ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

КОД безопасности

2024 CTCRYPT

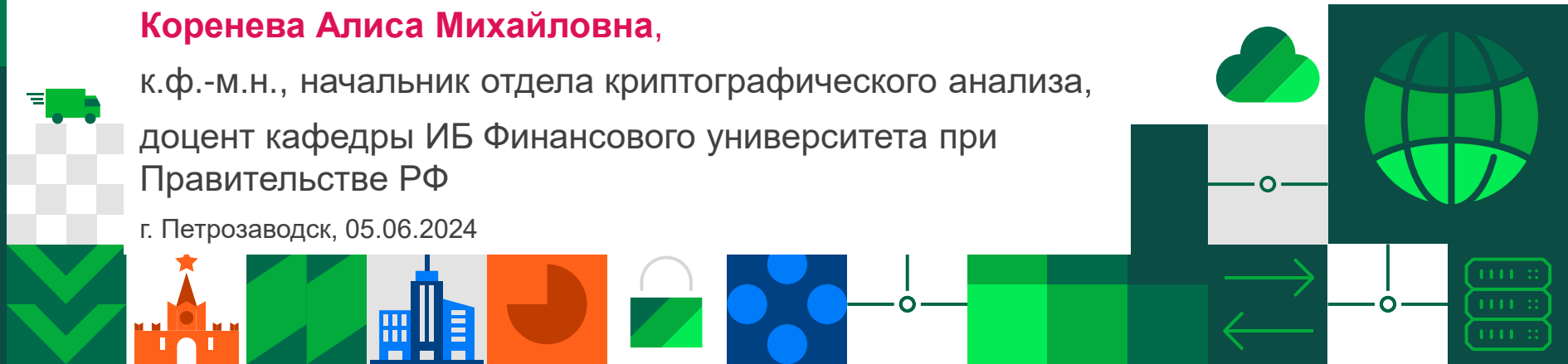
О некоторых вопросах генерации «случайных» чисел в криптографии

Коренева Алиса Михайловна,

к.ф.-м.н., начальник отдела криптографического анализа,

доцент кафедры ИБ Финансового университета при Правительстве РФ

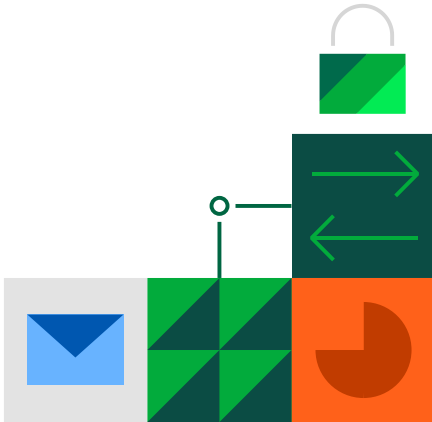
г. Петрозаводск, 05.06.2024



КОД безопасности

Содержание

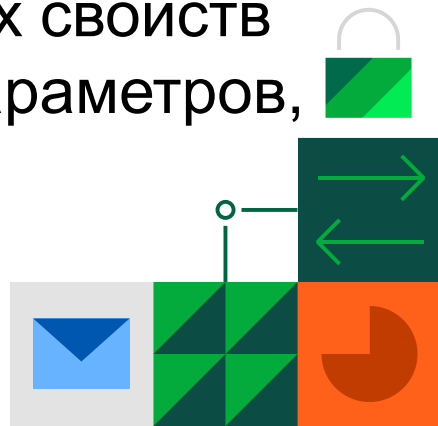
1. Что такое «случайность»?
2. Где «случайные» числа в криптографии?
3. Как получают криптографические ключи?



КОД безопасности

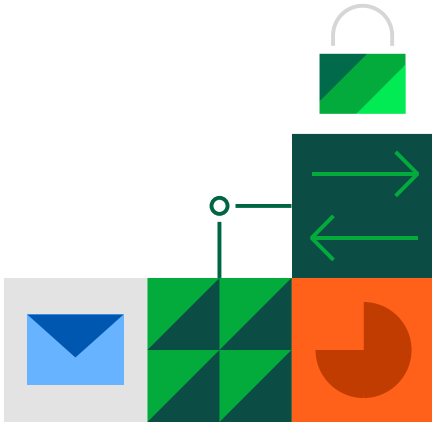
За пределами доклада

1. Математический фундамент
2. Конкретные схемы и реализации генераторов псевдослучайных последовательностей
3. Инструменты для проверки статистических свойств последовательностей (критерии, выбор параметров, готовые решения)



КОД безопасности

Содержание



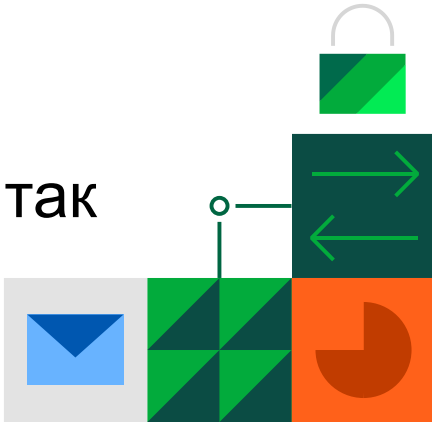
КОД безопасности

Введение

Специалисты по защите информации знают:

- ✓ защищённость информационных систем зависит от «криптографического» качества используемых в них ключей и сопутствующих параметров.

