iStorage®

Инструкция пользователя

diskAshur DT²®

Обязательно запишите свой PIN-код (пароль), так как без него вы несможете получить доступ к данным, хранящимся на устройстве.

Если у вас возникли трудности в настройке устройства, пожалуйста обратитесь нашу техническую поддержку: support@datawaysecurity.com

diskAshur DT²®

iStorage®

Иструкция переведена компанией Dataway Security. При расхождении терминов, рекомендуем обратиться к инструкции на английском языке.

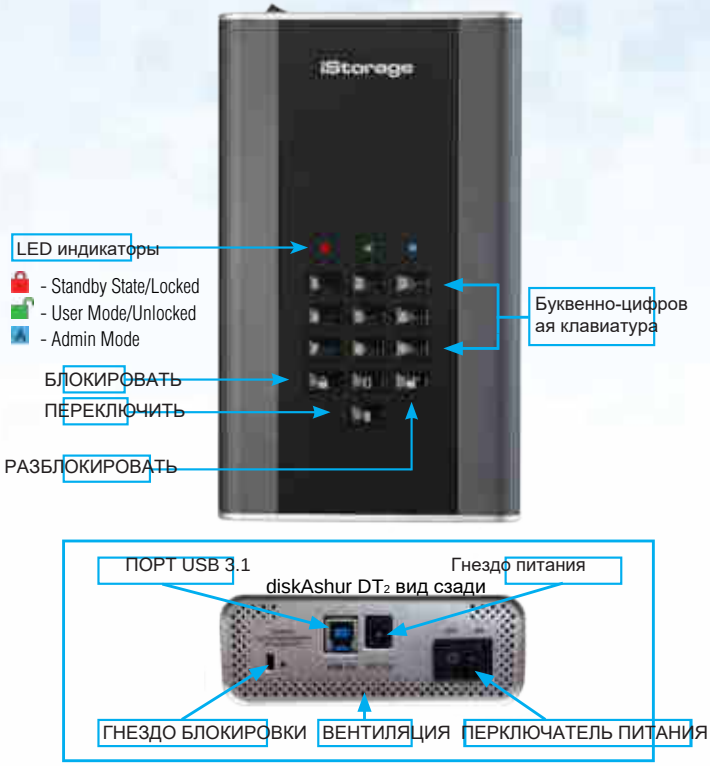
FC CE RoHS

Соответствует условиям TAA

diskAshur DT²®

iStorage®

Содержание



Введение

diskAshur DT^2 это простой в использовании, безопасный, аппаратно зашифрованный жесткий диск емкостью до 14 ТБ. Просто подключите его к электропитанию и соедитите с по помощью кабеля USB 3.1 с компьютером и введите PIN-код из 7-15 цифр. Если введен верный PIN-код, данные, хранящиеся на диске будут расшифрованы и станут доступными.

Для того, чтобы заблокировать устройство просто отключите diskAshur DT^2 от компьютера. Все содержимое диска будет зашифровано (полное шифрование) используя 256-битное аппаратное шифрование AES военного уровня (режим XTS). Если устройство было украдено или утеряно, либо неверный PIN-код был введен 15 раз подряд, произойдет сброс настроек, ключ шифрования будет удален и вся информация, хранившаяся на диске будет потеряна без возможности восстановления.

Одной из уникальных и базовых функций безопасности GDPR-совместимого диска, является специализированный аппаратный защищенный микропроцессор (совместим с Common Criteria EAL4 +), в котором используются встроенные механизмы физической защиты, предназначенные для защиты от внешнего вмешательства, обходных атак и инъекций. В отличие от аналогов, diskAshur DT2 реагирует на автоматические атаки, автоматически переходя в замороженное состояние блокировки, что делает все подобные атаки попросту бесполезными. Говоря простым языком, без PIN-кода к вашим данным не подобраться!

