F6

Индекс кибербезопасности

Аналитический отчет

Результаты внешнего сканирования

Оглавление

Общая картина

Компания прошла внешний анализ защищённости в рамках Индекса кибербезопасности F6. Цель исследования — получить независимую оценку уровня цифровой устойчивости, определить ключевые риски и понять, насколько действующая стратегия безопасности поддерживает цели бизнеса.

Результаты показали разную степень зрелости внутри и за пределами инфраструктуры. Внутренние процессы выстроены последовательно: функционируют SOC и EDR-системы, действует патч-менеджмент, регламентированы сценарии реагирования на инциденты. Команда умеет выявлять угрозы и устранять последствия — это создаёт надёжный фундамент.

Внешний контур при этом остаётся зоной повышенного внимания. Анализ выявил уязвимости в программном обеспечении, ошибки конфигураций и использование устаревших протоколов. Кроме того, часть подключений подрядчиков осуществляется вне корпоративного контроля, что расширяет возможную поверхность атаки.

Вывод

Компания демонстрирует высокий уровень организованности и зрелости внутри периметра, но для перехода к категории высокой устойчивости необходимо системно управлять внешними активами, актуализировать программное обеспечение и контролировать использование корпоративных учётных записей за пределами инфраструктуры.

Проведённая оценка является частью 360-анализа — методологии, позволяющей рассматривать безопасность не как отдельный ИТ-функционал, а как элемент управляемости компании. Такой подход помогает видеть не только технические уязвимости, но и организационные взаимосвязи: насколько процессы между ИТ, безопасностью и бизнес-подразделениями согласованы, где есть зависимости от человеческого фактора и насколько культура защиты встроена в повседневную работу.

Цифровая витрина компании

В рамках анализа была зафиксирована структура цифровых активов, доступных в открытом интернете:

- домены и поддомены, включая тестовые и внутренние сервисы;
- публичные IP-адреса и веб-интерфейсы;
- SSL/TLS-сертификаты и их конфигурации;
- используемое серверное и клиентское ПО;
- внешние компоненты подрядчиков и сторонних платформ.

Часть активов функционирует без централизованного контроля:

- выявлены сервисы, работающие на устаревших версиях PHP, Nginx и jQuery, для которых существуют готовые эксплойты;
- несколько сертификатов близки к истечению, часть ресурсов использует устаревшие протоколы, что вызывает предупреждения о небезопасном соединении у пользователей;
- обнаружены ошибки в DNS-конфигурации и отсутствие DNSSEC, повышающие риск подмены ответов и отказов в обслуживании;
- отдельные активы размещены на площадках подрядчиков и в зарубежных юрисдикциях, где требования к комплаенсу различаются. Это требует дополнительного контроля SLA и защиты данных.

Вывод

Цифровая витрина компании сформирована, но избыточная открытость и отсутствие централизованного управления активами увеличивают поверхность атаки. Для устойчивости бизнеса необходимо внедрить постоянный мониторинг внешних ресурсов, актуализировать версии ПО и сертификаты, а также назначить ответственных за каждый актив.

Подробный разбор

по категориям

Анализ проведён по восьми направлениям Индекса F6. Баллы отражают зрелость защиты в каждом из них.

Уязвимости

0 / 10

На внешнем периметре выявлены критические CVE в Nginx, PHP и jQuery. Устаревшие версии позволяют выполнять произвольный код и развивать атаку без значительных ресурсов.

Утечки данных

7 / 10

В открытых источниках найдены корпоративные учётные записи сотрудников. Признаков компрометации нет, но повышен риск фишинга и повторного использования паролей.

Вредоносная активность

10 / 10

Следов заражения инфраструктуры и связанных с компанией вредоносных доменов не выявлено.

Сетевая безопасность

9 / 10

Периметр сегментирован, внешние соединения фильтруются. Критичных открытых портов нет.

SSL/TLS

8 / 10

Конфигурации в целом корректны, но часть сертификатов близка к истечению и применяются устаревшие протоколы. Рекомендуется переход на TLS 1.3 и централизованный контроль сроков.