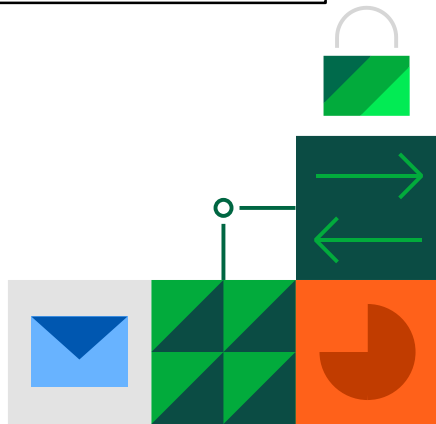
Одно из таких «криптографических» качеств – так называемая «случайность»



КОД безопасности

Вывод о случайности

Подходов много: есть удачные, есть не очень.
А в криптографии так вообще по своему.



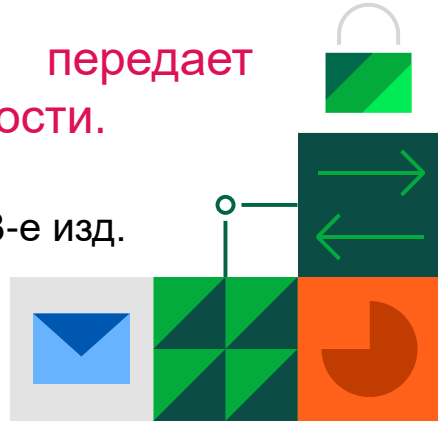
КОД безопасности

Случайная последовательность

Д. Г. Лемер (1951): «Случайная последовательность является смутным понятием, олицетворяющим идею последовательности, в которой каждый член является непредсказуемым для непосвященных и значения которой проходят определенное количество проверок, традиционных у статистиков и отчасти зависящих от пользователей, которым предложена последовательность».

Определение не является математически строгим, но передает некоторое интуитивное понимание случайной последовательности.

Кнут Д.Э. Искусство программирования, т. 2. Получисленные алгоритмы, 3-е изд.



КОД безопасности

Случайная последовательность

Д. Н. Франклин (1962): «Последовательность случайна, если она обладает ***любыми свойствами***, присущими всем бесчисленным последовательностям независимых выборок случайных равномерно распределенных величин».

Не вполне точное определение, приводящее в итоге к выводу, что подобных последовательностей не существует.

Кнут Д.Э. Искусство программирования, т. 2. Получисленные алгоритмы, 3-е изд.

КОД безопасности

Случайная последовательность

Определение R5. b−ичная последовательность называется случайной, если каждая бесконечная подпоследовательность, определенная исчислимым правилом подпоследовательностей, является 1-распределенной (равнораспределенной).

Определение R6. b−ичную последовательность $\langle X_n \rangle$ называют случайной, если для каждого эффективного алгоритма, точно определяющего бесконечную последовательность различных … чисел $\langle s_n \rangle$ …, подпоследовательность $\langle X_{s_n} \rangle$ … является случайной в смысле определения R5.

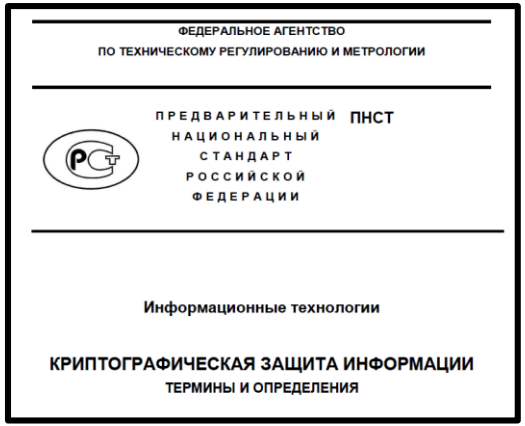
Д. Э. Кнут в 1966 г. утверждал, что определение R6 «удовлетворяет всем *разумным философским* требованиям случайности».

Кнут Д.Э. Искусство программирования, т. 2. Получисленные алгоритмы, 3-е изд.

КОД безопасности

А как у нас? (в криптографии)

ПНСТ 799-2022 «Информационные технологии. Криптографическая защита информации. **Термины и определения»:**



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ

Информационные технологии

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

А.2.9 **идеальная случайная последовательность** (ideal random sequence): Последовательность независимых случайных величин, имеющих равновероятное распределение на заданном конечном алфавите.

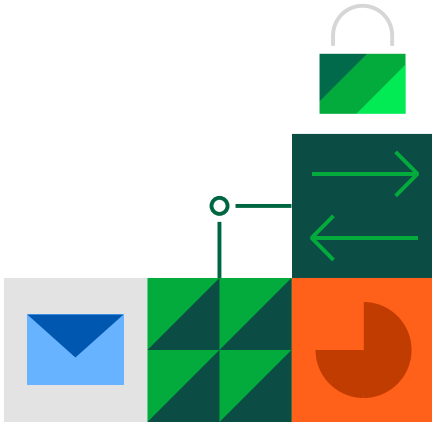
А.2.10 **псевдослучайная последовательность** (pseudo-random sequence): Последовательность, порожденная детерминированным устройством или программой, обладающая свойствами, близкими к свойствам типичных реализаций идеальной случайной последовательности.

Примечание – Адаптировано из ИСО/МЭК 18031:2011, статья 3.26 [18].

А.2.14 **случайное число** (random number): Случайная величина, имеющая равновероятное распределение на заданном конечном алфавите.

