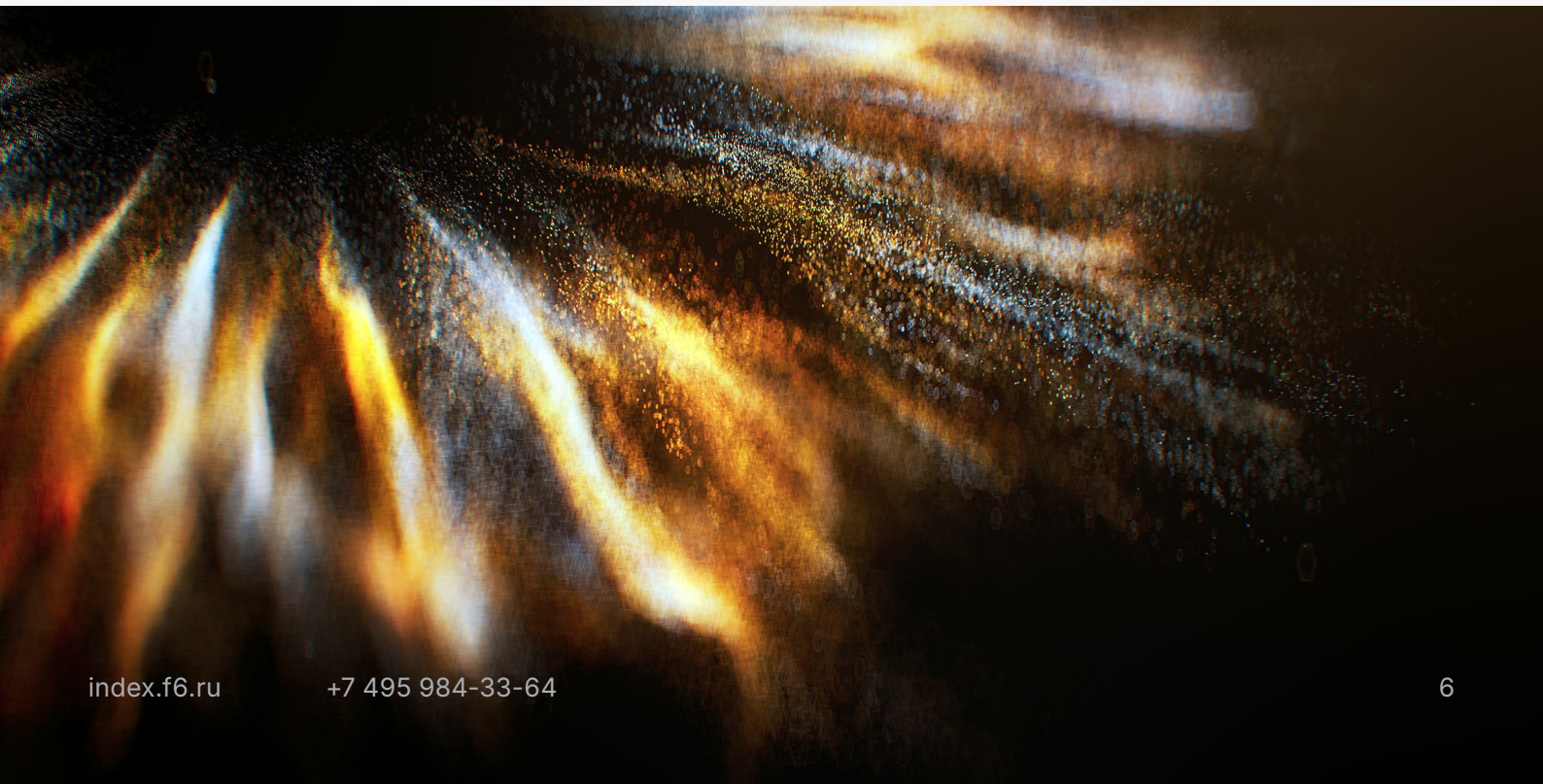
Выявление активных IP, субдоменов и портов