Почтовая безопасность

8 / 10

Проверки SPF, DKIM и DMARC пройдены успешно. Конфигурация защищает от подмены и несанкционированной рассылки.

DNS и домены

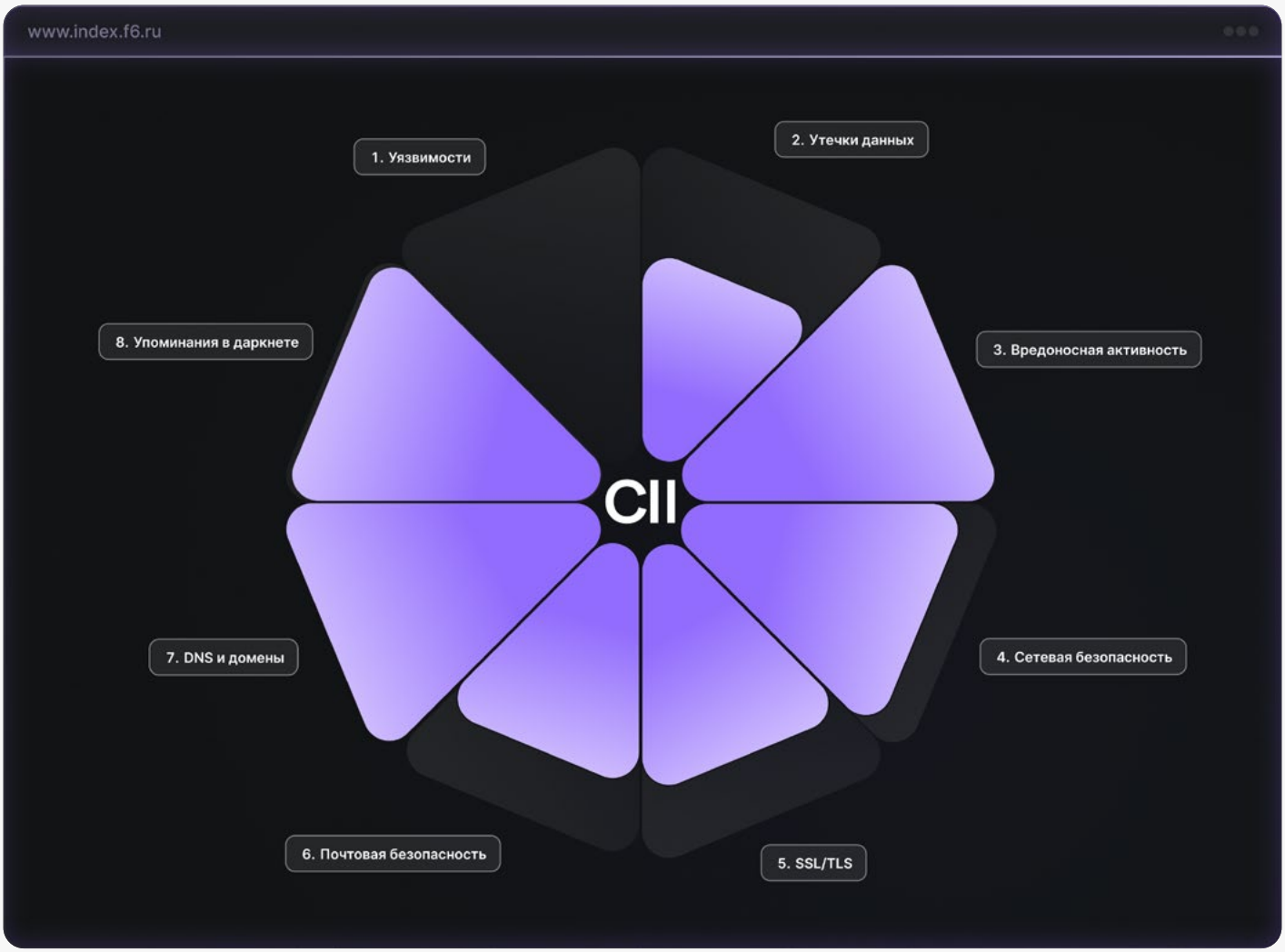
Отмечено отсутствие DNSSEC и устаревшие SOA-записи. Возможна подмена DNS-ответов и снижение устойчивости при DDoS.

