



**ИНФЕРИТ**  
Операционные  
системы

## Почему критично обновляться?

Обеспечение безопасности информации  
при эксплуатации ОС в информационных системах



**Фокин Максим**

Директор департамента сертификации  
и безопасной разработки



# Для чего нужны обновления ОС

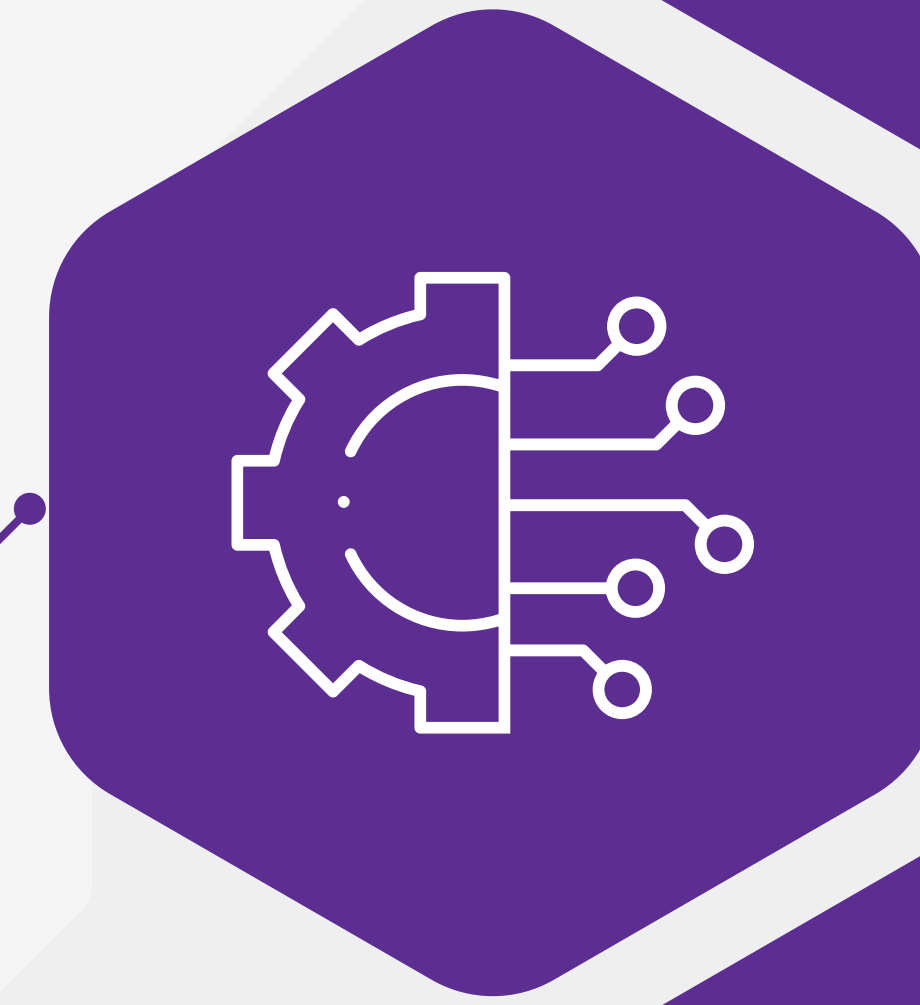
Новые функции  
и возможности



Увеличение  
производительности



Обеспечение  
совместимости



Обновления  
графического  
интерфейса



Обеспечение  
безопасности



