РусКрипто

О механизмах криптографической защиты данных публичных облачных хранилищ и перспективах стандартизации технических спецификаций к прикладным протоколам облачных хранилищ данных

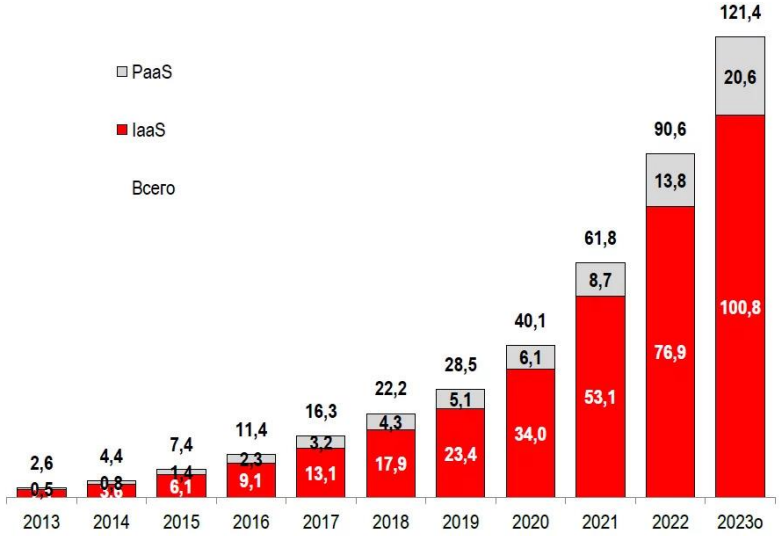
Минаков С. С., АНО «НТЦ ЦК»
Тихов С. В., НТП «Криптософт»

XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

ОБЛАЧНОЕ ХРАНИЛИЩЕ ДАННЫХ

РусКрипто

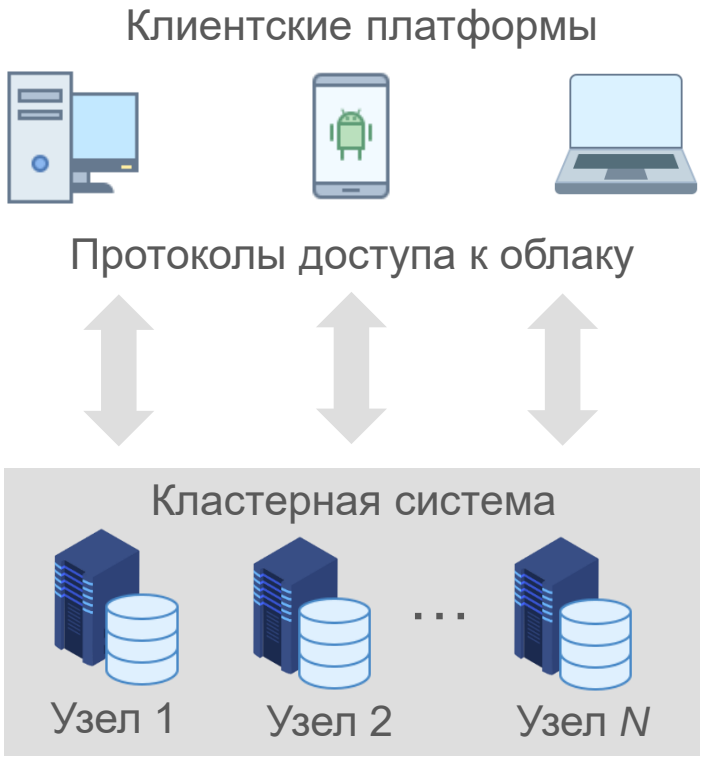
Облачное хранилище данных — это модель онлайн-хранилища, в котором данные хранятся на многочисленных распределенных в сети серверах, предоставляемых в пользование клиентам третьей стороной.



Рынок облачных инфраструктурных сервисов в России в 2013-2023 гг., млрд руб.

