Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

Шифрование носителей информации. Режим DEC.

Дмитрий Богданов, НИЯУ МИФИ
Владислав Ноздрунов, ТК 26

Модель носителя информации

Под **носителем информации** S с блочно-ориентированной структурой будем понимать занумерованную совокупность секторов одинаковой длины s:

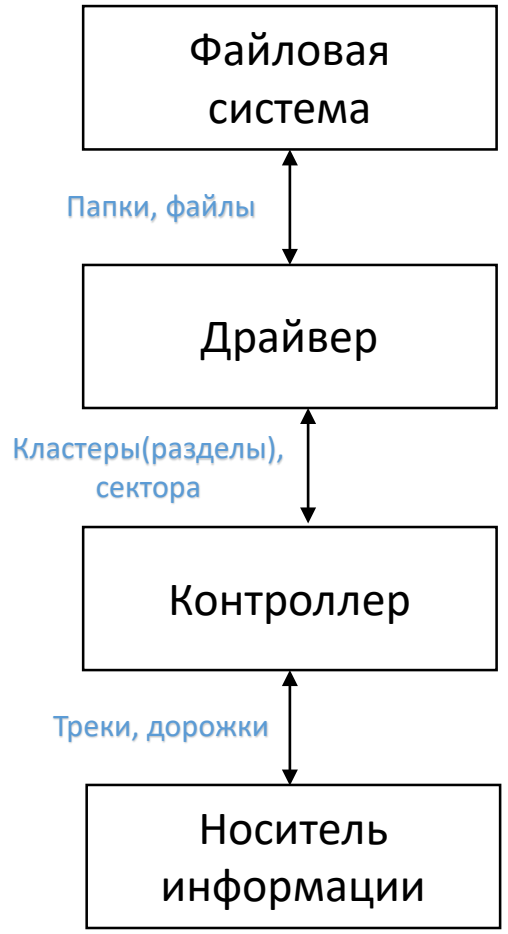
$$S = \{S_1, S_2, \dots, S_v\}, S_i \in V_s, v, s \in \mathbb{N}, i = 1,2, \dots, v.$$

Сектор является минимально адресуемой ячейкой носителя информации.

Типовой размер сектора на н.в. 4096 и 32768 бит.

Оценка максимальной емкости в н.в. составляет порядка 2^{62} бит.

Далее будем считать, что носитель состоит из 2^w разделов по 2^s секторов.



Особенности при шифровании

- Кластерная структура ⇒ прямой доступ к сектору
  иначе ⇒ существенные задержки в работе.
  - отказ от «тотального» шифрования;
  - преобразования для различных секторов должны отличаться ⇒ IV?
- Выработка и хранение векторов инициализации (IV / nonce)
  - Где хранить? (доп. место? потери на носителе?)
  - Как хранить? (replay атаки?)

⇒ IV = № сектора

⇓

Разные ключи для секторов, двухпроходные схемы, Tweak

Сценарии атак

- Кража
  - конфиденциальность
- Наблюдение
  - конфиденциальность
- Кража с возвращением
  - Конфиденциальность & целостность
- Активные атаки
  - Конфиденциальность & целостность