9 / 10

Упоминания в даркнете

Критичных упоминаний или обсуждений инфраструктуры не обнаружено.

10 / 10



Вывод

Основные риски сосредоточены в области уязвимого программного обеспечения и утечек учётных записей. Остальные направления демонстрируют устойчивое состояние. Для перехода к уровню высокой зрелости необходимо выстроить системный контроль внешнего периметра и обновление программных компонентов.

Технический отчёт

Карта уязвимостей

Уязвимость	Описание	Риск для бизнеса
Устаревшее ПО	На ряде внешних ресурсов установлены версии PHP, Nginx и jQuery с критическими CVE.	Возможность захвата инфраструктуры и выполнения произвольных команд.
Открытые формы входа	На некоторых ресурсах отсутствует ограничение числа неудачных попыток авторизации.	Возможен перебор паролей с использованием данных из утечек.
Расширенная поверхность атаки	Десятки поддоменов, включая тестовые и dev-среды, остаются без закреплённых владельцев.	Возможна компрометация через забытые сервисы.
Учётные записи в утечках	В публичных базах обнаружены корпоративные e-mail сотрудников.	Риск фишинговых атак и компрометации при повторном использовании паролей.
SSL/TLS с устаревшими протоколами	На отдельных ресурсах используются TLS 1.0 / 1.1 и сертификаты с истекающим сроком.	Предупреждения о небезопасном соединении, риск перехвата трафика.
Ошибки DNS-конфигурации	Отсутствует DNSSEC, устаревшие SOA-записи, часть IP сгруппирована в одной подсети.	Возможна подмена ответов и снижение устойчивости при DDoS.

Вывод

Сочетание утечек, устаревшего ПО и неучтённых активов создаёт взаимосвязанную цепочку атаки. Используя утёкшие данные и открытые формы входа, злоумышленники могут проникнуть в инфраструктуру через уязвимые сервисы.

