

УТВЕРЖДЕН

0230259.01428-01 30 01-ЛУ

ПРОГРАММНЫЙ ДАТЧИК ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Формуляр

0230259.01428-01 30 01

Листов 23

Инев. № подл.	Подп. и дата	Взам. Инев. №	Инев. № дубл.	Подп. и дата

2023

Литера О₁

СОДЕРЖАНИЕ

1. Основные параметры и технические характеристики	3
1.1. Общие указания по эксплуатации программного датчика псевдослучайных чисел и ведению формуляра	3
1.2. Общие сведения о ПДСЧ	3
1.3. Основные технические характеристики и функции	3
1.4. Комплектность	4
1.4.1. Варианты поставки	4
1.4.2. Комплектность поставляемого изделия	4
1.4.3. Проверка целостности поставляемого изделия	5
1.5. Установка ПДСЧ	7
1.6. Сведения о хранении	7
1.7. Гарантийные обязательства	7
2. Сведения о состоянии ПДСЧ	8
3. Сведения о результатах проверки объекта	9
4. Сведения о рекламациях	10
5. Свидетельство о приемке ПДСЧ	11
6. Свидетельство об упаковке	12
7. Особые отметки	13
Приложение 1. Контрольные суммы компонентов программного обеспечения ПДСЧ	14
Приложение 2. Сведения о хранении	16
Приложение 3. Сведения о состоянии ПДСЧ	17
Приложение 4. Освидетельствование объектов специальными контрольными органами	19
Приложение 5. Учет предъявленных рекламаций	21
Перечень сокращений	22

1. ОСНОВНЫЕ ПАРАМЕТРЫ И ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

1.1. Общие указания по эксплуатации программного датчика псевдослучайных чисел и ведению формуляра

1.1.1. Данный формуляр является документом, удостоверяющим гарантированные предприятием-изготовителем основные характеристики программного датчика псевдослучайных чисел (далее – ПДСЧ), определяющим комплект поставки и содержащим сведения о состоянии ПДСЧ в процессе эксплуатации.

1.1.2. Для обеспечения функционирования ПДСЧ персонал должен быть ознакомлен с эксплуатационной документацией, приведенной в документе 0230259.01428-01 20 01 «Ведомость эксплуатационных документов».

1.1.3. Формуляр должен находиться в подразделении, ответственном за эксплуатацию ПДСЧ.

1.1.4. Все записи в формуляре производить от руки отчетливо и аккуратно. Подчистки, записи карандашом, смывающимися чернилами и незаверенные исправления не допускаются.

1.1.5. До начала опытной эксплуатации ПДСЧ должно быть завершено обучение, включая изучение эксплуатационной документации, всех должностных лиц и подразделений, которые будут эксплуатировать ПДСЧ.

1.2. Общие сведения о ПДСЧ

1.2.1. ПДСЧ предназначен для генерации последовательностей паролей, используемых в системах защиты информации.

ПДСЧ используется на объектах вычислительной техники, на которых осуществляется обработка информации, составляющей государственную тайну.

Особенности конкретного объекта вычислительной техники должны учитываться при настройке ПДСЧ во время его установки и эксплуатации на данном объекте.

1.2.2. Наименование изделия – Программный датчик псевдослучайных чисел.

1.2.3. Обозначение изделия – 0230259.01428-01.

1.2.4. Предприятие-изготовитель ПДСЧ – АО НИИ ЦПС.

1.3. Основные технические характеристики и функции

1.3.1. ПДСЧ функционирует на ЭВМ, работающих под управлением операционных систем (ОС) семейства Microsoft Windows (поддерживаются как 32-битные, так и 64-битные версии ОС), МСВС 3.0 (ФЛИР.80001-01 изменение № 13; ФЛИР.80001-12), МСВС 5.0 (ЦАВМ.11004-01), QNX 6.4.0, Эльбрус (ТВГИ.00316-10), Эльбрус-Д (ТВГИ.00950-01), Astra Linux Special Edition (РУСБ.10015-01 релиз «Смоленск» и РУСБ.10265-01 релиз «Ленинград») и ЗОСРВ «Нейтрино» (КПДА.10964-01, платформа x86).