КОД безопасности

Содержание



КОД безопасности

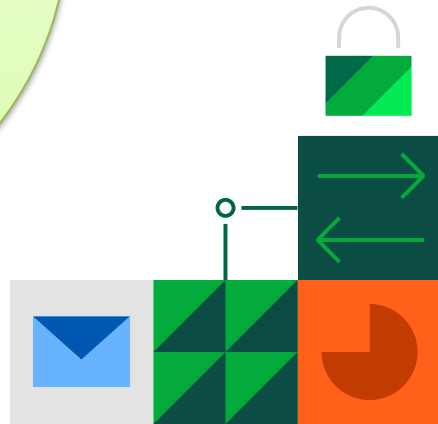
«Случайные» числа в криптографии

- Ключи для криптографических механизмов

Ключи

- Сопутствующая криптографическая информация:
  - ✓ Синхропосылка (IV)
  - ✓ Соль (salt)
  - ✓ Зерно (seed)
  - ✓ Маска (mask)
  - ✓ Нонс (nonce)
  - ✓ UKM
  - ✓ …

НЕ ключи



КОД безопасности

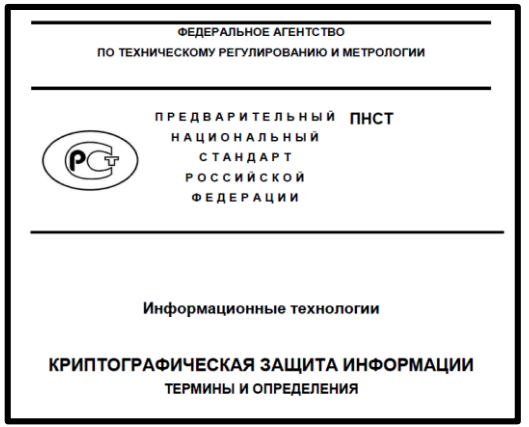
Криптографический ключ

ПНСТ 799-2022 «Информационные технологии. Криптографическая защита информации. **Термины и определения»:**

4 **криптографический ключ:** Изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование.

[ГОСТ Р 34.12 – 2015, пункт 2.1.8]

Примечание - См. также ИСО/МЭК 18033–1:2021, статья 3.16 [15], ГОСТ Р 56205-2017 IEC/TS 62443-1-1, статья 3.2.35; Р1323565.1.012, статьи 3.1.17, 3.1.19, 3.1.25, 3.1.27, 3.1.36, 3.1.37, 3.1.41.


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ

Информационные технологии

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

КОД безопасности

Синхропосылка

МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ (МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION (ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 34.13— 2018

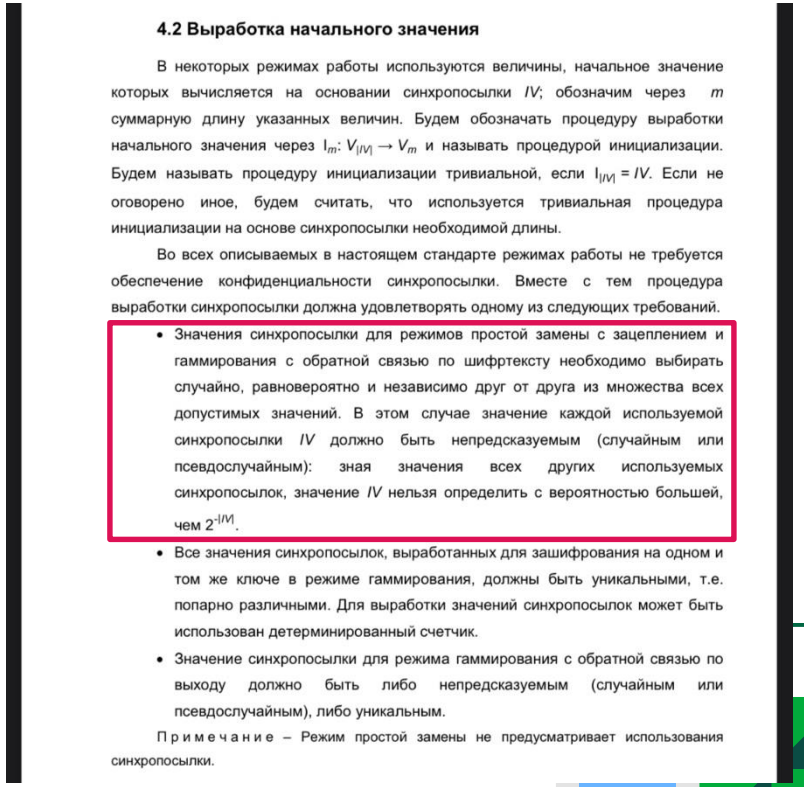
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Режимы работы блочных шифров

Издание официальное

- **Режимы работы блочных шифров:** ГОСТ 34.13-2018



4.2 Выработка начального значения

В некоторых режимах работы используются величины, начальное значение которых вычисляется на основании синхропосылки IV; обозначим через m суммарную длину указанных величин. Будем обозначать процедуру выработки начального значения через I_m: $V_{|IV|} \to V_m$ и называть процедурой инициализации. Будем называть процедуру инициализации тривиальной, если $I_{|IV|} = IV$. Если не оговорено иное, будем считать, что используется тривиальная процедура инициализации на основе синхропосылки необходимой длины.