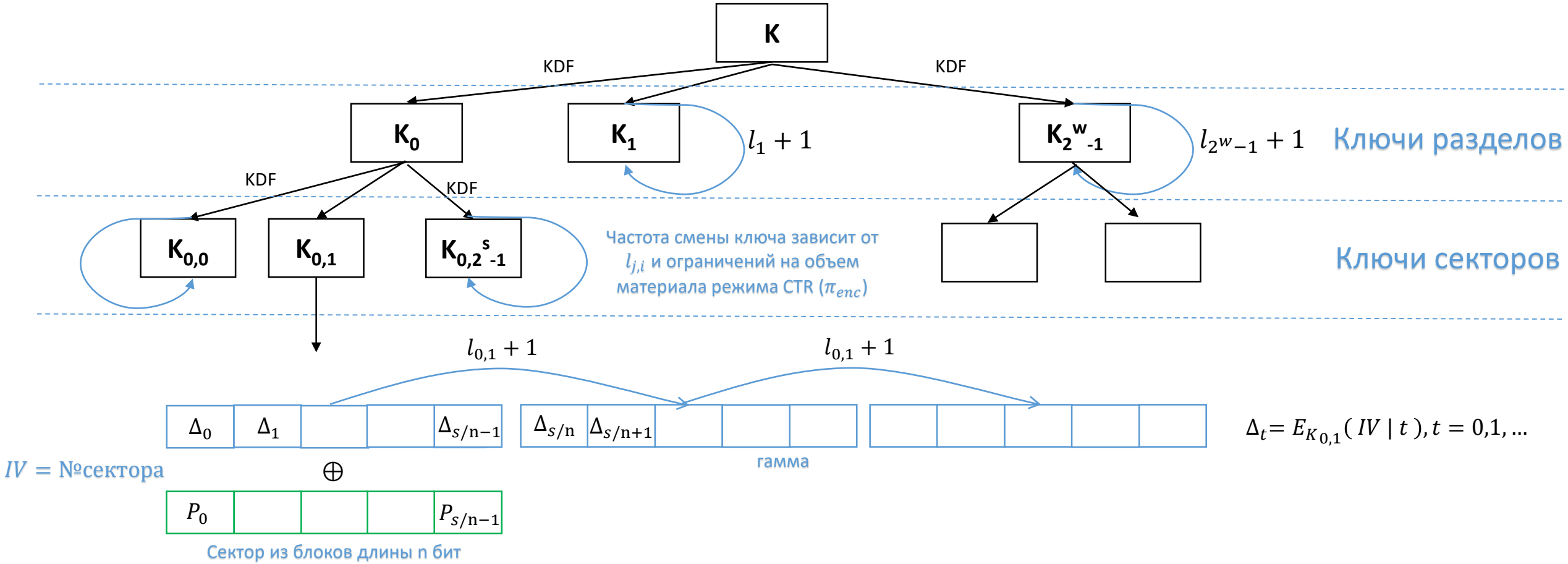
Возможности противника в сценарии наблюдения

- Имеет доступ для чтения данных с контроллера, т.е. видит шифртексты ⇒ *контроль объема материала обр. на ключе*

Максимизация возможностей:

- Имеет возможность запросить зашифрование произвольных данных, при этом область записи может определяться как устройством шифрования так и противником;
- Имеет возможность запросить расшифрование некоторого фиксированного сектора носителя информации (сектор противника).

DEC – Disk Encryption with CTR and KDF



KDF – P 1323565.1.022-2018

$l_j, l_{j,i} \in V_{n/2}$, -параметры для учета количества обработанного материала, n – размер блочного шифра.

Об объемах

Необходимо дополнительно хранить счетчики $l_i, l_{j,i} \in V_{n/2}$.

В таблицах ниже представлен объем информации, необходимый для функционирования предложенного режима от общего объема защищаемого носителя информации в процентах:

n/s	4096	32768
64	1,6%	0,2%
128	3,2%	0,4%

В каждом разделе ровно один сектор

n/s	4096	32768
64	0,8%	0,1%
128	1,6%	0,2%

В каждом разделе по 6 и более секторов

Об объемах

Необходимо дополнительно хранить счетчики $l_i, l_{j,i} \in V_{n/2}$.

Оценка сверху количества дополнительно хранимой информации для носителя информации объемом в 1 Tb.

n/s	**4096**	**32768**
64	9 Gb	2 Gb
128	17 Gb	3 Gb

В каждом разделе ровно один сектор

Вопросы

Контактная информация

Электронная почта:

Nozdrunov_vi@tc26.ru

Сайт:

www.tc26.ru