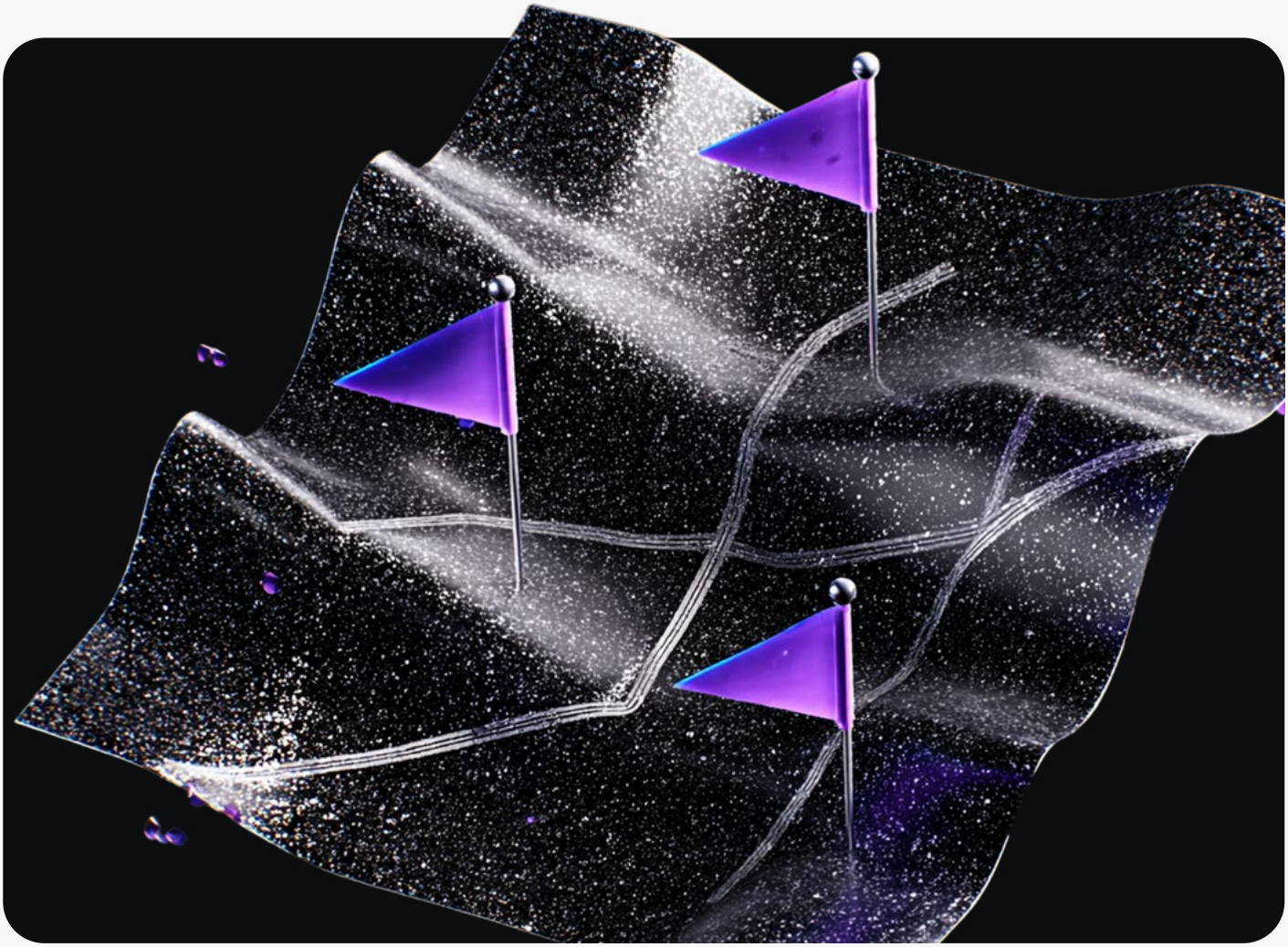
Позиционирование на матрице зрелости

По итогам анализа компания получила **68 баллов из 100**, что соответствует уровню BB — **«ИБ-энтузиасты»** по классификации Индекса F6.

Это уровень осознанного управления безопасностью: внедрены ключевые технологии и процессы, действует SOC, реагирование и патч-менеджмент организованы. При этом внешний контур требует перехода к непрерывному управлению — регулярному мониторингу, обновлениям и контролю подрядчиков.