Во всех описываемых в настоящем стандарте режимах работы не требуется обеспечение конфиденциальности синхропосылки. Вместе с тем процедура выработки синхропосылки должна удовлетворять одному из следующих требований.

- Значения синхропосылки для режимов простой замены с зацеплением и гаммирования с обратной связью по шифртексту необходимо выбирать случайно, равновероятно и независимо друг от друга из множества всех допустимых значений. В этом случае значение каждой используемой синхропосылки IV должно быть непредсказуемым (случайным или псевдослучайным): зная значения всех других используемых синхропосылок, значение IV нельзя определить с вероятностью большей, чем $2^{-|IV|}$.
- Все значения синхропосылок, выработанных для зашифрования на одном и том же ключе в режиме гаммирования, должны быть уникальными, т.е. попарно различными. Для выработки значений синхропосылок может быть использован детерминированный счетчик.
- Значение синхропосылки для режима гаммирования с обратной связью по выходу должно быть либо непредсказуемым (случайным или псевдослучайным), либо уникальным.

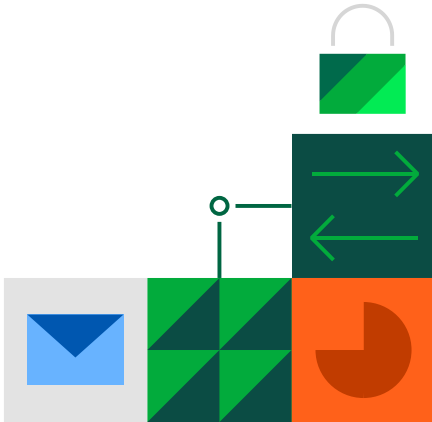
Примечание – Режим простой замены не предусматривает использования синхропосылки.

КОД безопасности

Виды ключей
(по типу криптосистемы)

- Секретный ключ для симметричной криптосистемы

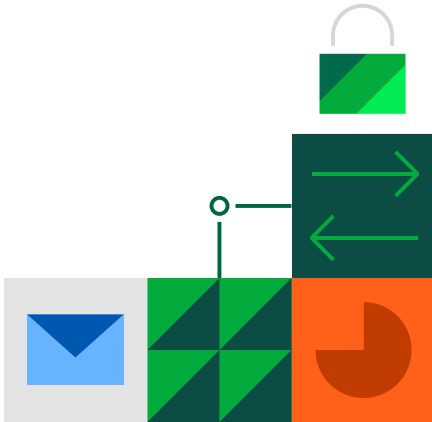
- Ключевая пара для асимметричной криптосистемы (закрытый и открытый ключ)



КОД безопасности

Виды ключей
(по назначению)

- ключ для шифрования данных на носителе (диск, флэшка)
- ключ для шифрования сетевого трафика
- ключ для проверки целостности данных
- ключ для формирования электронной подписи
- ключ для проверки электронной подписи
- ключ для шифрования других ключей
- ключ для вычисления имитовставки
- и другие



КОД безопасности

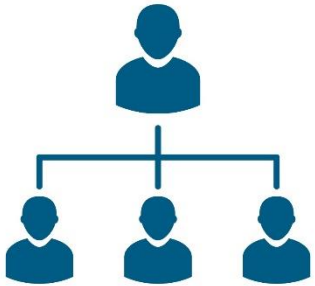
Виды ключей
(по времени жизни)

- Постоянные (долговременные)
- Сессионные (сеансовые)
- Одноразовые
- Эфемерные

КОД безопасности

Виды ключей
(по иерархии)

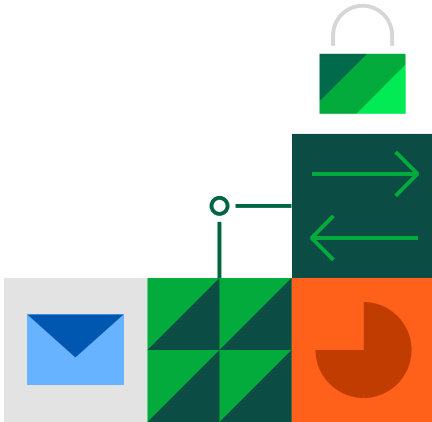
- Мастер-ключ
- Главный ключ
- Производный ключ



КОД безопасности

Содержание

1. Что такое случайные числа?
2. Где «случайные» числа в криптографии?
3. Как получают криптографические ключи?



КОД безопасности

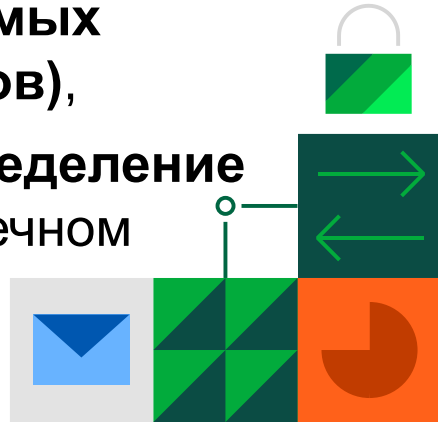
Идеальный ключ

Криптографические свойства **наилучшие**, если ключ похож на «**идеальную случайную последовательность» (ИСП)**

Математическая модель ИСП:

последовательность **независимых случайных величин (символов)**,

имеющих **равномерное распределение** вероятностей на заданном конечном алфавите.



КОД безопасности

Главная проблема

Детерминированный алгоритм НЕ может вырабатывать истинно случайные числа.