ОБЩАЯ АРХИТЕКТУРА ОБЛАЧНЫХ ХРАНИЛИЩ ДАННЫХ

- В основе архитектуры облачных хранилищ лежит кластерная система.
- Для каталогизации и увеличения скорости отклика системы используются кластерные файловые системы.
- Для доступа к облачным хранилищам используются специальные протоколы и интерфейсы доступа: WebDAV, AWS S3, CalDAV и др.



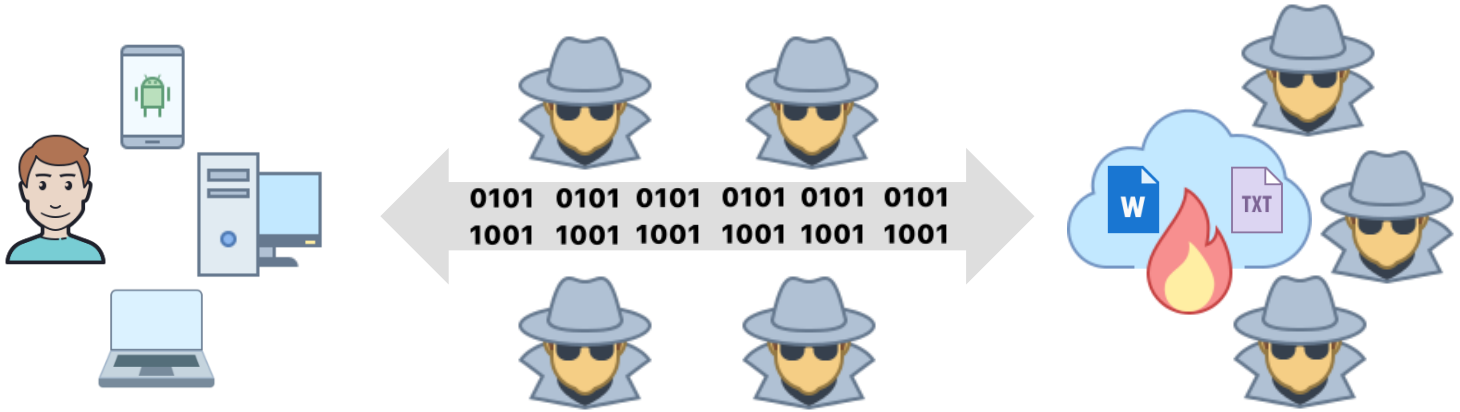
РусКрипто

ИНФОРМАЦИОННАЯ БЕЗОПАСТНОСТЬ ДАННЫХ В ОБЛАКЕ

РусКрипто

Облачные хранилища удобны и экономически эффективны, но имеют определенные проблемы, связанные с информационной безопасностью данных.

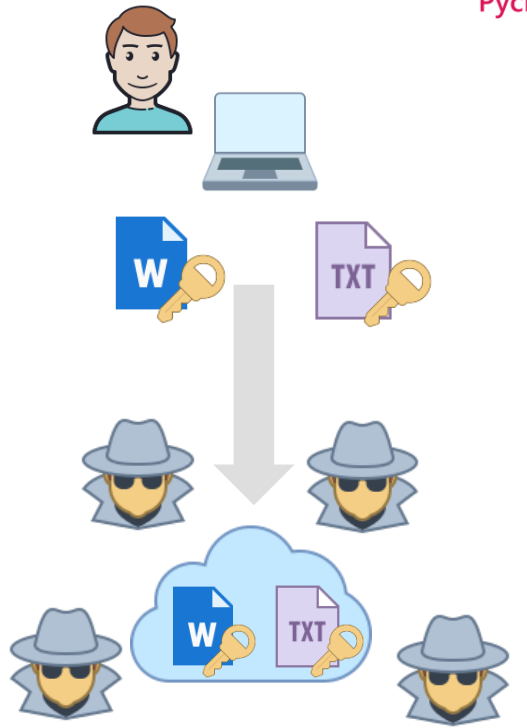
Облачные сервисы обработки и хранения данных постоянно подвергаются различным видам кибератак.