# Важность обновлений безопасности



Устранение выявленных уязвимостей в ОС



Уменьшение поверхности атаки для злоумышленника

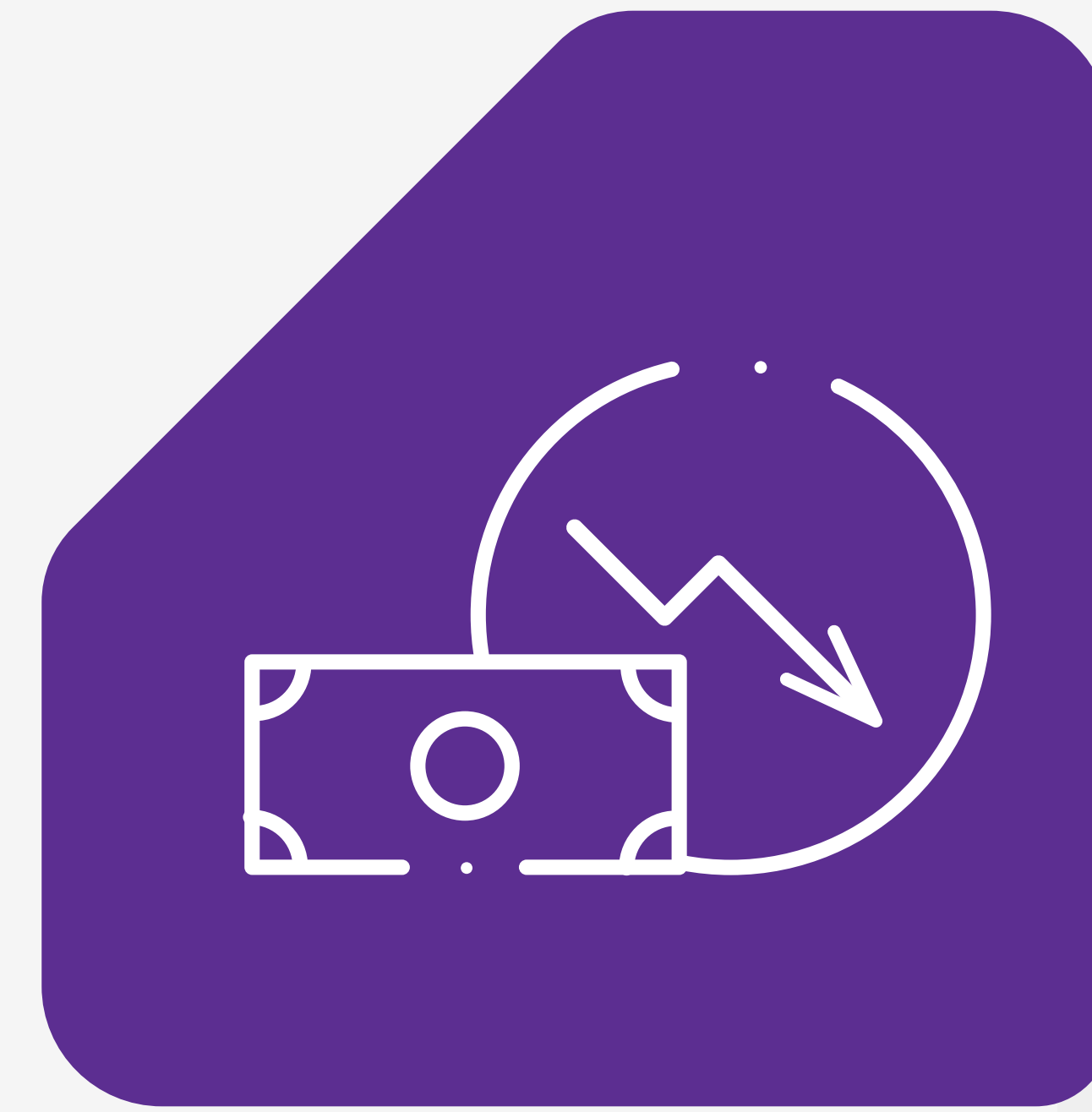


# К чему может привести несвоевременное обновление ОС

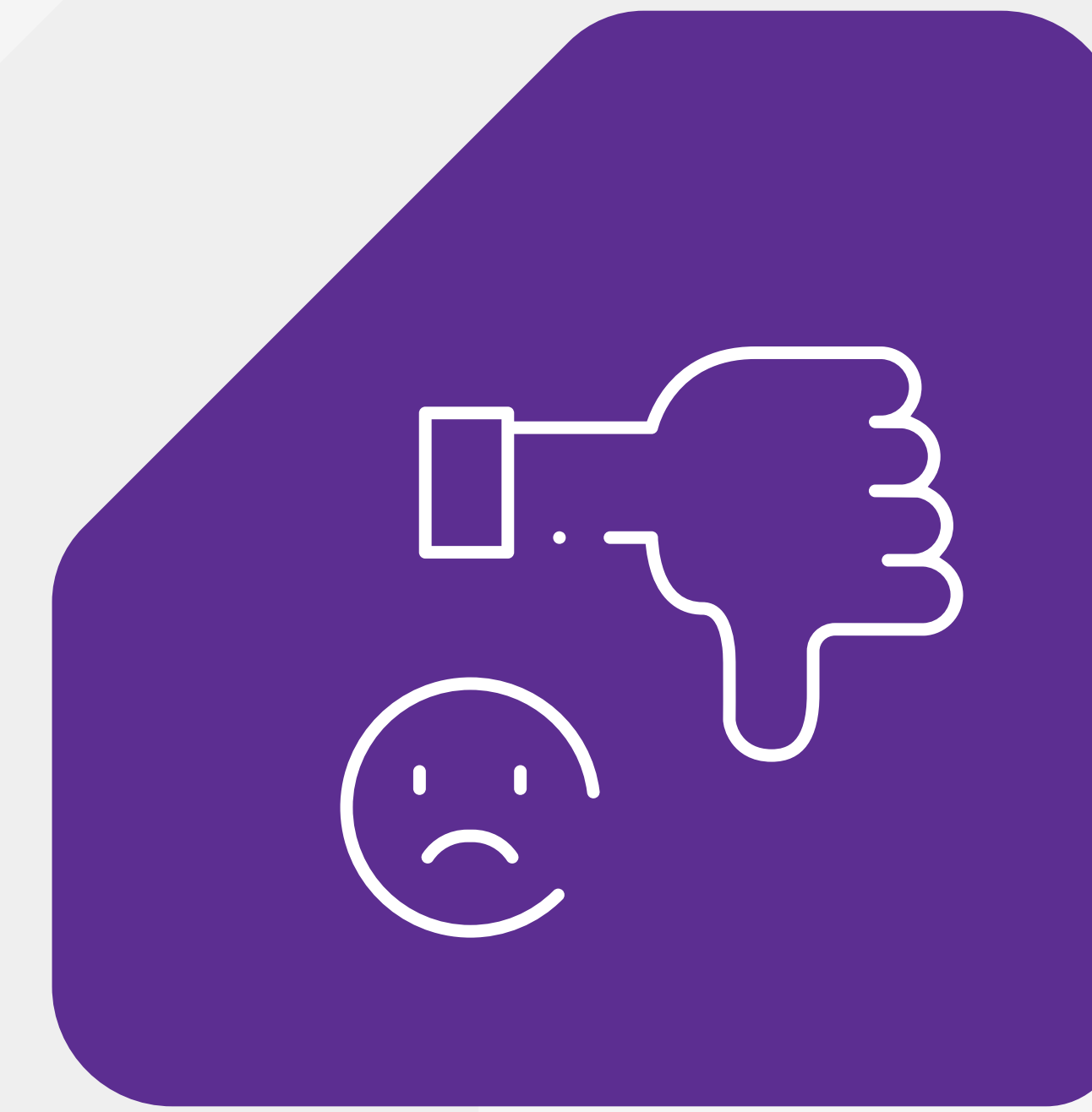
Почему критично обновляться?