Любой «арифметический» генератор рано или поздно зацикливается.

КОД безопасности

Реальность

Итак, **ключ** – это последовательность. **Ключ** должен быть похож на «идеальную случайную последовательность»

↓

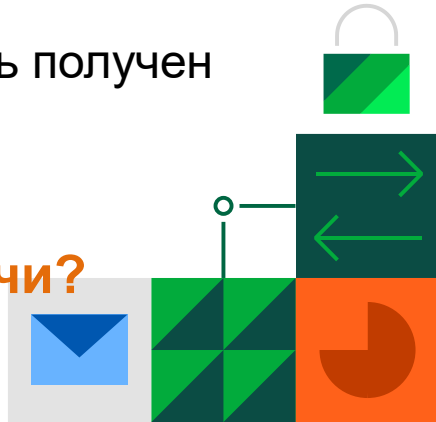
Чтобы получить идеальный ключ нужно «уметь» вырабатывать «случайную» последовательность.

↓

Доказано[*], что истинно случайный ключ **не может** быть получен алгоритмически.

↓

Что делать? Как получать «хорошие» ключи?



[*] – Herring C., Palmore J.I. Random Number Generators are Chaotic, 1995.

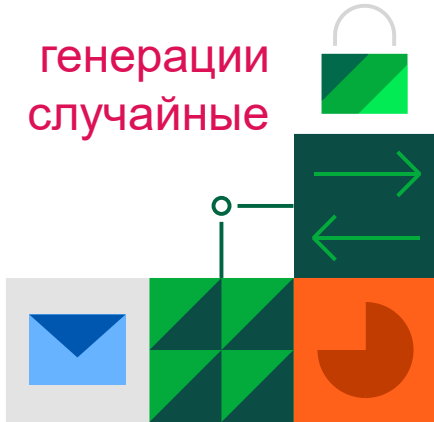
КОД безопасности

Вспомним, что

В криптографии…

Случайная идеальная последовательность является реализацией последовательности независимых случайных величин, имеющих равномерное распределение вероятностей на заданном конечном алфавите.

Программные генераторы предназначены для генерации псевдослучайных последовательностей, *имитирующих* случайные идеальные последовательности.



Фомичев В.М. Методы дискретной математики в криптологии.

КОД безопасности

Генератор случайных чисел

А.2.15 **генератор случайных чисел** (random number generator): Устройство или программный модуль, вырабатывающие последовательность случайных или псевдослучайных чисел.

Примечания

1 Существует два основных класса генераторов: детерминированные и недетерминированные. Первые основаны на детерминированных алгоритмах, которые вырабатывают последовательность бит из секретного начального заполнения (см. А.2.13). При использовании одного и того же секретного начального заполнения генератор воспроизводит одну и ту же последовательность. Недетерминированный генератор вырабатывает последовательность случайных чисел, которая зависит от некоторого непредсказуемого физического или биологического источника, и поэтому невоспроизводима.

ПНСТ 799-2022 «Информационные технологии. Криптографическая защита информации. Термины и определения»

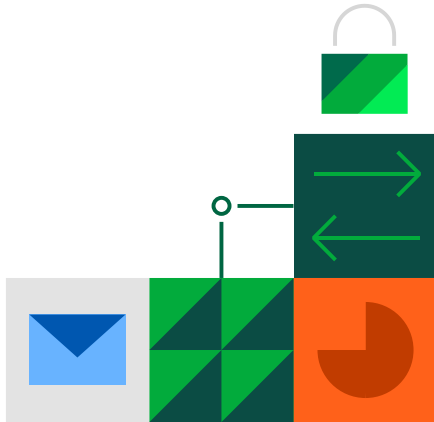
КОД безопасности

О важности начального заполнения

- Генерируемая любым программным методом последовательность зависит от выбора стартового числа (seed)
- При разных значениях seed – разные последовательности случайных чисел.

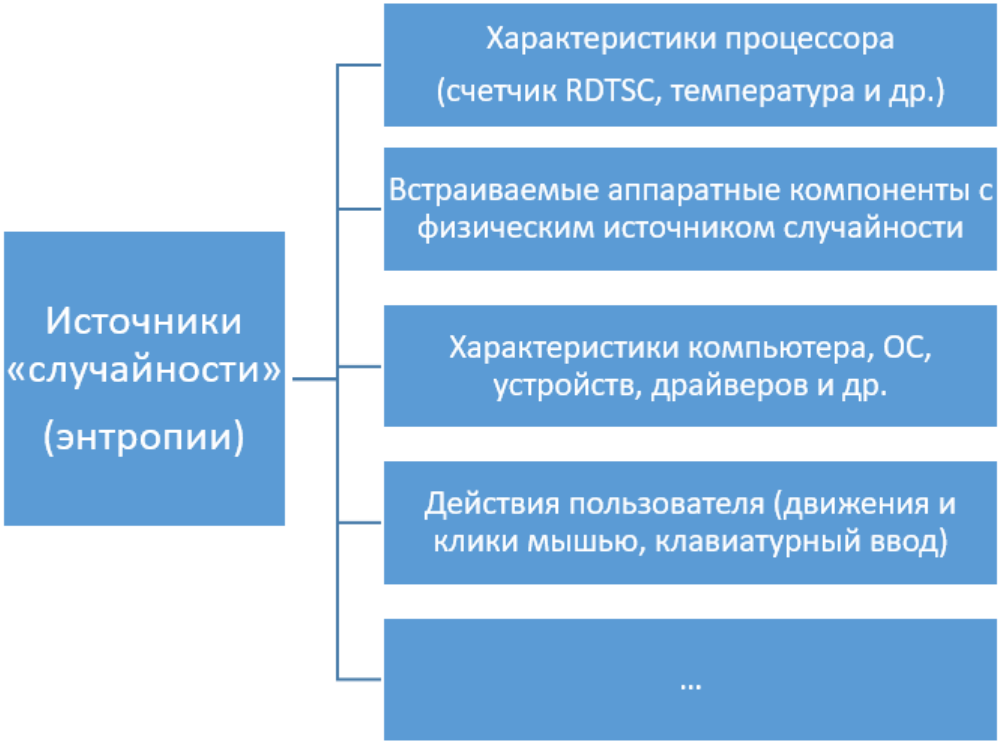
Необходимо получить «случайный» seed, с помощью которого будет генерироваться псевдослучайная последовательность.

