Security Policy

Поддерживаемые версии

В настоящее время поддерживаются следующие версии UPAK Frontend с обновлениями безопасности:

Версия	Поддерживается
1.0.x	:white_check_mark: Да
< 1.0	:x: Нет

Сообщение о уязвимостях безопасности

Безопасность пользователей UPAK Frontend имеет для нас первостепенное значение. Если вы обнаружили уязвимость безопасности, пожалуйста, сообщите об этом ответственно.

Как сообщить о уязвимости

Пожалуйста, НЕ создавайте публичные GitHub issues для уязвимостей безопасности.

Вместо этого:

1. **Отправьте email на**: security@upak.space
2. **Укажите в теме**: `[SECURITY] Vulnerability Report`
3. **Включите следующую информацию**:
   - Описание уязвимости
   - Шаги для воспроизведения
   - Потенциальное воздействие
   - Предлагаемое решение (если есть)

Что ожидать

- **Подтверждение получения**: в течение 24 часов
- **Первоначальная оценка**: в течение 72 часов
- **Статус обновления**: еженедельно до разрешения
- **Исправление**: в зависимости от серьезности (см. ниже)

Временные рамки для исправлений

Уровень серьезности	Время исправления
Критический	24-48 часов
Высокий	7 дней
Средний	30 дней
Низкий	90 дней

Политика ответственного разглашения

Мы придерживаемся политики ответственного разглашения информации:

1. **Не публикуйте** подробности уязвимости до выпуска исправления
2. **Дайте нам разумное время** для исправления проблемы
3. **Не используйте** уязвимость для доступа к данным, которые вам не принадлежат

Вознаграждение

Хотя мы не предлагаем денежное вознаграждение, мы:

- Публично признаем вашу находку (с вашего согласия)
- Добавим вас в зал славы безопасности
- Предоставим кредиты в наших релизах

Scope (Область применения)

В области применения ✅

- **Frontend приложение**: Все компоненты Next.js
- **API endpoints**: /api/* routes
- **Authentication**: NextAuth.js реализация
- **Database**: Prisma ORM запросы
- **Docker containers**: Production конфигурации
- **CI/CD pipeline**: GitHub Actions workflows

Вне области применения ❌

- **Third-party зависимости**: За исключением наших конфигураций
- **Infrastructure**: Хостинг провайдеры, CDN
- **Social engineering**: Фишинг, обман пользователей
- **Physical attacks**: Доступ к серверам
- **DDoS attacks**: Атаки на доступность

Лучшие практики безопасности

Для разработчиков

- **Валидация входных данных**: Используйте Zod для всех inputs
- **Sanitization**: Очищайте все пользовательские данные
- **Authentication**: Используйте NextAuth.js правильно
- **Authorization**: Проверяйте права доступа
- **Environment variables**: Никогда не коммитьте секреты
- **Dependencies**: Регулярно обновляйте зависимости

Для пользователей

- **Пароли**: Используйте сильные, уникальные пароли
- **2FA**: Включите двухфакторную аутентификацию (когда доступна)
- **Updates**: Используйте последнюю версию браузера
- **HTTPS**: Всегда проверяйте SSL сертификат
- **Phishing**: Остерегайтесь подозрительных ссылок

Конфигурация безопасности

Headers безопасности

```
# Content Security Policy
add_header Content-Security-Policy "default-src 'self'; script-src 'self' 'unsafe-in-
line'";

# Prevent clickjacking
add_header X-Frame-Options DENY;

# Prevent MIME type sniffing
add_header X-Content-Type-Options nosniff;

# XSS Protection
add_header X-XSS-Protection "1; mode=block";

# HSTS
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains";
```

Rate Limiting

```
# API rate limiting
limit_req_zone $binary_remote_addr zone=api:10m rate=10r/s;

# Auth rate limiting
limit_req_zone $binary_remote_addr zone=login:10m rate=1r/s;
```

Мониторинг безопасности

Автоматические проверки

- **GitHub Security Advisories**: Автоматическое сканирование зависимостей
- **Snyk**: Проверка уязвимостей в CI/CD

- **ESLint Security Plugin**: Статический анализ кода
- **Dependabot**: Автоматические PR для обновлений безопасности

Логирование

```
// Логирование подозрительной активности
console.warn('Suspicious activity detected:', {
  ip: request.ip,
  userAgent: request.headers['user-agent'],
  timestamp: new Date().toISOString()
})
```

Инциденты безопасности

История инцидентов

Дата	Уровень	Описание	Статус
-	-	-	Нет зарегистрированных инцидентов

Процедура реагирования

1. **Обнаружение** → Немедленное уведомление команды
2. **Оценка** → Определение масштаба и воздействия
3. **Изоляция** → Ограничение распространения
4. **Исправление** → Устранение уязвимости
5. **Восстановление** → Возврат к нормальной работе
6. **Анализ** → Post-mortem и улучшения

Соответствие стандартам

- **OWASP Top 10**: Регулярные проверки
- **GDPR**: Обработка персональных данных
- **SOC 2**: Контроли безопасности (планируется)
- **ISO 27001**: Система менеджмента безопасности (планируется)

Контакты

- **Security Team**: security@upak.space
- **General Contact**: support@upak.space
- **Telegram**: @upak_security (https://t.me/upak_security)

Благодарности

Спасибо следующим исследователям безопасности за их ответственное раскрытие:

- Список будет обновляться по мере поступления отчетов

Дата последнего обновления: Август 2025
Версия документа: 1.0.0