Комплектация

1. Привод diskAshur DT²
2. USB кабель
3. Универсальный адаптер питания
4. Руководство по быстрому запуску

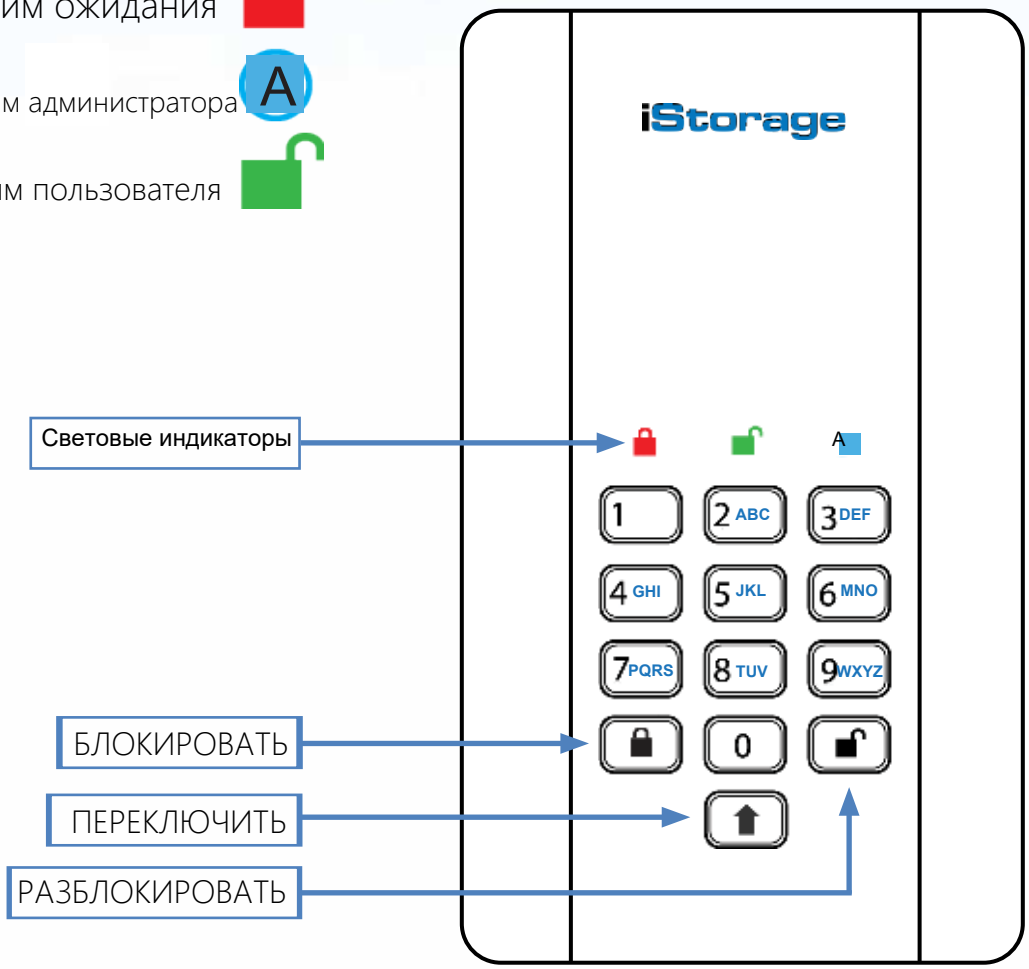
1. Схема устройства

Световой индикатор использует седующие цвета для отображения различных режимов работы:

КРАСНЫЙ: Режим ожидания

ГОЛУБОЙ: Режим администратора

ЗЕЛЕНЫЙ: Режим пользователя



Кнопка “РАЗБЛОКИРОВАТЬ” используется для получения доступа к устройству, а также для подтверждения следующих действий:

- Ввод PIN-кода
- Подтверждение нового PIN-кода
- Доступ к различнм настройкам команд

Кнопка “ПЕРЕКЛЮЧИТЬ” может использоваться для дополнительных комбинаций. Например, сочетание **ПЕРЕКЛЮЧИТЬ** + **1** принимает значение, отличное от просто **1**.
Чтобы создать PIN-код с помощью дополнительных комбинаций нажмите и удерживайте кнопку "Переключение" при вводе PIN-кода из 7-15 цифр. Пример: "ПЕРЕКЛЮЧИТЬ" + 26756498.
Для того, чтобы заблокировать устройство и перевести его в состояние ожидания () нажмите кнопку "БЛОКИРОВАТЬ" .

