Пример отчёта

AI-пентест внешнего периметра

СнабКонтур

Маркетплейс B2B-закупок
snabkontur.example

Business

Три технические уязвимости и три юридических риска. Доказательства, последствия для бизнеса и рекомендации по устранению.

1 домен	7 ч 02 м	2
для начала проверки	до первого уведомления	технических риска открыты

Проверка: 19-24 октября 2026
Повторная проверка: 25 октября 2026
Юрисдикция заказчика: Россия

Компания и результаты вымышлены. Пример показывает, что получает заказчик по итогам проверки.

Два пути к данным остаются открытыми

На 25 октября коммерческие выгрузки доступны по прямой ссылке, а кэш документов выдаёт файл без проверки подписи.

1 High	1 Medium	1 закрыт
выгрузки с условиями поставщиков	закрытые документы в кэше	доступ к служебному журналу

F01

Коммерческие условия могут попасть наружу

Публичная сборка раскрыла адрес индекса выгрузок. Индекс дал прямую ссылку на CSV с поставщиками и индивидуальными ценами. Источник ссылки скрыт, сам файл пока доступен.

F02

Подпись защищает документ только до попадания в кэш

После законного открытия PDF сервер отдаёт его по тому же пути без подписи. В PDF указаны условия заказа, имя, email и телефон представителя покупателя.

F03

Защитный шлюз можно было обойти

По IP тестового стенда открывался служебный журнал основного сайта. Заказчик ограничил доступ; повторная проверка подтвердила исправление.

Также найдены три юридические проблемы: недоступная политика, объединённые согласия и риск раскрытия персональных данных. План устранения - на страницах 10-11. Оценка финансовых последствий одного инцидента - 376 000 ₽, расчёт на странице 12.

От главной страницы к коммерческой выгрузке

Исходная позиция: посетитель знает только домен. Учётной записи, доступа к коду и списка внутренних адресов у него нет.

01

Публичный JavaScript

Главная загружает app.72c9.js. В конце файла есть sourceMappingURL: app.72c9.js.map. Это обычная ссылка в ответе сайта.

02

Карта исходников

В sourcesContent обнаружен exportIndexUrl с полным адресом /legacy/exports/6d5b2e4f/manifest.json. Случайный сегмент получен из сборки; перебор не требуется.

03

Индекс выгрузок

Индекс возвращает имя CSV со случайным идентификатором. Теперь известен полный путь к конкретной выгрузке поставщиков.

04

Данные без входа

GET с Range: bytes=0-511 возвращает 206 и начало CSV с индивидуальными ценами. Этого достаточно, чтобы подтвердить доступ; чтение остановлено.

Каждый ответ раскрывает адрес следующего запроса. Удалить карту исходников недостаточно: по уже известной ссылке файл по-прежнему можно скачать. Нужна проверка прав доступа к самой выгрузке.

Как проходила проверка

Заказчик передал домен snabkontur.example, подтвердил владение и разрешил тестирование. Агенты работали из интернета, без аккаунтов и подключения к внутренней сети.

14
обнаруженных доменных имён

5
проверенных веб-узлов

12 640
HTTP-запросов в журнале

Что проверили

Основной сайт и **api**: формы, согласия и файлы приложения. **files**: документы и кэш. **stage**: общий сервер и служебные страницы. **status**: страница состояния, значимых находок нет.

Из 14 адресов отвечали 9. Четыре сервиса сторонних провайдеров исключены из активных тестов. Новые адреса проверяли только в согласованных границах.

Разведка	Связал DNS, сертификаты, ссылки и обнаруженные веб-узлы.
Контекст приложения	Прошёл калькулятор, изучил JavaScript и связанные файлы.
Проверка гипотез	Сравнил подписанные и неподписанные запросы, кэш и origin.
Подготовка отчёта	Собрал доказательства, убрал повторы и описал находки.

Специалист подтвердил три технические находки и отправил срочное уведомление. Также проверены публичные формы и документы на юридические риски. Первый результат заказчик получил через 7 ч 02 м.

Нагрузка: до 2 запросов в секунду суммарно. Запросы помечены User-Agent CyberYozh-Audit/1.0. По сообщению заказчика тестирование останавливается.