«Повтор ключа – главное преступление в криптографии!» (с)



КОД безопасности

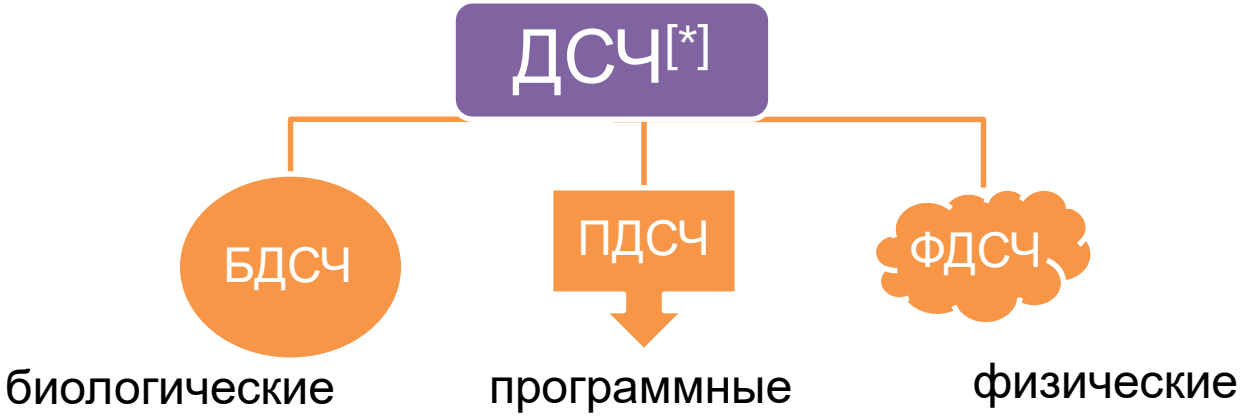
Откуда брать «случайность»?



КОД безопасности

Какие бывают ДСЧ

Датчик случайных чисел – составная часть средства криптографической защиты информации.



[*] – Р 1323565.1.012-2017 «Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации», стр. 13.

КОД безопасности

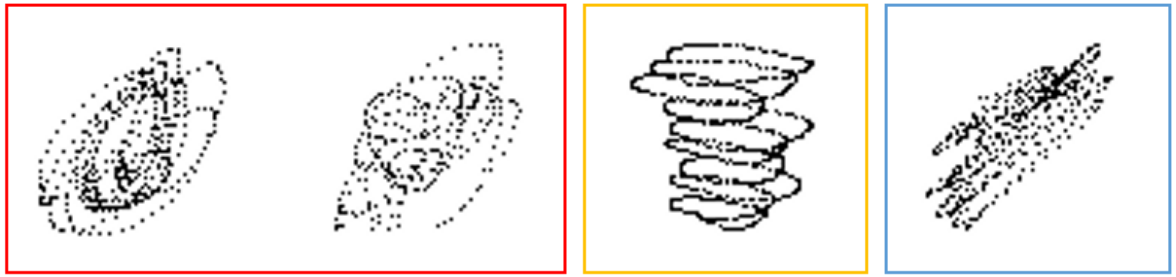
БиоДСЧ

- На основе клавиатуры
- На основе мыши:
  - неосмысленные (произвольные) действия
  - осмысленные действия

КОД безопасности

БиоДСЧ

При заполнении пула энтропии с помощью движений мышью возникает сходство между движениями мыши для одного и того же пользователя[*].



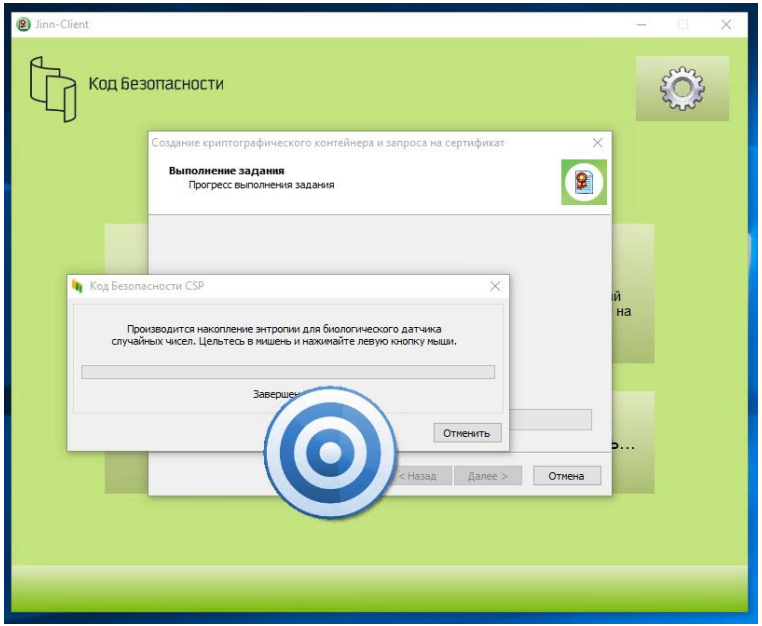
Пользователь A | Пользователь B | Пользователь C