2. Подключение устройства

Перед подключением диска к внешнему устройству, ознакомьтесь со следующими предостережениями.

Внимание: Используйте только те кабели, которые поставляются в комплекте. Использование посторонних кабелей может привести к повреждению устройства.

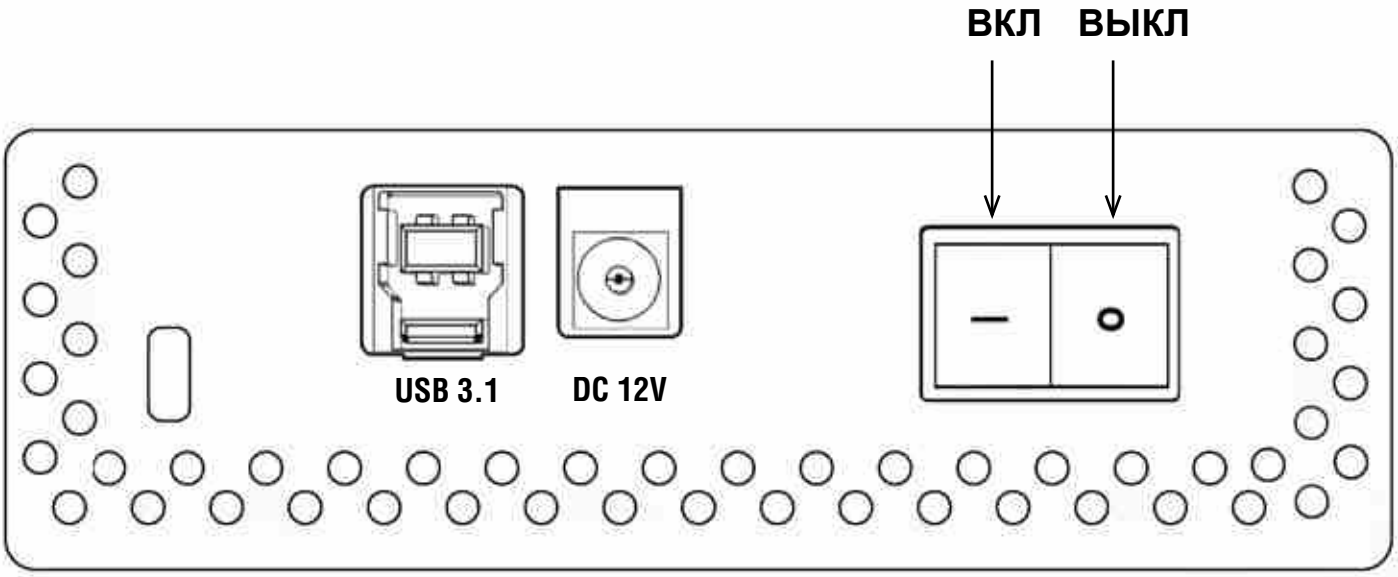
1. Убедитесь, что переключатель питания на задней стороне привода находится в положении **ВЫКЛ**.

2. Подключите устройство к электросети с помощью адаптера питания в комплекте.

3. Подключите USB кабель к приводу и доступному USB порту вашего компьютера

4. Переведите переключатель питания на задней стороне устройства в положение **ВКЛ.**

5. Световой индикатор должен загореться **КРАСНЫМ**, показывая, что устройство готово к использованию.