ШИФРОВАНИЕ ДАННЫХ

РусКрипто

Возможным решением проблемы обеспечения информационной безопасности данных в облаке является **шифрование данных**, размещаемых в «облаках», **на стороне клиента**, что обеспечивает защиту данных как при передаче по публичному каналу связи, так и при хранении на удаленных серверах облачного центра.



ЗАЩИЩЕННЫЙ ДОСТУП К ОБЛАКУ ПО ПРОТОКОЛУ WEBDAV

РусКрипто

>>>Request (исходный)

```
PUT /readme.pdf HTTP/1.1
Host: webdav.yandex.ru
Accept: */*
Authorization: xxx
Etag: xxx
Sha256: xxx
Expect: 100-continue
Content-Type: application/binary
Content-Length: xxx

<содержимое файла>
```

>>>Request (измененный)

```
PUT /readme.pdf HTTP/1.1
Host: webdav.yandex.ru
Accept: */*
Authorization: xxx
Etag: xxx
Sha256: xxx
Expect: 100-continue
Content-Type: application/binary
Content-Length: xxx

<зашифрованное
содержимое файла>
```

ЗАЩИЩЕННЫЙ ДОСТУП К ОБЛАКУ ПО ПРОТОКОЛУ AWS S3

РусКрипто

>>>Request (исходный)

```
PUT /Key+? HTTP/1.1
Host: storage.yandexcloud.net
Authorization: xxx
Content-Length: xxx
Content-MD5: xxx
Content-Type: xxx

<содержимое файла>
```

>>>Request (измененный)

```
PUT /Key+? HTTP/1.1
Host: storage.yandexcloud.net
Authorization: xxx
Content-Length: xxx
Content-MD5: xxx
Content-Type: xxx

<зашифрованное
содержимое файла>
```