Атаки  
на организацию



Финансовые  
потери



Потеря имиджа  
на рынке



Санкции  
от регуляторов  
в области ИБ

# Пример последствий несвоевременного обновления ОС

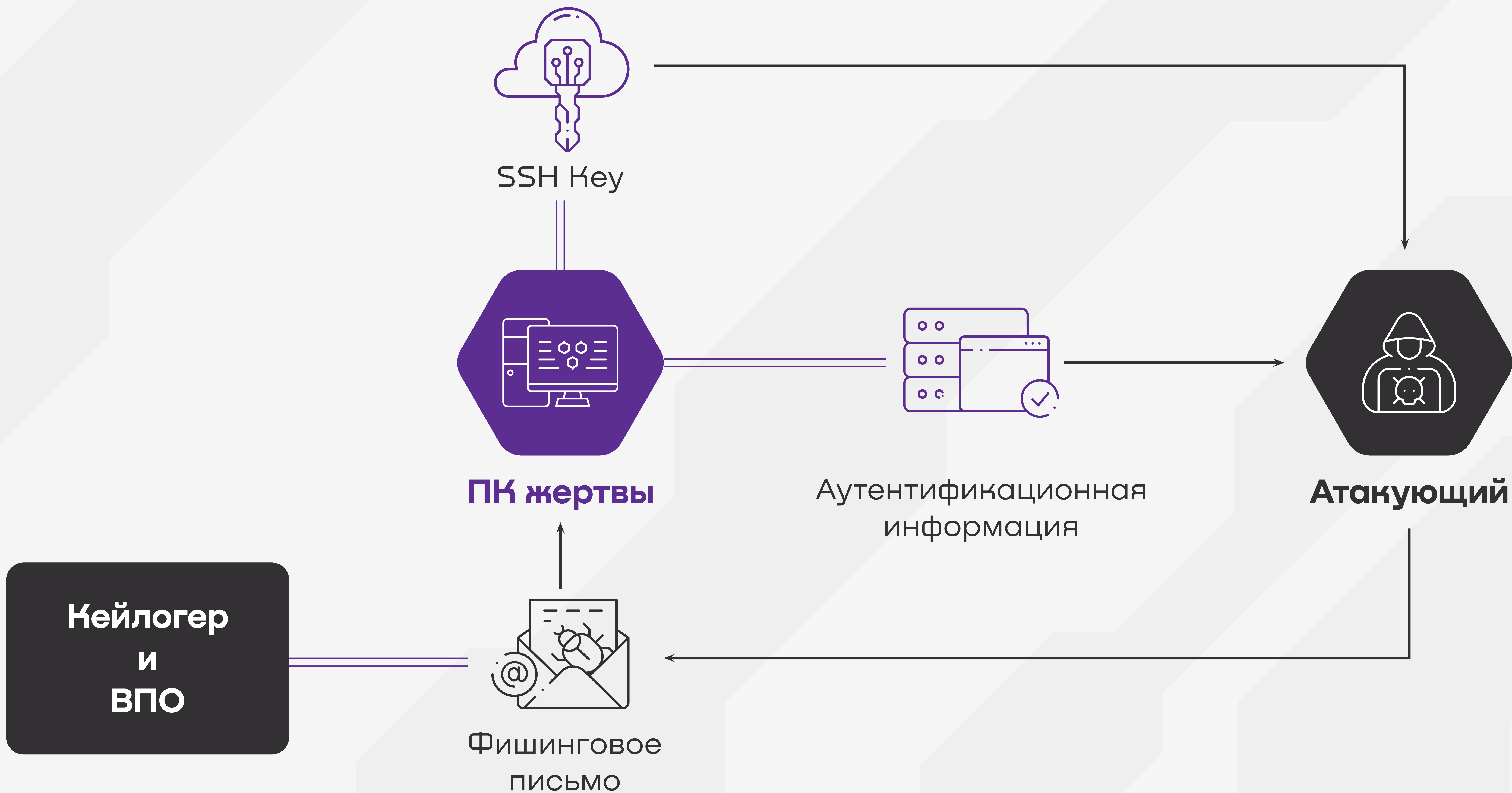
WannaCry — пострадало более 500 000 компьютеров, безвозвратно потерявших доступ к информации.