3. Состояния индикатора diskAshur DT²

При подключенном устройстве существует три возможных состояния световых индикаторов, которые описаны в таблице ниже.

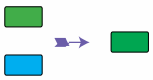
КРАСНЫЙ	ЗЕЛЕНЫЙ	ГОЛУБОЙ	Состояние устройства
Горит	Выкл	Выкл	Возврат к заводским настройкам 1
Горит	Горит	Горит	Грубая сила 2
Горит	Выкл	Выкл	Режим ожидания 3

1. В состоянии "Возврат к заводским настройкам" устройство ожидает задания PIN-кода администратора.
2. В состоянии "Грубая сила" устройство ожидает действий пользователя по запросу новых попыток ввода PIN-кода.
3. В состоянии "Режим ожидания" устройство ожидает действий по его разблокировке, переходу в режим администратора или сбросу настроек.

4. Как пользоваться diskAshur DT² в первый раз

По умолчанию в устройстве diskAshur DT² установлен PIN-код администратора **11223344**. Несмотря на то, что устройство готово к использованию, **мы настоятельно рекомендуем сразу задать новый PIN-код администратора,** следуя инструкциям в разделе 8 "Изменение PIN-кода администратора".

Для того, чтобы разблокировать устройство при первом использовании с PIN-кодом по умолчанию выполните 3 простых шага, описанных в таблице ниже.

Инструкции - первое использование	Индикатор	Состояние индикатора
1. Подключите устройство к USB порту		КРАСНЫЙ индикатор горит в ожидани ввода PIN-кода.
2.Введите PIN-код (по умолчанию - 11223344)		КРАСНЫЙ индиктор продолжает гореть
3.В течение 10 секунд нажмите кнопку **"РАЗБЛОКИРОВАТЬ"** один раз, чтобы разблокировать устройство		ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы поочередно мигнут несколько раз, после чего загорится ГОЛУБОЙ индикатор, затем включится мигающий ЗЕЛЕНЫЙ, который сменится постоянно горящим ЗЕЛЕНЫМ индикатором

Примечение: как только устройство будет успешно разблокировано, загорится ЗЕЛЕНЫЙ индикатор и будет оставаться в этом положении. Устройство может быть немедленно заблокировано посредством однократного нажатия кнопки "**БЛОКИРОВАТЬ**"либо клика на иконке 'Безопасно изъять аппаратное средство/Изъять' в вашей операционной системе. Во избежение повреждения данных, рекомендуем использовать второй способ.

5. Разблокировка устройства

Привод diskAshur DT2 может быть разблокирован посредством ввода PIN-кода администратора или пользователя, когда устройство находится в состоянии ожидания (горит КРАСНЫЙ индикатор).

1. Чтобы разблокировать диск как администратор, введите PIN-код **Администратора** и нажмите кнопку “РАЗБЛОКИРОВАТЬ”.
2. Чтобы разблокировать диск как пользователь, сначала нажмите кнопку “РАЗБЛОКИРОВАТЬ” (все индикаторы, начнут мигать и погаснут), а затем введите PIN-код пользователя и повторно нажмите кнопку "РАЗБЛОКИРОВАТЬ".
3. Если был введен верный PIN-код, оба ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы будут поочередно мигать, а затем загорится ЗЕЛЕНЫЙ индикатор.
4. Если был введен верный PIN-код администратора, оба ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы будут поочередно мигать, затем на 1 секунду загорится ГОЛУБОЙ индикатор, а затем загорится ЗЕЛЕНЫЙ индикатор, показывая, что устройство было разблокировано.
5. Если был введен верный PIN-код, на дисплей выводится название устройства “iStorage diskAshur DT2 USB Device” под сообщением “Computer Management/De-vice Manager”.

В разблокированном состоянии (горит ЗЕЛЕНЫЙ индикатор) возможны 2 типа поведения индикаторов, описанные ниже.

