

Пентест

Проверяем защиту так, как это сделал бы атакующий, — по договору

Проверяем защиту так, как это сделал бы атакующий, — по договору и с письменного разрешения. В отчёте только подтверждённые уязвимости: что нашли, чем грозит и как исправить. Повторная проверка после исправлений входит в цену.

для кого

Компаниям, которым нужен ответ на вопрос «что будет, если нас атакуют»:

- крупный клиент или банк просит отчёт о проверке защищённости
- запускаете личный кабинет, портал или приложение с данными клиентов
- после экспресс-аудита нужно проверить, насколько опасны найденные слабые места
- был инцидент, и нужно понять, какие ещё двери открыты

что вы получаете

- **Правила проведения** — границы, окна работ, контакты на случай сбоя — до начала
- **Внешний периметр** — сервисы, почта, VPN, удалённый доступ, открытые порты
- **Веб-приложения** — авторизация, роли, платежи, API, типовые уязвимости из OWASP Top 10
- **Внутренняя сеть** — что может злоумышленник, попавший в офисную сеть, и как далеко он дойдёт
- **Отчёт для двух аудиторий** — резюме для руководителя и шаги для ИТ по каждой уязвимости
- **Повторная проверка** — после исправлений подтверждаем, что уязвимость закрыта

цена · срок

ТАРИФ	что входит	цена	срок
Внешний периметр	До 16 внешних адресов: сервисы, почта, VPN, открытые порты	от 6 900 BYN	2 нед
Веб-приложение ★ ЧАЩЕ БЕРУТ	Личный кабинет или портал с ролями плюс 4 внешних адреса	от 10 200 BYN	2–3 нед
Комплексный	Периметр, веб-приложение и внутренняя сеть до 50 хостов	от 20 300 BYN	4–5 нед

— Цены в белорусских рублях без НДС, 20% НДС добавляется в счёт.

— Точный состав и сумму соберите в калькуляторе на viviар.by/pricing: если параметры подтвердятся на звонке, в предложении не будет больше расчёта.

— Оплата: 50% предоплата, остаток по акту.

1. Подтверждённые уязвимости

Каждую находку проверяем вручную, ложные срабатывания сканера в отчёт не попадают.

3. Готовое продолжение

Если исправить своими силами не получается — исправим в рамках разработки или поддержки.

2. Бережно к работе

Агрессивные проверки — только в согласованное окно, опасные для работы систем действия заранее обсуждаем.

ЧАСТЫЕ ВОПРОСЫ

Это законно?

Да, при договоре и письменном разрешении владельца системы. Для систем, не относящихся к критически важным объектам, лицензия не требуется. Для обязательных проверок по требованиям ОАЦ организаций из перечня Совмина работает аттестованный центр кибербезопасности — такие проверки ведём через партнёра.

Чем пентест отличается от экспресс-аудита?

Аудит оценивает, как устроена безопасность в целом и что поправить в первую очередь. Пентест проверяет конкретные системы на практике и доказывает, что уязвимость реальна.

Вы не положите нам сайт?

Риск минимальный: нагрузочные и разрушающие проверки не проводим без отдельного согласования, работаем в окна, которые вы назначите, и держим связь с вашим ИТ.

Что нужно от нас?

Список адресов и приложений, разрешение за подписью руководителя, контакт ИТ на время работ. Для проверки с учётными записями — тестовые пользователи с разными ролями.

КАК НАЧАТЬ

Напишите на info@viviar.by или позвоните по +375 44 506-00-05. Соберите расчёт на viviar.by/pricing и отправьте его нам — перезвоним в течение рабочего дня и зафиксируем цену.

info@viviar.by · +375 44 506-00-05