F01 · Высокий риск · CVSS 7.5

Частично исправлено

Выгрузка цен доступна без входа

Обнаружено 19.10, 16:40 МСК. Уведомление 17:02 МСК, через 22 минуты. Входная точка и полный путь получены цепочкой на странице 3.

```
GET /legacy/exports/6d5b2e4f/manifest.json HTTP/1.1
Host: snabkontur.example
User-Agent: CyberYozh-Audit/1.0

HTTP/1.1 200 OK
Date: Mon, 19 Oct 2026 13:39:48 GMT
Content-Type: application/json
X-Request-ID: 831b01fbda344c579116c7347b1b4ea2

{"file":"suppliers-20261018-a81f52.csv"}

GET /legacy/exports/6d5b2e4f/suppliers-20261018-a81f52.csv HTTP/1.1
Host: snabkontur.example
Range: bytes=0-511

HTTP/1.1 206 Partial Content
Date: Mon, 19 Oct 2026 13:40:12 GMT
Content-Type: text/csv; charset=utf-8
Content-Range: bytes 0-511/18472
X-Request-ID: 0eb60ad8a45046a2ab5f0f86380dddb5

supplier_id,sku,net_price,discount_pct
SUP-018,VALVE-50,14800,17
```

Последствия

Посторонний может прочитать индивидуальные цены и скидки поставщиков. Все адреса получены с публичного сайта, вход не требуется. Проверка подтвердила чтение данных; изменение файлов и остановка сервиса не проверялись.

Что исправить разработчикам и администраторам

Убрать экспорт из публичного каталога, проверять права на каждый файл, закрыть старые URL и сбросить кэш. При повторной проверке карта исходников уже была закрыта, а старая ссылка на CSV по-прежнему возвращала 206.

CVSS 3.1: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CWE-552 / доступные извне файлы

F02 · Средний риск · CVSS 6.5 Открыто

Кэш выдаёт PDF без подписи

Обнаружено 20.10, 16:15 МСК. Проверены два документа из публичного калькулятора на тестовых данных CY-TEST. Личный кабинет не использовался.

Калькулятор выдаёт ссылку с exp и sig. После её открытия другой клиент без cookies получает тот же PDF без этих параметров. Пока файла нет в кэше, такой запрос возвращает 403.

```
GET /quotes/2026/10/20/000184.pdf HTTP/1.1
Host: files.snabkontur.example
User-Agent: CyberYozh-Audit/1.0

HTTP/1.1 200 OK
Date: Tue, 20 Oct 2026 13:15:09 GMT
Content-Type: application/pdf
Cache-Control: public, max-age=3600
Age: 41
X-Cache: HIT
X-Request-ID: 9a4097fe04194679b9791d69cf7b672e

%PDF-1.7
```

Контроль: до прогрева тот же неподписанный запрос получал 403 / MISS. После прогрева хэш тела совпал с подписанным ответом. Различались только параметры подписи; cookies не передавались.

Какие данные раскрываются

PDF содержит ФИО, рабочие email и телефон контактного лица, условия заказа. Файл должен быть ранее открыт владельцем, что учтено в оценке UI:R. Последовательные номера видны в тестовых PDF; чужие документы не перебирались.

Что исправить DevOps

Отключить общий кэш для закрытых PDF, проверить подпись до любого cache HIT и очистить старые объекты. Повторить тесты с отсутствующей, неверной и просроченной подписью.

CVSS 3.1: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

CWE-524 / чувствительная информация в кэше

F03 · Средний риск · CVSS 5.3

Исправлено

Служебный журнал открыт по прямому IP

Обнаружено 21.10, 12:10 МСК. DNS тестового стенда раскрыл IP общего сервера: 203.0.113.42. Проверка выполнена с SNI и Host основного домена.

Через штатный защитный шлюз маршрут /ops/jobs закрыт. При обращении к тому же сайту по прямому IP сервер отдавал служебный журнал: названия задач, внутренние пути и состояние синхронизации.

IP 203.0.113.42 / TLS SNI: snabkontur.example

```
GET /ops/jobs?limit=1 HTTP/1.1
Host: snabkontur.example
User-Agent: CyberYozh-Audit/1.0

HTTP/1.1 200 OK
Date: Wed, 21 Oct 2026 09:10:32 GMT
Content-Type: application/json
X-Request-ID: 2c96579c79bd46da8a8221062be2de17

{"jobs":[{"name":"orders-sync","state":"failed",
"path":"/srv/app/exports","lastRun":"2026-10-21T09:07:10Z"}]}
```

Сравнение: по штатному DNS тот же запрос получил 403. По прямому IP открылся журнал с параметрами задач. Подтверждено чтение служебных сведений; возможности управления сервером не обнаружены.

Что исправить администраторам

Принимать запросы к основному серверу только с адресов защитного шлюза. Разделить тестовый стенд и основной сайт. Дополнительно закрыть /ops в самом приложении.

Повторная проверка: 25.10, 11:20 МСК

Прямой запрос и запрос через шлюз возвращают 403. Через имя stage служебный журнал основного сайта также недоступен.