КРАСНЫЙ	ЗЕЛЕНЫЙ	ГОЛУБОЙ	diskAshur DT2
Выкл	Горит	Выкл	Не происходит передачи данных
Выкл	Мигает	Выкл	Происходит передача данных

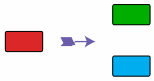
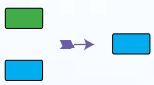
6. Блокировка устройства

Чтобы заблокировать привод нажмите кнопку “**БЛОКИРОВАТЬ**” один раз либо кликните на иконку ‘Безопасно изъять аппаратное средство/Изъять’ в вашей операционной системе. Если происходит передача данных, дождитесь ее окончания перед блокировкой. Если был включен таймер автоблокировки, то устройство самостоятельно заблокируется по истечении заданного периода времени.

Примечание: Устройство diskAshur DT2 не определяется ОС находясь в состоянии ожидания.

7. Вход в режим администратора

Выполните следующие шаги, чтобы войти в Режим администратора

1. В состоянии ожидания (горит КРАСНЫЙ индикатор) нажмите и удерживайте следующее сочетание кнопок “**РАЗБЛОКИРОВАТЬ + 1**”		КРАСНЫЙ индикатор погаснет, начнут мигать ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы
2. Введите PIN-код администратора (по умолчанию - 11223344) и нажмите кнопку “**РАЗБЛОКИРОВАТЬ**”		ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы будут быстро и синхронно мигать в течение нескольких секунд, затем загорится ЗЕЛЕНЫЙ индикатор, который в итоге сменится на постоянно горящий ГОЛУБОЙ индикатор, показывающий, что diskAshur DT2 работает в Режиме администратора.

Чтобы выйти из Режима администратора, нажмите кнопку “**БЛОКИРОВАТЬ**”.

8. Изменение PIN-кода администратора

Требования к PIN-коду:

- Длина от 7 до 15 цифр
- Не должен состоять только из повторяющихся цифр. Пример: (3-3-3-3-3-3-3-3)
- Не может содержать только последовательные цифры. Пример: (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

Совет: В качестве PIN-кода вы можете использовать запоминающееся имя, фразу либо любую другую комбинацию букв и цифр. Для этого нужно нажать кнопку с соответствующей буквой.

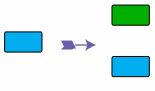
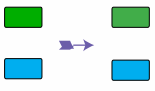
Ниже приведены примеры подобных алфавитно-цифровых PIN-кодов:

- Чтобы ввести слово “**password**” нужно нажать следующие кнопки:
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- Чтобы ввести слово “**istorage**” последовательно нажимайте:
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

Используя данный метод, вы сможете создать достаточно длинные и легко запоминающиеся PIN-коды.

Примечание: Кнопка "ПЕРЕКЛЮЧИТЬ" может использоваться для задания дополнительных комбинаций цифр. **ПЕРЕКЛЮЧИТЬ** + 1 это значение отличное от просто 1.
Чтобы создать PIN-код используя дополнительные комбинации нажмите и удерживайте кнопку **"ПЕРЕКЛЮЧИТЬ"** при вводе PIN-кода из 7-15 цифр. например: **ПЕРЕКЛЮЧИТЬ** + **26756498**.

Чтобы изменить PIN-код администратора сначала перейдите в “**Режим администратора**”, выполнив шаги, указанные в разделе 7. Как только привод перейдет в **Режим администратора** (горит ГОЛУБОЙ индикатор) выполните следующие действия:

1. В Режиме администратора нажмите и удерживайте кнопки “**РАЗБЛОКИРОВАТЬ + 2**”		Постоянно горящий ГОЛУБОЙ индикатор сменится на мигающий ЗЕЛЕНЫЙ и горящий ГОЛУБОЙ индикаторы
2. Введите новый PIN-код администратора и нажмите кнопку “**РАЗБЛОКИРОВАТЬ**”		Комбинация мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов сменится мигающим ЗЕЛЕНЫМ , а затем вновь загорится ГОЛУБОЙ индикатор.
3. Повторно введите новый PIN-код администратора и нажмите кнопку “**РАЗБЛОКИРОВАТЬ**”		Комбинация мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО идикаторов сменится быстро мигающим ГОЛУБЫМ индикатором, который через короткое время загорится постоянно, показывая, что PIN-код администратора был успешно изменен.