Проверка сертификатов и конфигураций

Сопоставление с базами CVE

Детект активностей вредоносного ПО

Проверка публичных и даркнет-источников на утечки и упоминания



Почему это важно бизнесу

Формирование осознанного подхода к защите от киберугроз

С помощью индекса мы закладываем основу для культуры зрелого и осознанного управления цифровыми рисками как части корпоративной стратегии

Обоснование решений

Конкретные цифры для аргументации. Индекс предоставляет измеримые данные, которые можно использовать при планировании бюджета, цифровой трансформации и управлении рисками.

Общий язык для бизнеса и ИБ

Ясный, понятный бизнесу формат. Индекс становится новой точкой входа в диалог между ИБ и C-level: зрелость информационной безопасности представлена в понятной и ценной для бизнеса форме.

Сигнал рынку

Прозрачность и доверие. Участие в Индексе усиливает доверие со стороны клиентов, партнёров и инвесторов, демонстрируя системный подход к ИБ.

Дорожная карта развития

Приоритеты и ориентиры. Отчёт содержит приоритизированные рекомендации, бенчмаркинг и векторы роста по ключевым аспектам цифровой безопасности.

Требования ужесточаются — ответственность растет

Федеральный закон № 420-ФЗ и приказ ФСТЭК № 117 вводят жёсткие правила игры: штрафы, уголовная ответственность, обязательные регламенты и отчётность. **Защита становится не просто внутренним вопросом — это зона контроля государства с реальными рисками.** Индекс помогает выявлять уязвимости до того, как ими заинтересуются проверяющие.

Как проходит процесс

1 / 5

Компания подаёт заявку: указывается корпоративный почтовый домен

2 / 5

Система ASM запускает анализ, выявляя связанную цифровую инфраструктуру

3 / 5

Аудитор присылает индивидуальный опросник для уточнения архитектуры

4 / 5

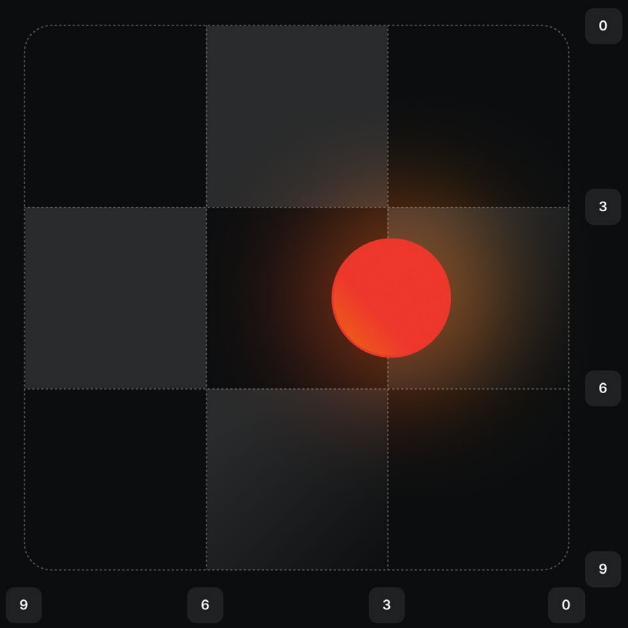
После сбора данных проводится расчёт по восьми категориям

5 / 5

Вы получаете результат:

- баллы по каждой категории
- визуальную «паутинку»
- карту проблем и приоритетов
- сравнение с рынком

Карта проблем:



CII Cyber Identity Index

Индекс F6 — ваш первый шаг к стратегическому управлению цифровыми рисками

Проверьте открытые уязвимости, получите персонализированную карту рисков и покажите рынку: у вас — системный подход и долгосрочная стратегия в кибербезопасности.

Узнать больше

index.f6.ru

+7 495 984-33-64