1.3.2. ПДСЧ выполняет следующие функции:

- генерация последовательности паролей в соответствии с заданными параметрами;
- настройка параметров ПДСЧ;
- проверка корректности вводимых исходных данных;
- вывод массива паролей на экран и/или в файл;
- поддержка параметров командной строки;
- специальное преобразование файла паролей (ПДСЧ для ОС Windows);
- поддержка пользовательских библиотек специального преобразования (ПДСЧ для ОС Windows).

1.3.3. Эксплуатация программного изделия допустима только при соблюдении следующих условий:

- в прикладном и общем программном обеспечении не должно быть средств программирования и отладки;

[illegible]

1.4.3. Проверка целостности поставляемого изделия

1.4.3.1. Проверка целостности дистрибутива ПО ПДСЧ возможна в ОС Windows, MCBC 3.0/5.0, Эльбрус, Эльбрус-Д, Astra Linux, Нейтрино.

Расположение ПО ПДСЧ (при его наличии на дистрибутивном ЭН) приведено в таблице 2.

Таблица 2 – Расположение ПО ПДСЧ на дистрибутивном ЭН

ПО ПДСЧ	Расположение на дистрибутивном ЭН
ПО ПДСЧ для ОС Windows	ПДСЧ/Windows
ПО ПДСЧ для ОС MCBC 3.0	ПДСЧ/MCBC
ПО ПДСЧ для ОС MCBC 5.0	ПДСЧ/MCBC5
ПО ПДСЧ для ОС QNX	prcg_qnx
ПО ПДСЧ для ОС Эльбрус	ПДСЧ/Эльбрус
ПО ПДСЧ для ОС Эльбрус-Д	ПДСЧ/Эльбрус-Д
ПО ПДСЧ для ОС Astra Linux	ПДСЧ/AstraLinux
ПО ПДСЧ для ОС Astra Linux-Ленинград	ПДСЧ/AstraLinux-Ленинград
ПО ПДСЧ для ЗОСРВ Нейтрино	prcg_neutrino

1.4.3.2. Для проверки целостности дистрибутива ПО ПДСЧ в ОС Windows необходимо использовать программу расчета контрольных сумм – CHECKSUM.EXE, расположенную на дистрибутивном ЭН. Проверка осуществляется следующим образом:

- вставить дистрибутивный ЭН в привод компакт-дисков;
- в командной строке перейти в каталог дистрибутивного ЭН, выполнив следующие команды:

```
cd X:\
X:
```

где X: – буква диска, соответствующего используемому приводу компакт-дисков (например, E:);

- получить контрольные суммы ПДСЧ, выполнив следующие команды (для соответствующего варианта поставки, в случае поставки ПДСЧ для нескольких ОС необходимо выполнить команды для каждой из этих ОС):

1) для ОС Windows:

```
cd ПДСЧ\Windows
checksum\checksum.exe prcg.exe crypting.dll
cd ..\..
```

2) для ОС QNX:

```
cd prcg_qnx
checksum\checksum.exe prcg_qnx
cd ..
```

3) для ОС MCBC 3.0, MCBC 5.0, Эльбрус, Эльбрус-Д, Astra Linux, Нейтрино (вместо <каталог размещения> необходимо подставить каталог размещения ПО ПДСЧ на дистрибутивном ЭН в соответствии с таблицей 2, например, ПДСЧ/MCBC):

```
cd <каталог размещения>
checksum\checksum.exe prcg_lin
cd ..\..
```

Отображаемые контрольные суммы файлов должны соответствовать эталонным контрольным суммам (приложение 1, алгоритм CHECKSUM).

1.4.3.3. Для проверки целостности дистрибутива ПО ПДСЧ в ОС МСВС 3.0/5.0, Эльбрус, Эльбрус-Д, Astra Linux необходимо использовать встроенную в ОС программу расчета контрольных сумм – md5sum. Проверка осуществляется от имени суперпользователя следующим образом:

- вставить дистрибутивный ЭН в привод компакт-дисков;
- смонтировать дистрибутивный ЭН и перейти в каталог дистрибутива, выполнив в консоли следующие команды:

1) при проверке в ОС МСВС 3.0/5.0, Эльбрус:

```
mount /mnt/cdrom  
cd /mnt/cdrom
```

2) при проверке в ОС Эльбрус-Д:

```
mount /dev/sr0 /mnt/cdrom  
cd /mnt/cdrom
```

3) при проверке в ОС Astra Linux:

```
mount /dev/cdrom /media/cdrom -o utf8  
cd /media/cdrom
```