9. Установка политикии PIN-кода пользователя

Администратор может установить политику ограничений для PIN-кода пользователя. Такая политика включает в себя установку минимальной длины PIN-кода (от 7 до 15 цифр), а также обязательность '**Специального символа**'. “Специальный символ” вводится комбинацией кнопок 'ПЕРЕКЛЮЧИТЬ + цифра'.

Для того, чтобы установить политику PIN-кода пользователя (ограничения) требуется ввести 3 цифры, например '**091**'. Первые две цифры (**09**) задают минимальную длину PIN-кода (в данном случае, **9**), а последняя цифра (**1**) указывает, что должен быть использован 'Специальный символ', другими словами - сочетание '**ПЕРЕКЛЮЧИТЬ + цифра**'. Таким же образом, политика PIN-кода пользователя может быть установлена без необходимости использовать 'Специальный символ'. Например: '**120**', где первые две цифры (**12**) определяют минимальную длину PIN-кода (в данном примере,**12**), а последняя цифра (**0**) означает, что Специальный символ не является обязательным.

После того, как администратор установил политику PIN-кода, к примеру '091', должен быть создан новый PIN-код пользователя. Если администратор устанавливает PIN-код пользователя '**247688314**' с обязательным использованием '**Специального символа**' (ПЕРЕКЛЮЧИТЬ+цифра), то этот символ может быть вставлен в любом месте внутри PIN-кода из 7-15 цифр при вводе PIN-кода пользователя, как показано в примере ниже.

A. '**ПЕРЕКЛЮЧИТЬ+ 2**', '4', '7', '6', '8', '8', '3', '1', '4',

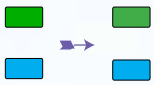
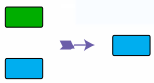
B. '2', '4', '**ПЕРЕКЛЮЧИТЬ + 7**', '6', '8', '8', '3', '1', '4',

C. '2', '4', '7', '6', '8', '8', '3', '1', '**ПЕРЕКЛЮЧИТЬ + 4**',

Примечения:

- Если при создании PIN-кода пользователя был использован 'Специальный символ', к примеру, как в примере '**B**' приведенном выше, в таком случае устройство может быть разблокировано только посредством введения PIN-кода со "Специальным символом" точно в таком порядке, как указано в примере '**B**' выше - ('2', '4', '**ПЕРЕКЛЮЧИТЬ + 7**', '6', '8', '8', '3', '1', '4').
- Пользователи имеют право изменять свой PIN-код, но он обязательно должен соответствовать 'Политике PIN-кода пользователя' (ограничениям), если она установлена.
- Установка новой политики PIN-кода пользователя означает автоматическое удаление существующего PIN-кода, если он был задан.
- Данная политика не распространяется на ‘саморазрушающийся PIN-код’. Требования к сложности саморазрушающегося PIN-кода и PIN-кода администратора неизменны: 7-15 цифр, специальный символ не обязателен.

Для того, чтобы устновить политику PIN-кода пользователя, сначала перейдите в “**Режим администратора**” выполнив действия, описанные в разделе 7. Когда устройство перейдет в **Режим администратора** (горит ГОЛУБОЙ индикатор), выполните следующие действия.

