

Vulnerability Disclosure Policy

Публичный порядок сообщения ВирТЭК об обнаруженной уязвимости или подозрительном событии безопасности.

Код документа	VIR-PUB-VDP-001
Категория	Информационная безопасность
Публикация	27.09.2026 • версия 1.0 • действует до замены новой редакцией

Публичная версия. Предназначена для размещения на сайте и предоставления заказчикам и партнёрам. Не содержит конфиденциальных технических деталей и не заменяет договорные условия или внутренние регламенты.

Связанные материалы: virtek.pro/trust-center • virtek.pro/documents

1. Назначение

ВирТЭК принимает сообщения об уязвимостях, ошибках конфигурации и подозрительной активности, которые могут затрагивать публичные сервисы компании или решения, находящиеся в зоне ответственности ВирТЭК. Цель процесса — безопасно получить сведения, оценить риск, локализовать проблему и организовать исправление.

2. Как сообщить

- Создайте обращение на портале поддержки ВирТЭК с пометкой «Информационная безопасность» либо направьте первичное сообщение на info@virtek.pro.
- Укажите затронутый сервис или адрес, дату и время наблюдения, краткое описание симптома и возможное влияние.
- Не отправляйте в первом сообщении пароли, приватные ключи, токены, персональные данные, дампы баз данных или иные секреты.
- Если для подтверждения нужны чувствительные материалы, дождитесь согласования безопасного канала передачи.

3. Что полезно приложить

- понятное описание наблюдаемого поведения и ожидаемого результата;
- минимально необходимую последовательность воспроизведения;
- версию приложения или компонента, если она известна;
- скриншот или фрагмент лога без секретов и лишних персональных данных;
- оценку возможного влияния, если она известна автору сообщения.

4. Чего не следует делать

- публиковать технические детали до первичной оценки и согласования раскрытия;

- передавать пароли, ключи, токены и другие секреты в открытом сообщении;
- нарушать работу сервисов, изменять или удалять данные для демонстрации проблемы;
- расширять проверку на системы и данные, к которым у исследователя нет законного права доступа.

5. Обработка сообщения

1. Регистрация обращения и подтверждение получения.
2. Первичная оценка затронутого сервиса, влияния и критичности.
3. При необходимости — согласование защищённого канала и получение дополнительных доказательств.
4. Локализация риска и постановка корректирующих действий.
5. Проверка исправления и закрытие обращения либо перевод в дальнейший процесс управления изменениями/инцидентами.

6. Важное ограничение

Документ не является разрешением на тестирование

Публикация данной политики не предоставляет право проводить несанкционированное сканирование, эксплуатацию уязвимостей, доступ к данным или иные действия за пределами законных полномочий. Для согласованных тестов область, методы и условия фиксируются отдельно.

Публикация и актуализация

Актуальная редакция документа публикуется на сайте ВирТЭК. Документ пересматривается при существенном изменении процессов, архитектуры, законодательства, договорной модели или требований заказчиков.

Актуальная версия: virtek.pro/documents