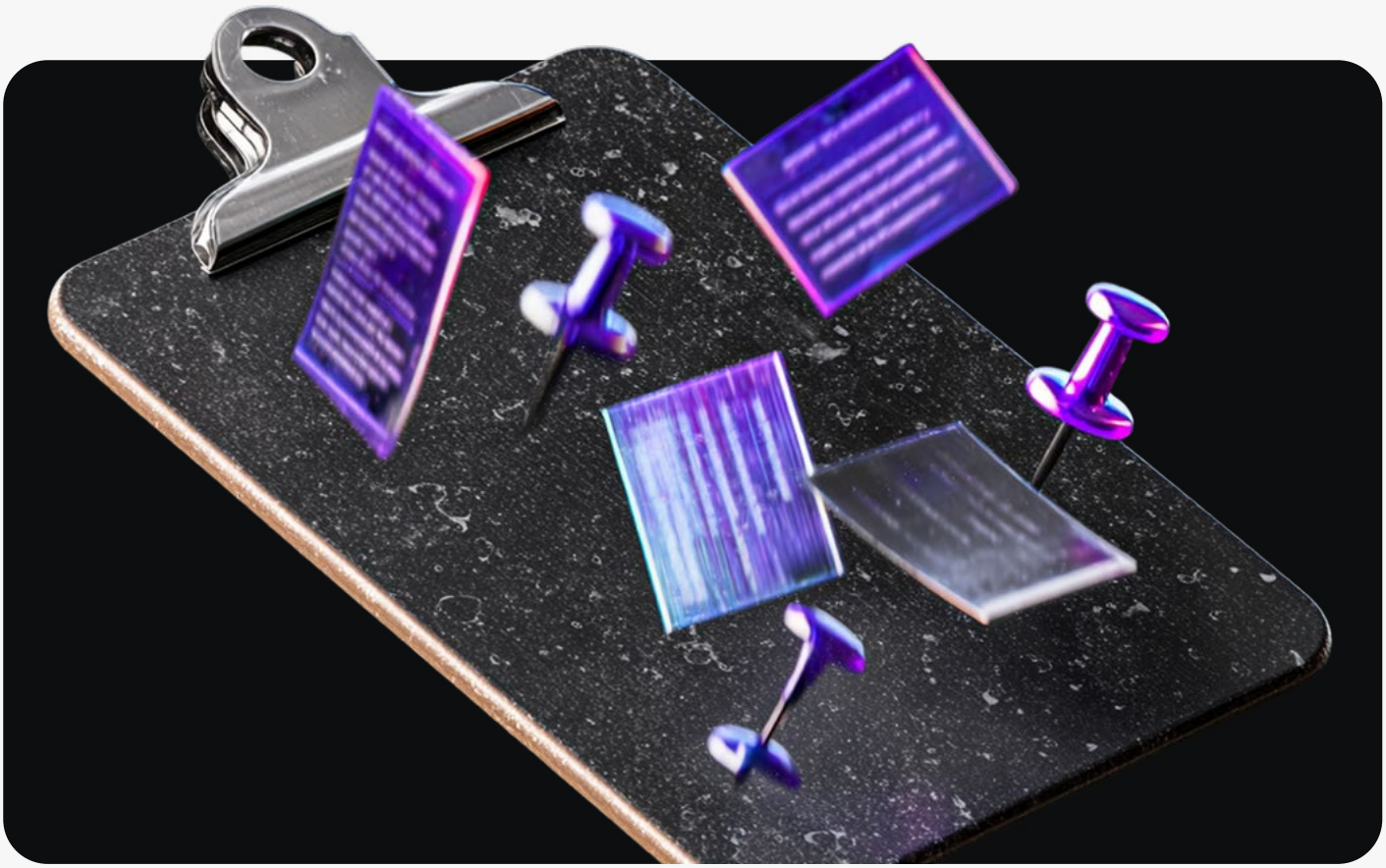
Вывод

Это уровень осознанного управления безопасностью: внедрены ключевые технологии и процессы, действует SOC, реагирование и патч-менеджмент организованы. При этом внешний контур требует перехода к непрерывному управлению — регулярному мониторингу, обновлениям и контролю подрядчиков.



Ключевые зоны риска

Зона риска	Описание	Риск для бизнеса
Расширенная поверхность атаки	Большое количество поддоменов, включая тестовые и CRM-сервисы, без закреплённых владельцев.	Потеря контроля, возможность разведки и эксплуатации забытых сервисов.
Устаревшее ПО	Внешние серверы работают на версиях с известными уязвимостями.	Возможность удалённого выполнения кода и компрометации сервисов.
Учётные записи в утечках	В открытых источниках обнаружены корпоративные e-mail.	Риск целевого фишинга и атак через повтор паролей.
Ошибки SSL/TLS	Используются устаревшие протоколы, сертификаты близки к истечению.	Предупреждения о небезопасном соединении, риск перехвата трафика.
DNS без DNSSEC	Устаревшие SOA-записи и сгруппированные IP-адреса.	Возможна подмена ответов и снижение устойчивости к DDoS.
Аутсорс и подрядчики	Использование личных устройств вне корпоративного контроля.	Потенциальная точка входа при компрометации подрядчика.



Актуальные группировки и схемы мошенничества

В ходе анализа учтены актуальные схемы атак и деятельность активных кибергруппировок, действующих в 2025 году.

Наиболее вероятные акторы:

- FIN7 (Carbanak), TA505 — фишинг, компрометация переписки, атаки на финансовые операции;
- LockBit, Play, Clop — ransomware-операторы, использующие уязвимости и доступы подрядчиков;
- APT41, Lazarus, Cloud Atlas — целенаправленные атаки на инфраструктуру и цепочки поставок;
- IT Army of Ukraine, Killnet — DDoS и дефейс публичных ресурсов.