**EternalBlue  
CVE-2017-0144**

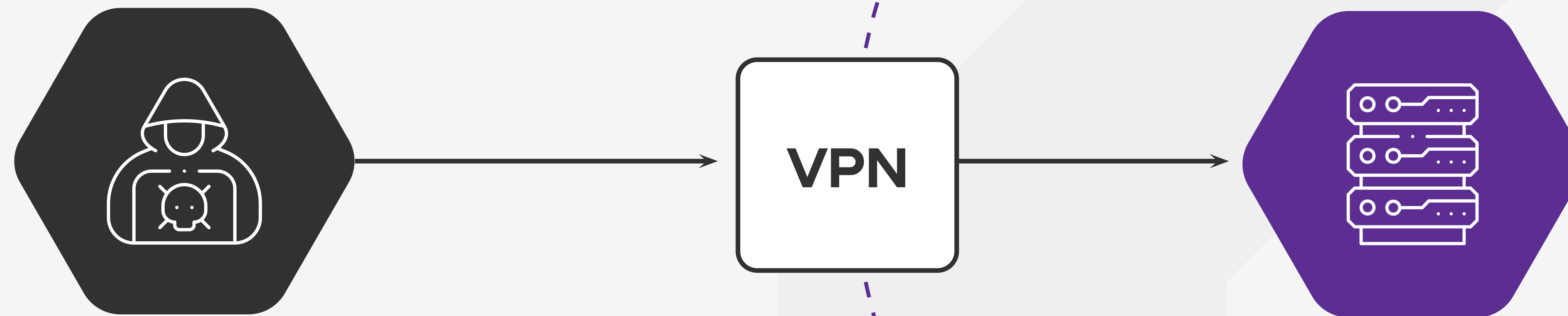


# Атака. Часть 1

Почему критично обновляться?