1. В режиме администратора нажмите и удерживайте кнопки “**РАЗБЛОКИРОВАТЬ + 7**”		ГОЛУБОЙ индикатор продолжит гореть, к нему добавится мигающий ЗЕЛЕНЫЙ индикатор.
2. Введите **3 цифры.** Важно помнить, что первые две цифры определяют минимальную длину PIN-кода, а последняя (0 или 1) - обязательно ли наличие специального символа.		ЗЕЛЕНЫЙ индикатор продолжит мигать, а ГОЛУБОЙ индикатор продолжит гореть.
3. Один раз нажмите кнопку "ПЕРЕКЛЮЧИТЬ"⬆		Комбинация мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО сменится на горящий ЗЕЛЕНЫЙ, а затем на постоянно горящий ГОЛУБОЙ индикатор, показывая, что политика PIN-кода пользователя была успешно установлена.

10. Как проверить политику PIN-кода пользователя

Администратор может проверить установленную политику PIN-кода пользователя и определить ограничение по минимальной длине PIN-кода , а также необходимость использования специального символа, наблюдая за последовательностью сигналов световых индикаторов и ориентируясь на таблицу ниже.

Чтобы проверить политику PIN-кода, сначала войдите в “**Режим администратора**”, выполнив действия, описанные в разделе 7. Когда устройство перейдет в Режим администратора (горит ГОЛУБОЙ индикатор), выполните следующие действия.

1. В режиме администратора нажмите и удерживайте кнопки **ПЕРЕКЛЮЧИТЬ** (⬆) + **7**”		Горящий ГОЛУБОЙ индикатор сменится на мигающие ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы

2. Нажмите кнопку “**РАЗБЛОКИРОВАТЬ**” и произойдет следующее:

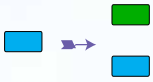
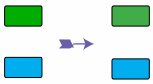
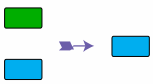
а. Все индикаторы (КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ) загорятся на 1 секунду.
б. Каждое мигание КРАСНОГО индикатора означает десять (10) символов PIN-кода.
в. Каждое мигание ЗЕЛЕНОГО индикатора означает один (1) символ PIN-кода.
г. Мигание ГОЛУБОГО показывает то, что "Специальный символ" является обязательным.
д. Все индикаторы (КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ) загорятся на 1 секунду.
е. Загорится ГОЛУБОЙ индикатор.

Таблица ниже описывает поведение световых индикаторов при проверке политики PIN-кода пользователя. К примеру, если был установлен PIN-код пользователя из 12 цифр с обязательным специальным символом, КРАСНЫЙ индикатор мигнет один (**1**) раз, ЗЕЛЕНЫЙ мигнет два (**2**) раза, а затем один раз мигнет СИНИЙ индикатор, показывая, что **Специальный символ** обязательно должен быть использован.

Описание PIN-кода	**Набор из 3 цифр**	**КРАСНЫЙ**	**ЗЕЛЕНЫЙ**	**ГОЛУБОЙ**
12-цифровой PIN-код со Специальным символом	121	1 мигание	2 мигания	1 мигание
12-циф ровой PIN-код без Специального символа	120	1 мигание	2 мигания	0
9-цифровой PIN-код со Специальным символом	091	0	9 миганий	1 мигание
9-цифровой PIN-код без Специального символа	090	0	9 миганий	0

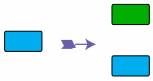
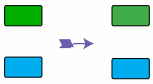
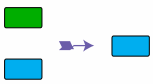
11. Добавление нового PIN-кода пользователя в режиме администратора

Для того, чтобы добавить нового пользователя сначала войдите в “Режим администратора”, выполнив действия, описанные в разделе 7. Когда устройство перейдет в Режим администратора (горит ГОЛУБОЙ индикатор), выполните следующие действия.