Типичные схемы атак:

- регистрация доменов-двойников и фишинговые рассылки;
- компрометация почтовых цепочек и подмена реквизитов;
- использование утёкших паролей (password spray, credential stuffing);
- атаки через подрядчиков и внешние платформы;
- вредоносные обновления и заражённая реклама.

Эти сценарии напрямую связаны с выявленными уязвимостями. Для бизнеса это означает необходимость перехода к проактивной модели: мониторинг внешних событий, контроль подрядчиков и постоянное обновление контуров защиты.

Позитивные аспекты и текущая защита

Компания демонстрирует зрелую внутреннюю систему безопасности.

Ключевые сильные стороны:

- функционирует SOC и установлены EDR-агенты;
- сеть сегментирована, реализованы фильтры соединений;
- действует патч-менеджмент и отлажено реагирование на инциденты;
- проводится обучение сотрудников и контроль цифровой гигиены;
- определены регламенты и зоны ответственности.

Вывод

Внутренняя защита компании сбалансирована и управляемая. Это подтверждает стратегически правильный курс — безопасность встроена в операционную деятельность, а процессы ориентированы на предотвращение, а не на реакцию.

Action-план и рекомендации

Направление	Рекомендация	Приоритет	Срок
Управление активами	Провести инвентаризацию доменов, поддоменов и внешних IP. Назначить ответственных за каждый ресурс.	Высокий	1 мес
Устаревшее ПО	Обновить версии PHP, Nginx, jQuery и другие компоненты с критическими CVE.	Высокий	1 мес
SSL/TLS	Перейти на TLS 1.3, обновить сертификаты, внедрить централизованный контроль сроков.	Средний	2 мес
DNS-защита	Включить DNSSEC, актуализировать SOA-записи, распределить IP по подсетям.	Средний	2 мес
Учётные записи	Проверить корпоративные почты, внедрить MFA и контроль слабых паролей.	Высокий	1 мес
Контроль подрядчиков	Проверить использование личных устройств, включить требования по ИБ в контракты и SLA.	Средний	3 мес
Мониторинг внешней поверхности	Настроить регулярное сканирование периметра и централизованный учёт уязвимостей.	Средний	2-3 мес
Аудит соответствия	Провести аудит по 152-ФЗ, 187-ФЗ и приказу ФСТЭК № 117.	Средний	3 мес
Тестирование готовности	Провести Red Teaming и анализ защищённости инфраструктуры и приложений.	Средний	4 мес

Вывод

Предложенный план переводит безопасность из разовых действий в управляемый процесс. Реализация мер позволит компании перейти на уровень зрелости A, повысить прозрачность управления и сократить издержки, связанные с инцидентами.

Как повысить уровень зрелости

Следующий шаг — закрепить достигнутый уровень внутренней защиты и устранить внешние риски.

Рекомендуется использовать решения F6, усиливающие мониторинг, управление активами и анализ угроз:

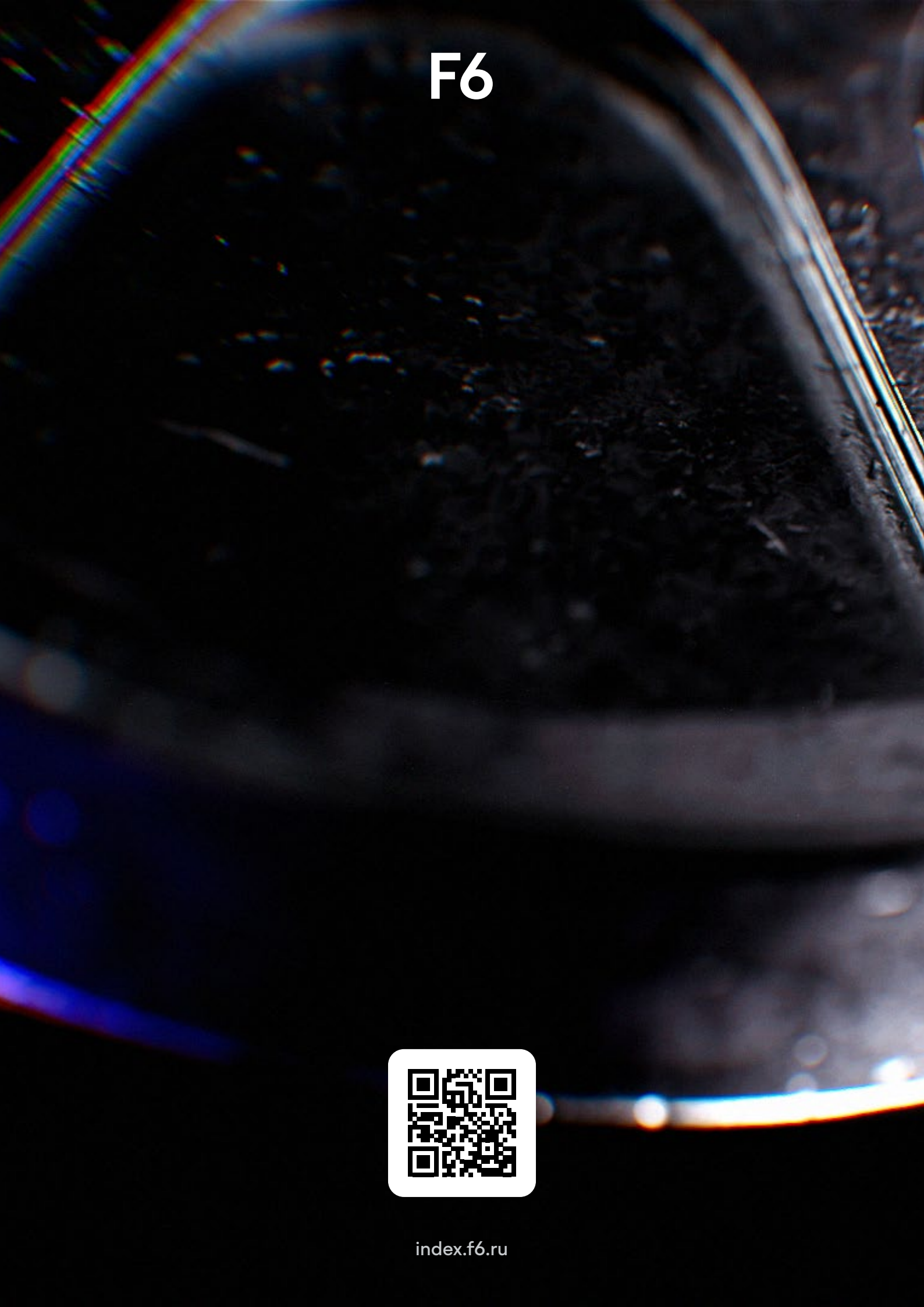
Решение	Для чего	Больше информации
F6 Attack Surface Management	Постоянный контроль внешних активов и сокращение поверхности атаки	
F6 Digital Risk Protection	Защита бренда и подрядчиков от фишинга и утечек	
F6 Threat Intelligence	Получение контекста атак и приоритетов реагирования.	

Повторная оценка Индекса через 3–6 месяцев позволит зафиксировать прогресс, подтвердить рост зрелости и показать, как принятые меры влияют на общую устойчивость компании.

Заключение

Оценка показала: у компании уже сформированы ключевые элементы защиты и понимание роли информационной безопасности. Следующий этап — развитие управленческой зрелости, когда безопасность становится не отдельным направлением, а частью стратегического цикла управления.

Формат 360-оценки F6 позволяет видеть киберриски в контексте бизнеса: где слабые места действительно угрожают операционной устойчивости, какие процессы работают, а какие требуют перестройки. Это даёт руководству возможность выстраивать стратегию не вслепую, а на основе данных, превращая безопасность в инструмент развития компании.


F6
index.f6.ru