CVSS 3.1: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CWE-420 / незащищённый альтернативный канал

Первое уведомление через 7 часов 2 минуты

Заказчик получил доказательство F01 и срочные меры в день обнаружения. Подготовка полного отчёта продолжалась параллельно.

19.10 / 10:00	T+0	**Старт внешней проверки** Согласованы адреса, допустимая нагрузка и канал связи.
19.10 / 16:40	T+6 ч 40 м	**F01 подтверждена** Записаны manifest и 512 байт CSV. Дальнейшее чтение прекращено.
19.10 / 17:02	T+7 ч 02 м	**Срочное уведомление** Переданы риск, URL, доказательство и мера: закрыть весь путь экспорта.
20.10 / 16:15	T+30 ч 15 м	**F02: обход подписи через кэш** Результат повторён на двух тестовых PDF; проверены согласия в форме.
21.10 / 12:10	T+50 ч 10 м	**F03: прямой доступ к серверу** Сравнены ответы шлюза и общего сервера, выявленного через stage.
22.10 / 15:30	T+77 ч 30 м	**Заказчик убрал карту исходников** Промежуточная проверка показала: прямая ссылка на CSV ещё работает.
23.10 / 11:20	T+97 ч 20 м	**Заказчик ограничил origin и /ops** Ожидается проверка всех внешних путей к этому маршруту.
24.10 / 10:00	T+120 ч	**Полный отчёт Business** Технические находки, юридические риски и план исправлений.
25.10 / 11:20	T+145 ч 20 м	**Повторная проверка** F01: частично. F02: открыто. F03: исправлено.

Время в таблице: МСК (UTC+3). Заголовок Date в HTTP-доказательствах: GMT (UTC).

Что исправлено и что осталось

На 25 октября закрыт прямой доступ к служебному журналу. Выгрузки и документы из кэша всё ещё доступны; ниже указаны оставшиеся работы.

F01 / HIGH — **Частично исправлено**

22.10 убрана карта исходников. 25.10 сохранённая ссылка на CSV возвращает 206. Файл по-прежнему доступен посторонним.

Приёмка: Закрыть файлы и старые URL на origin и в кэше. Проверить 403/404 для прямых ссылок.

Backend + DevOps / до 26.10

F02 / MEDIUM — **Открыто**

Изменение CDN-правила перенесено в окно обслуживания. На 25.10 неподписанный запрос после прогрева получает 200.

Приёмка: После правки и очистки кэша запросы без подписи, с неверной или просроченной подписью возвращают 403.

DevOps / окно 28.10

F03 / MEDIUM — **Исправлено**

25.10 прямой IP, штатный домен и stage больше не раскрывают журнал. Проверены три внешних маршрута.

Приёмка: Сохранить ограничения origin и проверку маршрута /ops при следующих релизах.

Infrastructure / контроль при релизе

Повторная проверка исправлений бесплатна в течение 60 дней. Следующую проверку проведём, когда команда сообщит об исправлениях.

Три юридические проблемы

Проверены форма расчёта /quote, ссылки на документы и выдача PDF. В этом кейсе оператор работает в России. На 25 октября перечисленные проблемы остаются открытыми.

Политика обработки данных недоступна

Форма собирает имя, email и телефон. Ссылка «Политика обработки персональных данных» в форме и в подвале ведёт на /privacy с ответом 404.

Посетитель не может ознакомиться с политикой при передаче данных. Это нарушает требование обеспечить доступ к ней на страницах сбора данных.

Рекомендация: Опубликовать действующую политику, проверить ссылки во всех формах. Указать оператора, цели, данные, сроки обработки и порядок обращений.

152-ФЗ, ч. 2 ст. 18.1

Согласия объединены в одной галочке

Обязательная галочка уже отмечена и объединяет оферту, обработку данных и рекламу. Без неё форма не отправляется.

Согласие на обработку данных должно оформляться отдельно. Такая форма также не даёт надёжного доказательства добровольной подписки на рекламу; отправка рассылок не проверялась.

Рекомендация: Определить законное основание для каждой цели. Если нужно согласие, оформить его отдельно. Подписку на рекламу сделать добровольной, с пустой галочкой и записью выбора.

152-ФЗ, ч. 1 и 3 ст. 9

38-ФЗ, ч. 1 ст. 18

Контакты покупателей могут попасть к посторонним

В PDF из калькулятора есть ФИО, рабочие email и телефон. Ошибка F02 позволяет получить документ из кэша без проверки подписи.

Возникает риск нарушения конфиденциальности и требований к защите персональных данных. Доступ подтверждён на тестовых документах; утечка реальных данных не установлена.