ЗАЩИЩЕННЫЙ ДОСТУП К ОБЛАКУ ПО ПРОТОКОЛУ CALDAV

РусКрипто

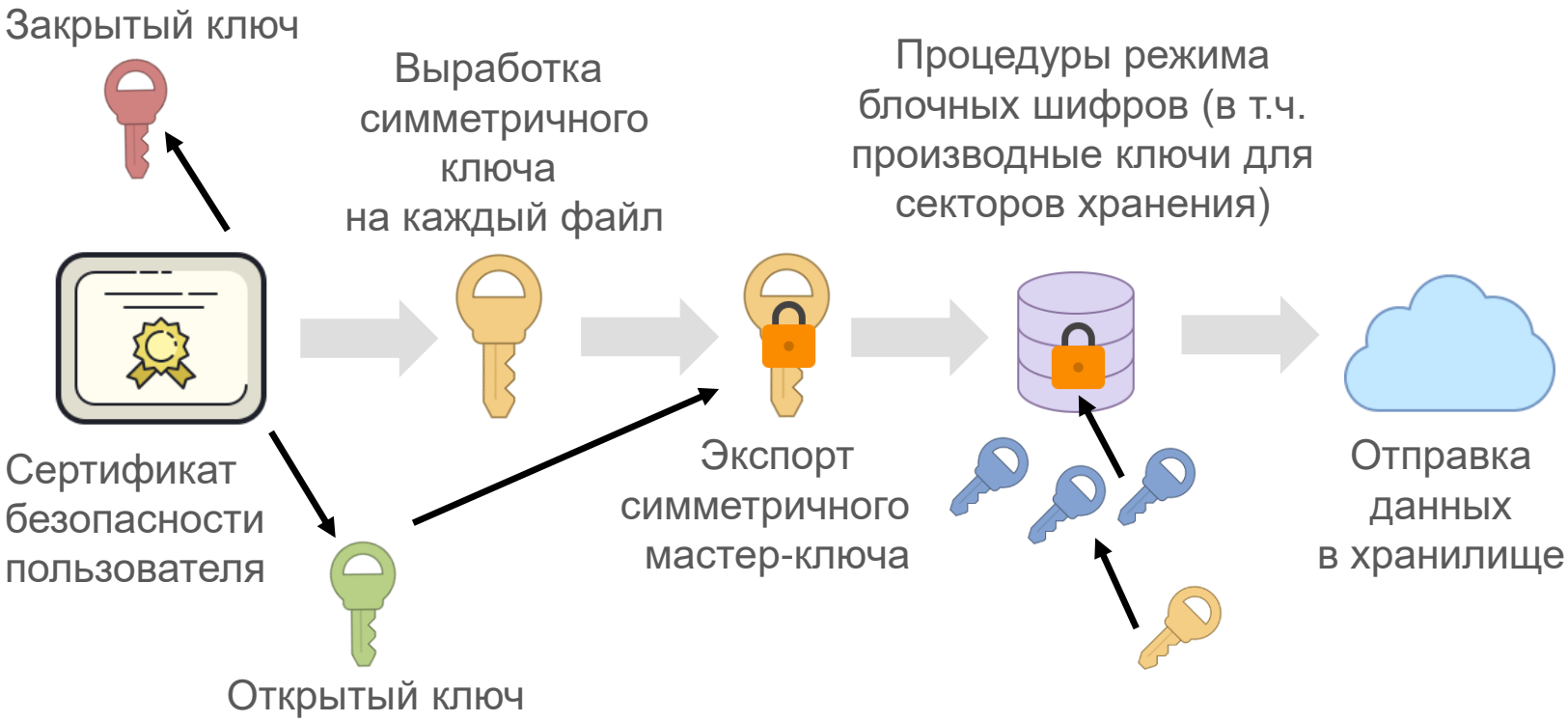
>>>Request (исходный)

```
PUT /calendars/events HTTP/1.1
Host: www.example.com
Content-Type: text/calendar
Content-Length: xxxx

BEGIN:VCALENDAR
BEGIN:VEVENT
DTSTAMP:20060712T182145Z
DTSTART:20060714T170000Z
DTEND:20060715T040000Z
SUMMARY: Victory Day
DESCRIPTION: Military parade
LOCATION: Moscow
END:VEVENT
END:VCALENDAR
```

>>>Request (измененный)

```
PUT /calendars/events HTTP/1.1
Host: www.example.com
Content-Type: text/calendar
Content-Length: xxxx

BEGIN:VCALENDAR
BEGIN:VEVENT
DTSTAMP:20060712T182145Z
DTSTART:20060714T170000Z
DTEND:20060715T040000Z
SUMMARY: <Криптотекст>
DESCRIPTION: <Криптотекст>
LOCATION: <Криптотекст>
END:VEVENT
END:VCALENDAR
```

ГИБРИДНАЯ КРИПТОГРАФИЧЕСКАЯ СХЕМА



РусКрипто

ХРАНЕНИЕ ПАРАМЕТРОВ ШИФРОВАНИЯ ОБЪЕКТА В ОБЛАКЕ

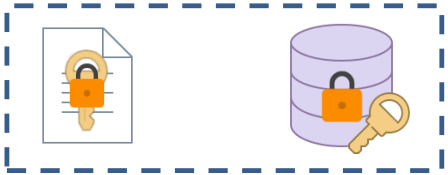
РусКрипто

Для расшифрования данных необходимо также сохранить (локально/на облаке) следующие криптографические параметры:

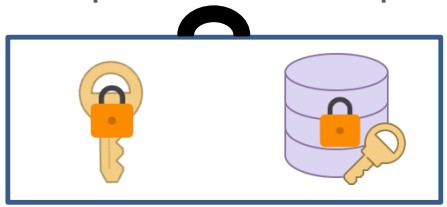
- алгоритм и режим шифрования;
- вектор инициализации;
- зашифрованный ключевой блоб;
- тег аутентификации (для AEAD-режимов шифрования).