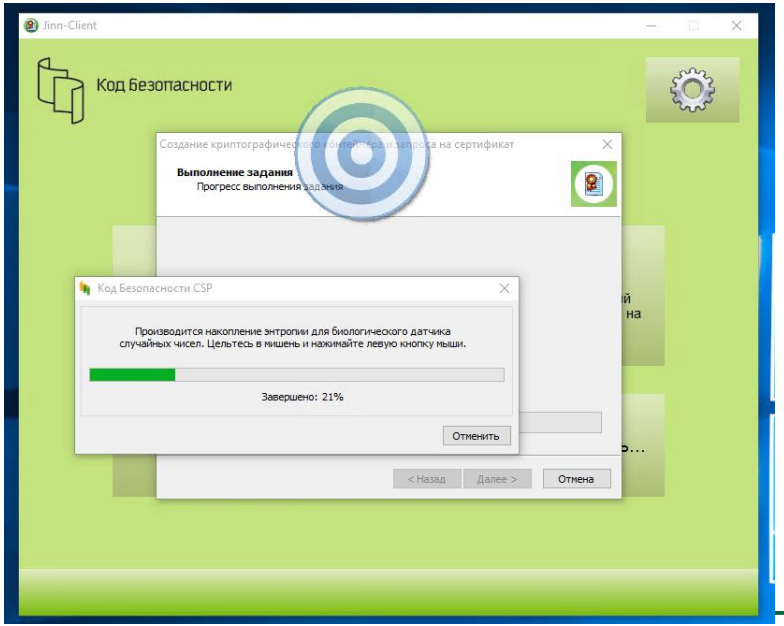
Промежуточные движения между началом движения мыши и ее замедлением обычно являются достаточно предсказуемыми [**]. Возможно осуществление локальной атаки злоумышленником

[*] – Hu, Liao, Wong, Zhou. A true random number generator based on mouse movement and chaotic cryptography, 2009.
[**] – Viega J., Messier M. Secure Programming Cookbook for C and C++. Recipes for Cryptography, Authentication, Input Validation & More, 2009

КОД безопасности

БиоДСЧ





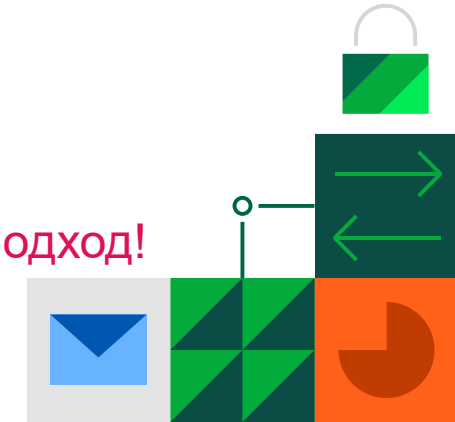
КОД безопасности

ФДСЧ

Примеры физических процессов, на основе которых может функционировать ФДСЧ:

- тепловой шум;
- лавинный пробой;
- время между приёмом фотонов;
- нестабильность работы физических элементов.

К анализу каждого процесса применяется индивидуальный подход!

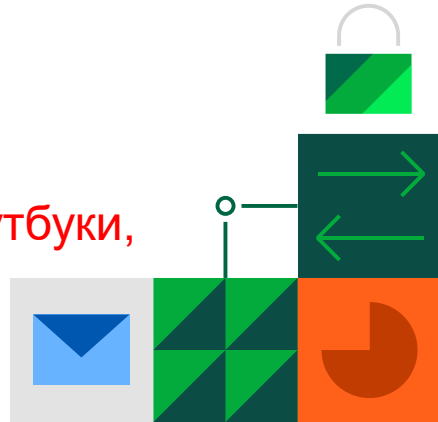


КОД безопасности

ФДСЧ

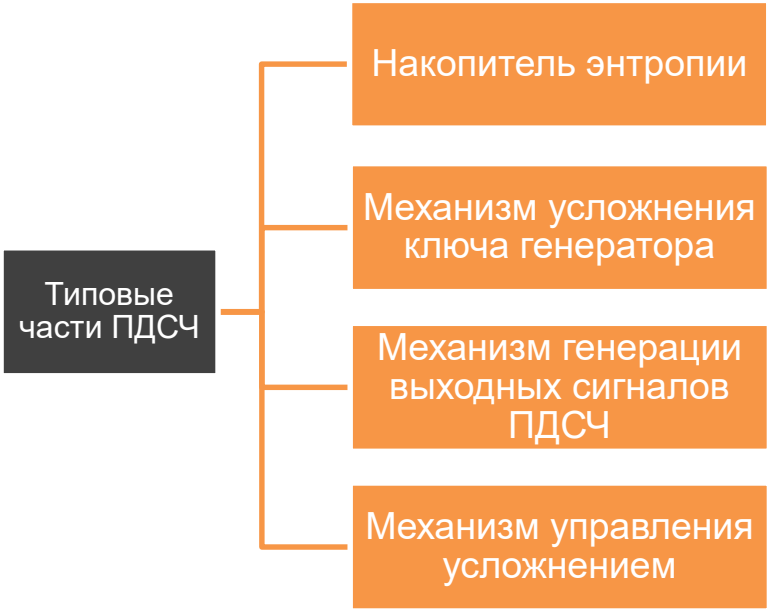
- Аппаратные ДСЧ на основе шумовых диодов
- Квантовые ДСЧ
- ДСЧ на основе кольцевых осцилляторов