- получить контрольные суммы ПДСЧ, выполнив следующие команды (для соответствующего варианта поставки, в случае поставки ПДСЧ для нескольких ОС необходимо выполнить команды для каждой из этих ОС):

1) для ОС Windows:

```
cd ПДСЧ/Windows  
md5sum prcg.exe crypting.dll  
cd ../..
```

2) для ОС QNX:

```
cd prcg_qnx  
md5sum prcg_qnx  
cd ..
```

3) для ОС МСВС 3.0, МСВС 5.0, Эльбрус, Эльбрус-Д, Astra Linux, Нейтрино (вместо <каталог размещения> необходимо подставить каталог размещения ПО ПДСЧ на дистрибутивном ЭН в соответствии с таблицей 2, например, ПДСЧ/МСВС):

```
cd <каталог размещения>  
md5sum prcg_lin  
cd ../..
```

Отображаемые контрольные суммы должны соответствовать эталонным контрольным суммам (приложение 1, алгоритм MD5).

1.4.3.4. Для проверки целостности дистрибутива ПО ПДСЧ в ЗОСРВ «Нейтрино» используется встроенная в ЗОСРВ программа расчета контрольных сумм – cksum. Проверка осуществляется от имени суперпользователя следующим образом:

- вставить дистрибутивный ЭН в привод компакт-дисков;
- перейти в каталог дистрибутива, выполнив в консоли следующую команду:

```
cd /fs/cd0/prcg_neutrino
```

- получить контрольные суммы ПДСЧ, выполнив следующую команду:

```
sh ./calc_cksum.sh
```

Отображаемые контрольные суммы модулей (в случае поставки ПДСЧ для нескольких ОС отображаются контрольные суммы модулей для каждой из этих ОС) должны соответствовать эталонным контрольным суммам (приложение 1, алгоритм CKSUM).

1.5. Установка ПДСЧ

Установка ПДСЧ осуществляется заказчиком или предприятием-изготовителем согласно договору на поставку.

1.6. Сведения о хранении

1.6.1. Хранение изделия допускается только в закрытых помещениях в упакованном виде при температуре от плюс 5 до плюс 40 °С и относительной влажности воздуха не более 80 %. Не допускается хранение вблизи магнитных полей и ферромагнитных материалов. Изделие должно храниться вдали от нагревательных приборов и должно быть защищено от прямых солнечных лучей.

1.6.2. ПДСЧ должен быть защищен от несанкционированного доступа, уничтожения и искажения.

На объекте к ПДСЧ должны быть допущены только специалисты службы ОБИ.

1.6.3. Полученный дистрибутивный ЭН с ПДСЧ необходимо хранить как эталон, а для эксплуатации использовать копию.

1.6.4. Организация, эксплуатирующая ПДСЧ, несет ответственность за несанкционированное размножение ПДСЧ.

1.6.5. Сведения о хранении, требующие документирования, заносятся в таблицу 1 приложения 2.

1.7. Гарантийные обязательства

1.7.1. Изготовитель (поставщик) гарантирует соответствие ПДСЧ требованиям технических условий (0230259.01428-01 94 01) при соблюдении потребителем условий эксплуатации, хранения и транспортирования, установленных эксплуатационной документацией.

1.7.2. Гарантийный срок эксплуатации ПДСЧ – 36 мес со дня изготовления изделия, включая гарантийный срок хранения изделия – 12 мес.

1.7.3. В случае обнаружения неисправностей, возникших по вине поставщика в течение гарантийного периода, порядок предъявления и удовлетворения рекламаций регламентируется ГОСТ РВ 0015-703-2019.

1.7.4. Действие гарантийных обязательств прекращается, если в гарантийный период потребитель нарушил условия и правила хранения, транспортирования, монтажа и эксплуатации, внес какие-либо изменения в программы ПДСЧ, поставляемые предприятием-поставщиком.

1.7.5. Периодически (при обновлении сертифицируемых параметров в рамках действия имеющегося сертификата) возможно обновление версии ПО ПДСЧ всем зарегистрированным пользователям ПДСЧ. Регистрация пользователей ПДСЧ производится разработчиком.

Контактный тел.: (4822) 39-92-34

e-mail: zi@cps.tver.ru

1.7.6. В случае заключения договора между заказчиком и поставщиком на сопровождение поставщик должен анализировать работу ПДСЧ на объекте заказчика и оказывать консультации по решению проблем, связанных с эксплуатацией ПДСЧ, на основе условий договора.