Существует три способа хранения параметров шифрования на облаке: метаданные, общий файл-контейнер и отдельный файл-контейнер.

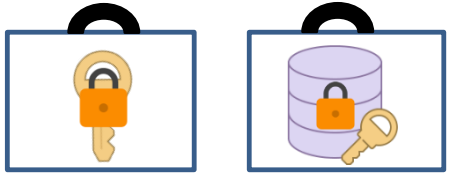
Метаданные объекта



Общий файл-контейнер



Отдельный файл-контейнер



ФОРМАТ КОНТЕЙНЕРА С ПАРАМЕТРАМИ ШИФРОВАНИЯ ДЛЯ ФАЙЛОВЫХ ХРАНИЛИЩ

РусКрипто

- “x-amz-cek-alg”: алгоритм и режим шифрования;
- “x-amz-iv”: вектор инициализации;
- “x-amz-key-v2”: зашифрованный ключевой блоб;
- “x-amz-key-dupl-count”: число дубликатов ключа;
- “x-amz-key-dupl-1”: 1-ый дубликат ключа шифрования объекта;
- "x-amz-tag-len": длина тега аутентификации (AEAD-режимы)


```
{
  "x-amz-cek-alg":"GOST_M/ECB",
  "x-amz-iv":"tWYAAOsjAAA=",
  "x-amz-key-dupl-count":“1",
  "x-amz-key-v2":"HAAAAAoAAAAEAAAA
AQAAAEgAAAALAgAAMGYAAFQGAAA
eNwAAMFkAAJoIAACrYAAA+G8AAEBc
AADMZgAAVAYAAB43AAAwWQAAmgg
AAKtgAAD4bwAAQFwAAMxmAAB0aW
suc3RhbmlzbGF2QGNyeXB0b3NvZnQu
cnUARXhTYW1wbGUxAGFueQAAAAA=",
  "x-amz-key-dupl-1":"gAAQTAAtW…AAAA=",
  "x-amz-tag-len":"0",
  "x-amz-wrap-alg":"csp“
}
```

ФОРМАТ ЗАЩИЩЕННОГО КОНТЕЙНЕРА ДЛЯ ПРОТОКОЛА CALDAV

РусКрипто

Защищенные данные представляют собой JSON-объект, содержащий как сами данные (поле “x-amz-encrypted-content”), так и параметры шифрования, необходимые для выполнения обратных криптографических преобразований.

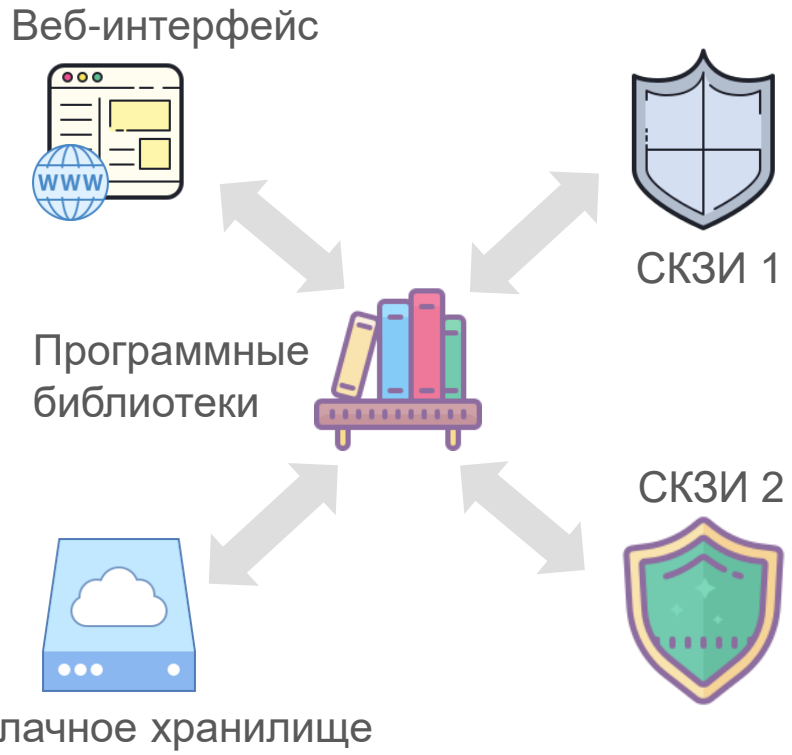
```
PUT /calendars …
…
BEGIN:VCALENDAR
BEGIN:VEVENT
…
SUMMARY: <…>
…
END:VEVENT
END:VCALENDAR
```

```
{
  "x-amz-cek-alg":"GOST_M/ECB",
  "x-amz-iv":"tWYAAOsjAAA=",
  "x-amz-key-dupl-count":“1",
  "x-amz-key-v2":"AAQAAMAAALA…AAAA=",
  "x-amz-key-dupl-1":"gAAQTAAtW…AAAA=",
  "x-amz-tag-len":"0",
  "x-amz-encrypted-content":"+Xr/F…Sd+A==“,
  "x-amz-wrap-alg":"csp“
}
```