Рекомендация: Закрыть выдачу PDF, очистить кэш и сохранить журналы доступа. Проверить, запрашивали ли посторонние реальные документы, и оценить необходимость уведомлений.

152-ФЗ, ч. 1 ст. 19

152-ФЗ, ст. 7

Что поручить команде

Для каждой проблемы определены ответственные и результат, который нужно проверить. Содержание документов и основания обработки сверяет юрист заказчика.

Политика	**Юрист и веб-разработчик** Документ соответствует действительным процессам компании. Ссылки в форме и подвале открываются без авторизации, сервер возвращает 200.
Согласия	**Юрист, маркетинг и разработчик** Заявка отправляется без подписки на рекламу. Согласия разделены. Сохраняются время, версия текста и выбор пользователя; отказ от рекламы прекращает рассылку.
Документы	**DevOps и ответственный за персональные данные** PDF без действующей подписи недоступен, в том числе из кэша. Журналы сохранены и проверены на обращения к реальным документам; выводы расследования зафиксированы.

Если подтвердится инцидент с персональными данными

При установленной неправомерной или случайной передаче либо доступе к данным, повлекших нарушение прав людей, оператор уведомляет Роскомнадзор с момента выявления инцидента:

В течение 24 часов - об инциденте, предполагаемых причинах и вреде, принятых мерах и контактном лице.
В течение 72 часов - о результатах внутреннего расследования.

152-ФЗ, ч. 3.1 ст. 21

Тестовый доступ сам по себе не доказывает такой инцидент.

Сценарий инцидента: 376 000 ₽

Пример расчёта для этого проекта: 60 заказов в день, средний чек 80 000 ₽, валовая маржа 12%, 12 часов активных продаж.

144 000 ₽

Потерянная маржа

Приостановка выдачи документов на 6 часов затрагивает 30 заказов. Предполагаем, что половина не вернётся.

30 × 50% × 80 000 ₽ × 12%

112 000 ₽

Разбор и восстановление

32 человеко-часа разработки, инфраструктуры и поддержки по внутренней расчётной ставке 3 500 ₽.

32 ч × 3 500 ₽

120 000 ₽

Уступки после раскрытия цен

Дополнительная скидка 1,5% на затронутый оборот 4 млн ₽ в месяц в течение двух месяцев.

4 000 000 ₽ × 2 × 1,5%

BUSINESS ОТ 39 900 ₽

В этом сценарии стоимость проверки составляет около 10,6% суммы последствий. Для вашего проекта расчёт строится на показателях вашей компании.

Допущение: в одном инциденте раскрылись цены и пришлось приостановить выдачу документов. Это возможные расходы, без оценки вероятности. Штрафы и долгосрочная потеря клиентов в сумму не включены.

Проверять после изменений и раз в квартал

Новый релиз может снова открыть выгрузку, изменить правило кэша или связать тестовый стенд с основным сервером. После таких изменений проверку стоит повторять.

СЕЙЧАС

Закрыть технические и юридические риски

Закрыть доступ к выгрузкам и PDF, исправить политику и согласия. Повторная проверка технических исправлений в течение 60 дней входит в текущую работу.

ПОСЛЕ ЗНАЧИМОГО РЕЛИЗА

Проверить изменённые участки

Новые сборки, правила CDN, экспорт документов, DNS и маршруты стендов. Объём новой проверки согласовать до запуска.

РАЗ В КВАРТАЛ

Обновить карту периметра

Повторить Business для текущего состояния домена. Сопоставить новые и исчезнувшие узлы, изменения защиты и повторившиеся ошибки.

БЮДЖЕТ НА ЧЕТЫРЕ ПРОВЕРКИ BUSINESS

от 159 600 ₽ в год

Расчёт: 4 × 39 900 ₽ за отдельные проверки. Конечный объём и стоимость фиксируются до начала работ.

CVSS 3.1 / методика оценки тяжести

RFC 9111 / HTTP-кэширование

Business

Пришлите домен. Получите первый результат в течение 24 часов.

от 39 900 ₽

Полный отчёт Business: 5-7 дней.
Оплата картой, переводом или криптовалютой.

Внешняя проверка	AI-агенты исследуют сайт, поддомены и доступные из интернета сервисы.
Подтверждённые находки	Специалист проверяет значимые результаты и помогает определить приоритет.
Помощь с исправлениями	Рекомендации разработчику и бесплатный ретест исправлений в течение 60 дней.

Обсудить проверку

Написать в Telegram

support@cyberyozh.com

cyberyozh.com/pentest

До старта согласуем объём, цену и разрешение на проверку.

Компания, находки, журнал и финансовые допущения в этом примере вымышлены.