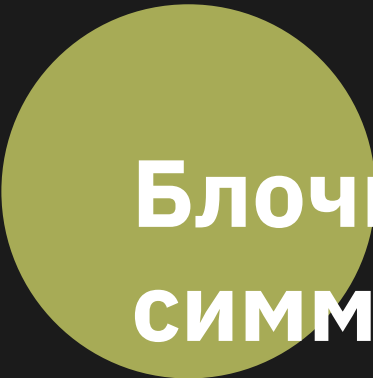


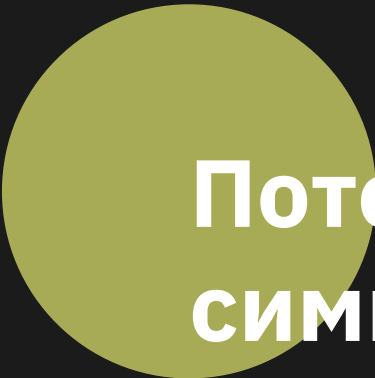


# ВЫБОР СТАНДАРТОВ


Области обеспечения безопасности компьютерной информации




**Блочное  
симметричное  
шифрование**  
17 алгоритмов



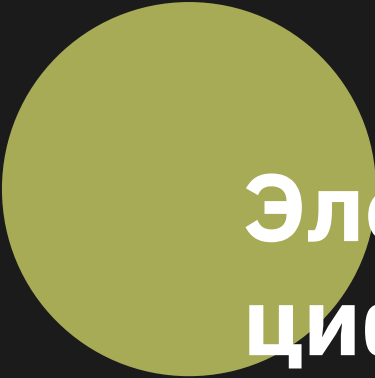
**Потоковое  
симметричное  
шифрование**  
6 алгоритмов



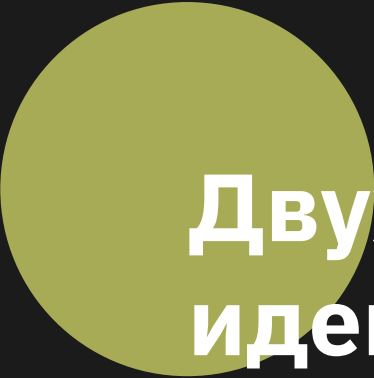
**Асимметричное  
шифрование**  
5 алгоритмов



**Хэширование**  
1 алгоритм



**Электронная  
цифровая  
подпись**  
7 алгоритмов



**Двухключевая  
идентификация**  
1 алгоритм

# ОСНОВНЫЕ МОМЕНТЫ

1. Организаторы конкурса не преследовали цель выбрать наилучший из алгоритмов в каждой из перечисленных категорий

2. Кроме алгоритмов, присланных на конкурс, рассматривались и известные криптографические стандарты



3. Не был установлен какой-либо конкретный размер блока шифруемых данных, поэтому в конкурсе рассматривались 64-, 128-, 160- и 256-битные блочные шифры



# ОРГАНИЗАТОРЫ КОНКУРСА

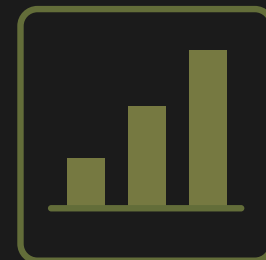
Бельгия

**Католический  
Университет  
г. Лювен**



Германия

**Корпорация  
Siemens AG**



Франция

**Высшее учебное  
заведение Ecole  
Normale Supérieure**



Израиль

**Технологический  
Институт Technion**



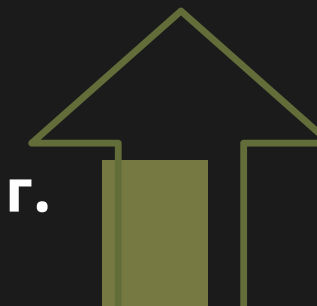
Великобритания

**Университет  
Royal Holloway**



Норвегия

**Университет г.  
Берген**



# РЕЗУЛЬТАТЫ NESSIE



## Блочные шифры

У - MISTY1 , Camellia ,  
SHACAL-2, AES



## Шифрование с открытым ключом

ACE Encrypt, PSEC-KEM,  
RSA-KEM



## Алгоритмы электронных подписей

ECDSA, RSA-PSS (RSA Labora,  
SFLASH



## Алгоритмы вычисления кодов аутентификации сообщений и хэш- функции

Two-Track-MAC, UMAC, CBC-MAC,  
HMAC, Whirlpool, SHA-256, SHA-  
384 and SHA-512



## Алгоритмы для идентификации

GPS

стандартов до

The image shows a composite graphic. At the bottom is a close-up of a computer keyboard. Overlaid on this is a semi-transparent dark circle containing a screenshot of a code editor. The code editor displays PHP code for a login page, including functions for printing URLs, handling login attempts, and displaying error messages. Below the code, there are several buttons with keyboard shortcuts: 'WriteOut Justify' (Alt+O, Alt+J), 'Read File Where Is' (Alt+R, Alt+W), 'Prev Page Next Page' (Alt+P, Alt+N), and 'Cut Text UnCut Text' (Alt+C, Alt+U). The text 'стандартов до' is written in large, bold, white Cyrillic letters in the upper right corner of the image.