В ряде случаев ФДСЧ имеют трудности с встраиванием в ноутбуки, планшеты, смартфоны



КОД безопасности

ПДСЧ



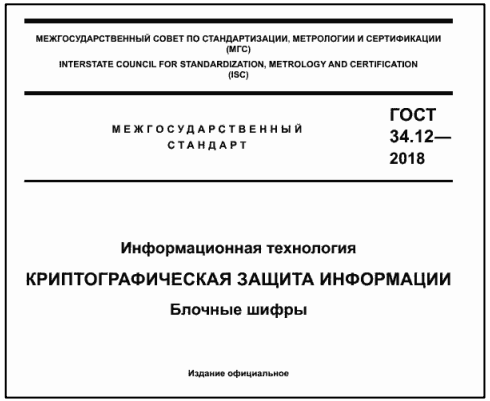
Для реализации модуля ПДСЧ могут использоваться [*]:

- функция хэширования
- блочный шифр

[*] Л.Ю. Щербаков, А.В. Домашев, Прикладная криптография. Использование и синтез криптографических интерфейсов

КОД безопасности

РОССИЙСКИЕ КРИПТОСТАНДАРТЫ


МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ (МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION (ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 34.12— 2018

Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Блочные шифры

Издание официальное

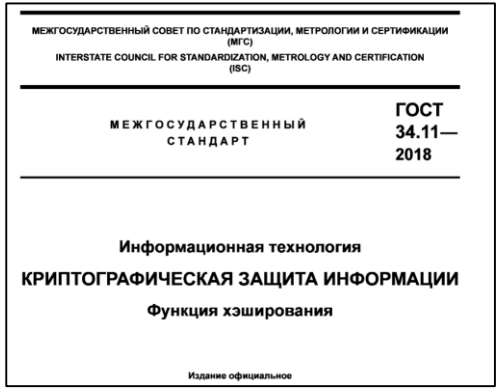

МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ (МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION (ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 34.13— 2018

Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Режимы работы блочных шифров

Издание официальное


МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ (МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION (ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 34.11— 2018

Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Функция хэширования

Издание официальное

- **Блочные шифры:** ГОСТ 34.12-2018 (“Магма” и “Кузнечик”)
- **Режимы работы блочных шифров:** ГОСТ 34.13-2018
- **Функция хэширования:** ГОСТ 34.11-2018

КОД безопасности

Спасибо за внимание!

a.koreneva@securitycode.ru

https://www.securitycode.ru/

Приложение А

Как проверять ДСЧ. Что говорят документы?

1) На этапе разработки ДСЧ необходимо провести построение, обоснование и анализ теоретико-вероятностной модели, а также необходимо провести экспериментальную проверка соответствия указанной модели реализации.
2) На этапе работы должна осуществляться проверка статистического качества выходной последовательности ДСЧ. Данная проверка должна осуществляться в ходе регламентных (периодических, в том числе в автоматическом режиме) проверок датчика случайных чисел (регламентный контроль) и в автоматическом режиме в процессе функционирования СКЗИ (динамический контроль).

"Требования к средствам криптографической защиты информации в платежных устройствах с терминальным ядром, серверных компонентах платежных систем (HSM модулях), платежных картах и иных технических средствах информационной инфраструктуры платежной системы, используемых при осуществлении переводов денежных средств, указанных в пункте 2.20 положения Банка России от 9 июня 2012 г. N 382-П" (утв. ФСБ России 24.01.2020, 28.02.2020 N ФТ-56-3/32)

Теоретико-вероятностная модель (ТВМ)

ТВМ – это модель, основанная на применении статистических и теоретико-вероятностных методов по отношению к повторяющимся феноменам, в которой обеспечивается учет случайных факторов в процессе функционирования системы. Модель содержит описание вероятностных характеристик случайных процессов и дальнейшее их сопоставление с результатами измерений.

- Теоретико-вероятностная модель БиоДСЧ – описание вероятностных характеристик операций, выполняемых для формирования выходной последовательности БиоДСЧ [Тыщенко Н.С. «О подходах к обоснованию качеств биологических датчиков случайных чисел»].
- Теоретико-вероятностная модель ФДСЧ – описание и вероятностные характеристики сигнала случайного процесса, генерируемого недетерминируемой физической системой, а также методов его преобразования.
- Теоретико-вероятностная модель ПДСЧ – описание конечного автомата, преобразовывающего инициализирующую последовательность.

Экспериментальная проверка

1) Проверка соответствия получаемых данных теоретико-вероятностной модели.
2) Проверка правильной обработки данных.
3) Проверка соответствия реализации.
4) Проверка устойчивости по отношению к возможным изменениям внешних и внутренних условий.
5) Проверка статистических свойств выходной последовательности.