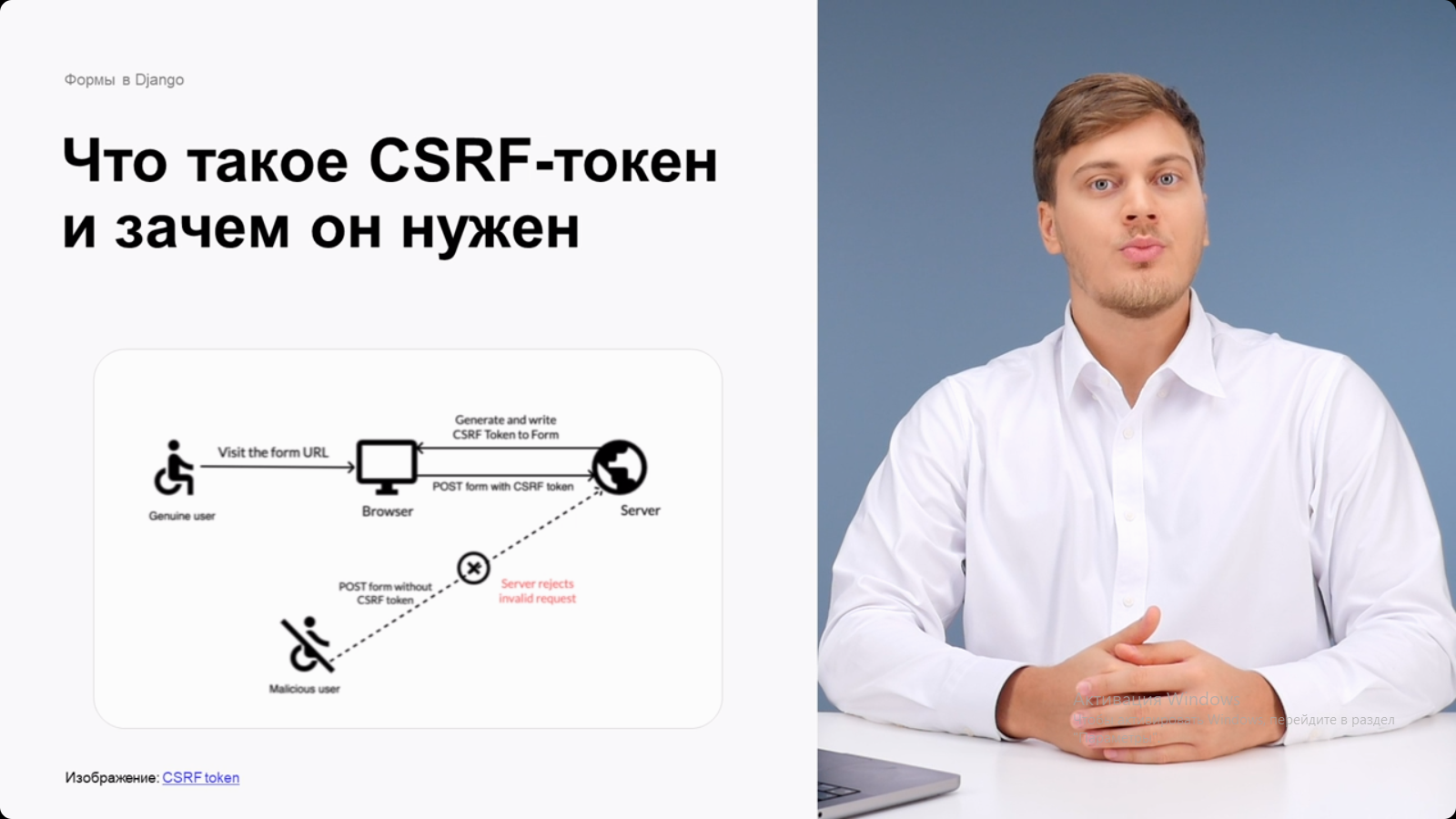
**6.5 Что такое CSRF-токен и зачем он нужен**

CSRF-токен это инструмент защиты. Это такой тип атаки. Он расшифровывается как Сross Site Request Forgery и переводится как атака с межсетевой подделкой запросов. Такой вид атаки заставляет конечного пользователя выполнять нежелательные действия в вэб приложении, в котором он аутентифицировал себя. Злоумышленник заставляет пользователя сделать запрос, который тот не планировал в своих интересах.

CSRF это распространённая атака, поэтому Django реализует csrf-токен и позволяет использовать его в шаблонах. Django требует использование csrf-токена при публикации форм и при использовании небезопасных запросов. Токен генерируется на бэкенде при каждом новом запросе и он основывается на секретном ключе, указанном в настройках. Поэтому его нельзя подменить. При публикации формы или выполнении другого небезопасного запроса Django проверяет csrf-токен на валидность и отвергает невалидные формы.

Так как от разработчика не требуется ничего, кроме добавления одного токена в форму, рекомендуется использовать эту защиту всегда. Этот инструмент позволяет защитить приложения при обработке небезопасных методов запросов. Помимо post-запросов небезопасными являются также delete, put и patch. Безопасными являются те методы, которые ни чего не меняют на бэкенде, это get, head и options.

Описание

* [How to use Django’s CSRF protection](https://docs.djangoproject.com/en/4.1/howto/csrf/)
* [What is a CSRF token in Django?](https://www.educative.io/answers/what-is-a-csrf-token-in-django)