МАКЕТ ПРОГРАММНО-ТЕХНИЧЕСКОГО РЕШЕНИЯ ПО ЗАЩИТЕ ДАННЫХ В ОБЛАКАХ

РусКрипто

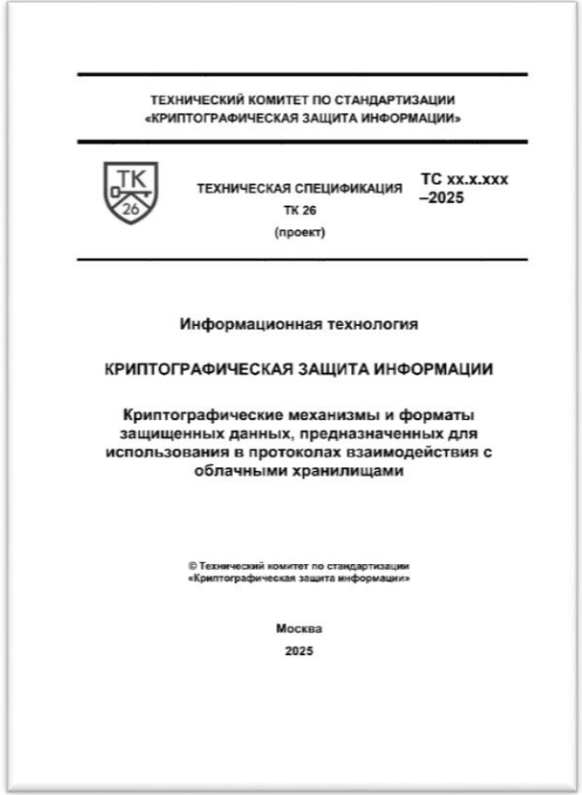
Обеспечение защищенного доступа к облачным хранилищам практически проверено с использованием серийных СКЗИ «QP Криптофон», «КриптоПро CSP», а также экспериментальных образцов с новыми режимами блочных шифров CTR-ACPKM, MGM2, XEH и др.



СТАНДАРТИЗАЦИЯ

РусКрипто

- Для эффективной работы механизмов криптографической защиты данных в облаках требуется стандартизация технических спецификаций к прикладным протоколам и интерфейсам, используемым для взаимодействия с облачными хранилищами данных.
- Разработка такого документа национальной системы стандартизации включена в план работ ТК 26 на 2025 год.



ТЕХНИЧЕСКИЙ КОМИТЕТ ПО СТАНДАРТИЗАЦИИ
«КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ
ТК 26
(проект)

ТС xx.x.xxx
–2025

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические механизмы и форматы защищенных данных, предназначенных для использования в протоколах взаимодействия с облачными хранилищами

Москва
2025

РусКрипто

СПАСИБО
ЗА ВНИМАНИЕ