2. СВЕДЕНИЯ О СОСТОЯНИИ ПДСЧ

Сведения о состоянии ПО ПДСЧ фиксируются в таблицах 1, 2 приложения 3.

3. СВЕДЕНИЯ О РЕЗУЛЬТАТАХ ПРОВЕРКИ ОБЪЕКТА

При освидетельствовании объекта специальными контрольными органами сведения о результатах проверки инспектирующими лицами фиксируются в таблицах 1, 2 приложения 4.

4. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

В случае когда изделие, по мнению заказчика, ненадлежащим образом выполняет или не выполняет свои функции, он уведомляет об этом предприятие-поставщика. При этом должны прилагаться следующие материалы:

- письмо с изложением сути претензии и обнаруженных признаков неработоспособности изделия;
- конкретная информация на дистрибутивном ЭН, в которой были выявлены указанные недостатки;
- подробное описание процедуры управления работой ПДСЧ, позволяющей воспроизвести ситуацию, подтверждающую факт неработоспособности.

При подаче рекламаций сведения о них должны фиксироваться в таблице 1 приложения 5.

5. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ ПДСЧ

Программный датчик псевдослучайных чисел 0230259.01428-01 № _____
заводской номер

изготовлен и принят в соответствии с обязательными требованиями государственных стандартов, техническими условиями 0230259.01428-01 94 01 и признан годным для эксплуатации.

Начальник ОТК

МП

личная подпись

расшифровка подписи

год, месяц, число

обозначение документа,
по которому производится поставка

Руководитель
предприятия

МП

личная подпись

расшифровка подписи

год, месяц, число

Заказчик
(при наличии)

МП

личная подпись

расшифровка подписи

год, месяц, число

6. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ

Программный датчик псевдослучайных чисел 0230259.01428-01 № _____
упакован _____
наименование или код изготовителя
согласно требованиям, предусмотренным в технических условиях 0230259.01428-01 94 01.

должность_____
личная подпись_____
расшифровка подписи_____
год, месяц, число

7. ОСОБЫЕ ОТМЕТКИ

КОНТРОЛЬНЫЕ СУММЫ КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПДСЧ

1. Контрольные суммы по алгоритму CHECKSUM

1.1. ПО ПДСЧ для ОС Windows:

- модуль **Crypting.dll**: 36 41 D2 D2 E6 1E 51 33 C2 90 FD 8B 74 AE DE B4 8C
- модуль **preg.exe**: BF FD 96 9E A5 90 22 C1 09 F0 87 7E 7E B8 9F E6 06

1.2. ПО ПДСЧ для ОС MCBC 3.0:

- модуль **preg_lin**: A6 9D 4A 6B 52 C6 C2 D4 0B AA 68 A4 92 61 FB D3 A8

1.3. ПО ПДСЧ для ОС QNX:

- модуль **preg_qnx**: 25 DB 48 9A A0 72 D4 BA 41 84 25 01 73 6D 75 7F F4

1.4. ПО ПДСЧ для ОС MCBC 5.0:

- модуль **preg_lin**: 69 87 7A FD A8 AA 16 B9 50 F0 AE 69 2A D9 8D 28 07

1.5. ПО ПДСЧ для ОС Эльбрус:

- модуль **preg_lin**: 5B 08 94 3D 10 95 9A 88 EA 69 A6 18 84 69 1E 99 BE

1.6. ПО ПДСЧ для ОС Эльбрус-Д:

- модуль **preg_lin**: 38 EB F4 05 C1 F1 01 6D B3 6F 5D 88 4E B4 72 19 A7

1.7. ПО ПДСЧ для ОС Astra Linux:

- модуль **preg_lin**: 77 35 56 8D A3 F2 E6 E5 F5 42 29 10 51 AD 86 79 6D

1.8. ПО ПДСЧ для ОС Astra Linux-Ленинград:

- модуль **preg_lin**: 84 D0 1B 59 88 12 34 FA 46 0C C1 EC 58 B4 83 C4 8B

1.9. ПО ПДСЧ для ЗОСРВ Нейтрино:

- модуль **preg_lin**: E7 80 DE EA 98 5C A9 FE CD C1 10 56 11 DE 61 C2 60

2. Контрольные суммы по алгоритму MD5

2.1. ПО ПДСЧ для ОС Windows:

- модуль **Crypting.dll**: 9dcdb726086dc29d016724928f1396f9
- модуль **preg.exe**: e0daf3023817897503c170d6b930e802

2.2. ПО ПДСЧ для ОС MCBC 3.0:

- модуль **preg_lin**: 3e08379f9ef4440cc5c63c12d147909f

2.3. ПО ПДСЧ для ОС QNX:

- модуль **preg_qnx**: aa06d1e8b798cd6e99d7a7abf97cc87d

2.4. ПО ПДСЧ для ОС MCBC 5.0:

- модуль **preg_lin**: 4b4aabbab74aa02254b2955cd010f2d5

2.5. ПО ПДСЧ для ОС Эльбрус:

- модуль **preg_lin**: d07774c7cc2c783e845f0a741144af1f

2.6. ПО ПДСЧ для ОС Эльбрус-Д:

- модуль **preg_lin**: 99e05c05d9c168ce39e81ac6f4a5a6f8

2.7. ПО ПДСЧ для ОС Astra Linux:

- модуль **preg_lin**: 8844e1cb5514d65e1ee633a2db8cb8f7

2.8. ПО ПДСЧ для ОС Astra Linux-Ленинград:

- модуль **preg_lin**: e33d5e01a88223f09c6dea60de645115

2.9. ПО ПДСЧ для ЗОСРВ Нейтрино:

- модуль **preg_lin**: ba8f72967cb71c241cf31751a8fc730c

3. Контрольные суммы по алгоритму CKSUM

3.1. ПО ПДСЧ для ОС Astra Linux:

- модуль **preg_lin**: 3778653057

3.2. ПО ПДСЧ для ОС Astra Linux-Ленинград:

- модуль **preg_lin**: 3856668052
- 3.3. ПО ПДСЧ для ОС Windows:
 - модуль **preg.exe**: 673256504
 - модуль **Crypting.dll**: 4074325730
- 3.4. ПО ПДСЧ для ОС MCBC 3.0:
 - модуль **preg_lin**: 2269603923
- 3.5. ПО ПДСЧ для ОС MCBC 5.0:
 - модуль **preg_lin**: 1855384914
- 3.6. ПО ПДСЧ для ОС Эльбрус:
 - модуль **preg_lin**: 439554623
- 3.7. ПО ПДСЧ для ОС Эльбрус-Д:
 - модуль **preg_lin**: 137685474
- 3.8. ПО ПДСЧ для ЗОСРВ Нейтрино:
 - модуль **preg_lin**: 3081901849
- 3.9. ПО ПДСЧ для ОС QNX:
 - модуль **preg_qnx**: 83654777

СВЕДЕНИЯ О ХРАНЕНИИ

Сведения о хранении фиксируются в таблице 1 данного приложения.

Таблица 1 – Сведения о хранении

[illegible]

СВЕДЕНИЯ О СОСТОЯНИИ ПДСЧ

Сведения об установке ПО ПДСЧ на ЭВМ при эксплуатации на объекте и сведения об изменениях ПО фиксируются в таблицах 1 и 2 данного приложения соответственно.

Таблица 1 – Сведения об установке ПО ПДСЧ на ЭВМ при эксплуатации на объекте

[illegible]

[illegible]

Освидетельствование объектов специальными контрольными органами и сведения о результатах проверки инспектирующими лицами фиксируются в таблицах 1 и 2 данного приложения соответственно.

Таблица 1 – Освидетельствование объектов специальными контрольными органами

[illegible]

[illegible]

УЧЕТ ПРЕДЪЯВЛЕННЫХ РЕКЛАМАЦИЙ

Учет предъявленных рекламаций фиксируется в таблице 1 данного приложения.

Таблица 1 – Учет предъявленных рекламаций

[illegible]

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ЗОСРВ	– защищенная операционная система реального времени
МО	– Министерство обороны
МСВС	– мобильная система Вооруженных сил
ОБИ	– обеспечение безопасности информации
ОС	– операционная система
ОТК	– отдел технического контроля
ПДСЧ	– программный датчик псевдослучайных чисел
ПО	– программное обеспечение
ЭВМ	– электронно-вычислительная машина
ЭД	– эксплуатационная документация
ЭН	– электронный носитель

[illegible]