# Атака. Часть 2



**Атакующий**

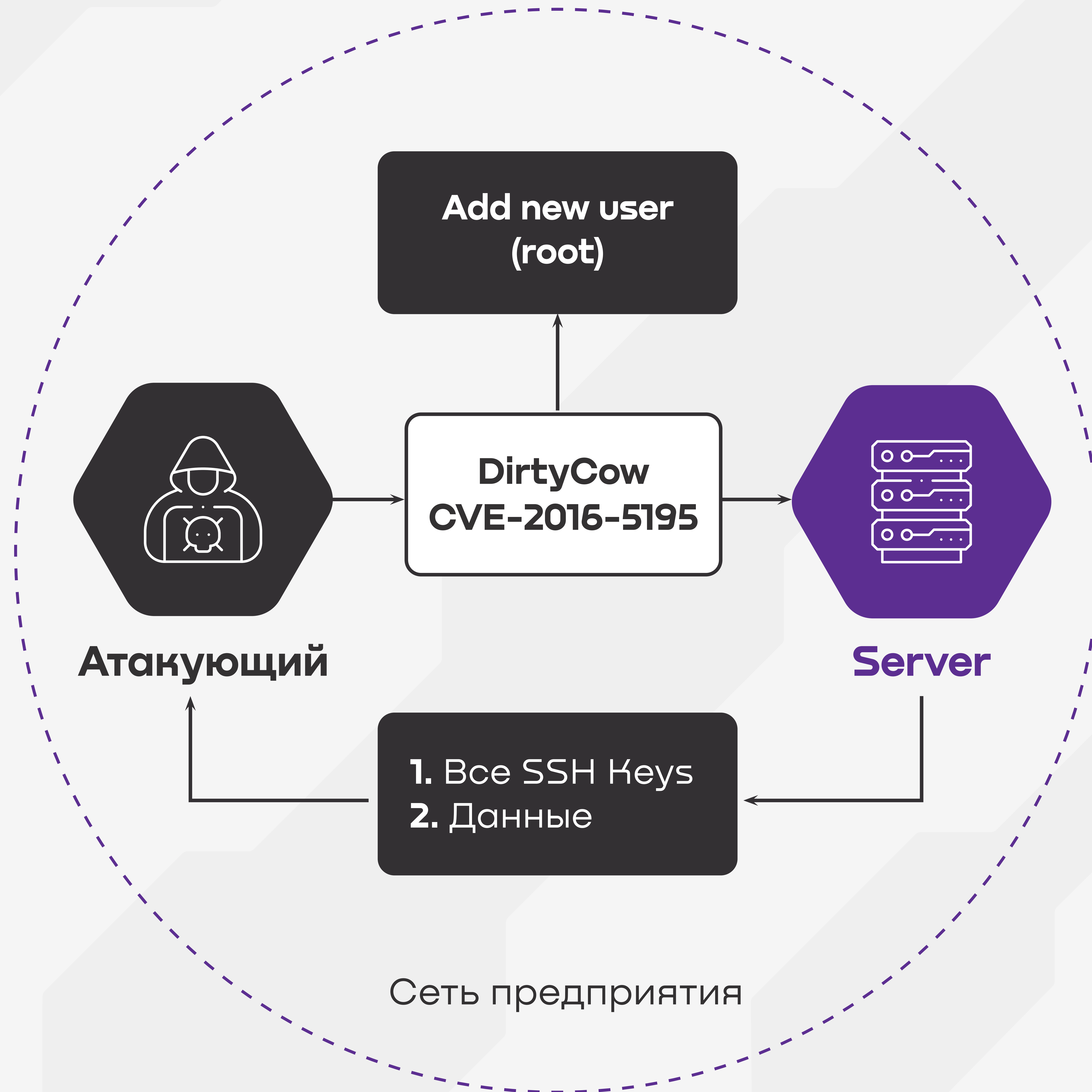
**Server**

Сеть  
предприятия

- 1. Логин и пароль от корпоративных сервисов.
- 2. SSH Key и пароль от него



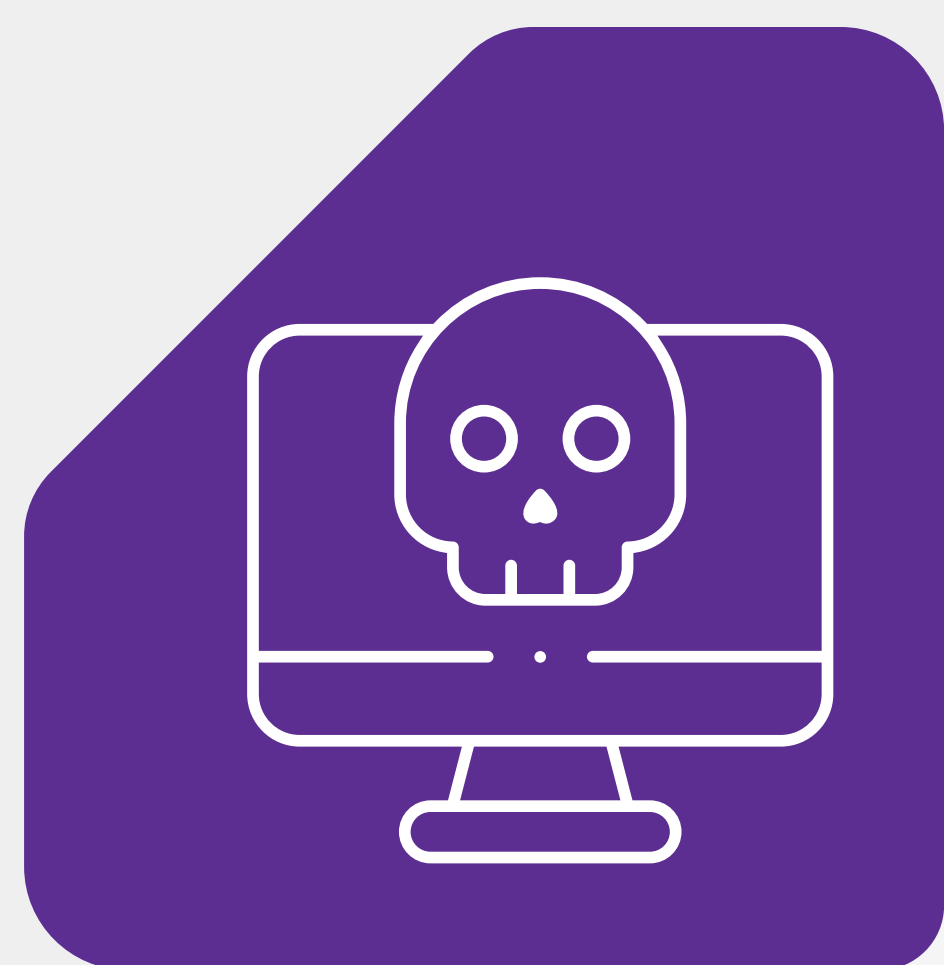
# Атака. Часть 3



Почему критично обновляться?



# Атака. Итог



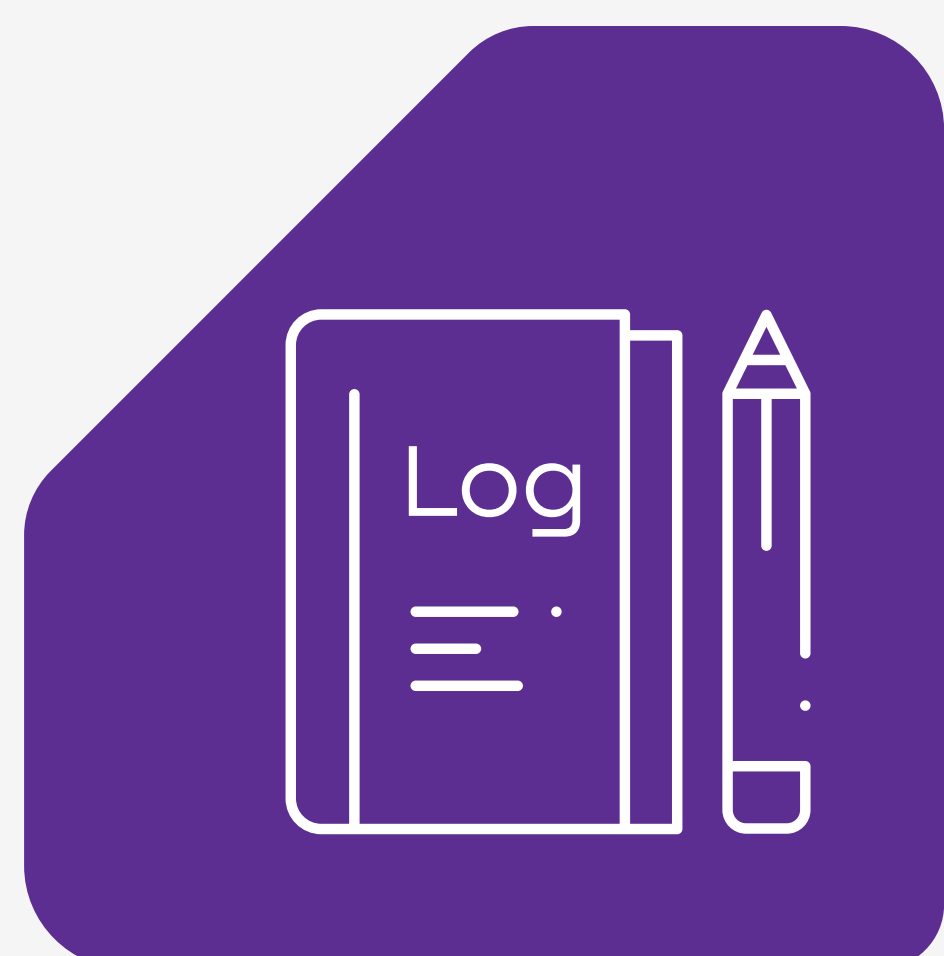
## ВПО

На важном корпоративном сервере было оставлено ВПО (бэкдор).



## SSH Keys

Украдены все SSH ключи, хранящиеся на сервере.



## Log files

Все логи сервера были почищены, в связи с чем расследование инцидента заняло продолжительное время



## Data

Все данные, хранящиеся на сервере были скомпрометированы, что в последствии отразилось на финансовых и репутационных потерях компании



Необходимо всегда своевременно обновлять ОС



Необходимо дополнительно проводить анализ уязвимостей ОС различными инструментами анализа и при обнаружении взаимодействовать с вендором ОС для их устранения



# Спасибо за внимание!



**Чтобы наши решения были доступны каждому**

Если вы заинтересованы в сотрудничестве с «Инферит», хотите обсудить проект и узнать больше о наших продуктах и услугах, мы будем рады помочь

8 800 707-85-53

[sales@inferit.ru](mailto:sales@inferit.ru) | [partners@inferit.ru](mailto:partners@inferit.ru)

[www.inferit.ru](http://www.inferit.ru)