1. В режиме администратора нажмите и удерживайте кнопки "РАЗБЛОКИРОВАТЬ" + 3		Постоянно горящий ГОЛУБОЙ индикатор сменится на мигающий ЗЕЛЕНЫЙ и горящий ГОЛУБОЙ индикаторы
2. Введите новый PIN-код пользователя и нажмите кнопку "РАЗБЛОКИРОВАТЬ"		Комбинация мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов сменится одиночным миганием ЗЕЛЕНОГО индикатора, затем ЗЕЛЕНЫЙ индикатор продолжит мигать, а ГОЛУБОЙ будет гореть постоянно.
3. Повторно введите новый PIN-код пользователя и нажмите кнопку “**РАЗБЛОКИРОВАТЬ**”		ЗЕЛЕНЫЙ индикатор будет быстро мигать несколько секунд и сменится на постоянно горящий ГОЛУБОЙ индикатор, показывая, что новый PIN-код пользователя был успешно создан.

12. Изменение PIN-кода пользователя в режиме администратора

Чтобы изменить существующий PIN-код пользователя, сначала войдите в “Режим администратора”, выполнив действия, описанные в разделе 7. Когда устройство перейдет в Режим администратора (горит ГОЛУБОЙ индикатор), выполните следующие действия.

1. В режиме администратора нажмите и удерживайте кнопки "РАЗБЛОКИРОВАТЬ" + 3		Постоянно горящий ГОЛУБОЙ индикатор сменится на мигающий ЗЕЛЕНЫЙ и горящий ГОЛУБОЙ индикаторы
2. Введите новый PIN-код пользователя и нажмите кнопку "РАЗБЛОКИРОВАТЬ"		Комбинация мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов сменится одиночным миганием ЗЕЛЕНОГО индикатора, затем ЗЕЛЕНЫЙ индикатор продолжит мигать, а ГОЛУБОЙ будет гореть постоянно.
3. Повторно введите новый PIN-код пользователя и нажмите кнопку “**РАЗБЛОКИРОВАТЬ**”		ЗЕЛЕНЫЙ индикатор будет быстро мигать несколько секунд и сменится на постоянно горящий ГОЛУБОЙ индикатор, показывая, что PIN-код пользователя был успешно изменен.

13. Удаление PIN-кода пользователя в режиме администратора

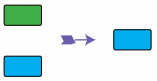
Чтобы удалить существующий PIN-код пользователя, сначала войдите в “Режим администратора”, выполнив действия, описанные в разделе 7. Когда устройство перейдет в Режим администратора (горит ГОЛУБОЙ индикатор), выполните следующие действия.

1. В режиме администратора нажмите и удерживайте кнопки "ПЕРЕКЛЮЧИТЬ" + 3, а затем отпустите.		Горящий ГОЛУБОЙ сменится на мигающий КРАСНЫЙ индикатор
1. В режиме администратора нажмите и удерживайте кнопки "ПЕРЕКЛЮЧИТЬ" + 3, а затем отпустите.		Мигающий КРАСНЫЙ индикатор сменится на горящий, а затем на постоянно горящий ГОЛУБОЙ, показывая, что PIN-код пользователя был успешно удален.

14. Установка "Только чтение" в режиме администратора

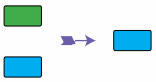
Важно: Если данные были только что скопированы на устройство, следует сначала отключить его правильным образом от операционной системы кликнув 'Безопасно изъять аппаратное средство/изъять' перед повторным подключением и установкой режима 'Только чтение/Защита от записи'.

Если администратор записал содержимое на устройство и ограничил доступ к нему ("Только чтение"), пользователь не сможет изменить эту настройку в режиме пользоватя. Для того, чтобы установить "Только чтение" сначала перейдите в "Режим администратора", выполнив действия, описанные в разделе 7. Когда устройство перейдет в Режим администратора (горит ГОЛУБОЙ индикатор), выполните следующие действия.

1. В режиме администатора нажмите и удерживайте кнопки "**7 + 6**". (7=**Т**олько + 6=**Ч**тение)		Постоянно горящий ГОЛУБОЙ индикатор сменится на мигающие ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы
2. Отпустите кнопки "7 + 6" и нажмите кнопку "РАЗБЛОКИРОВАТЬ"		Комбинация мигающих ЗЕЛЕНОГО и ГОЛУБОГО сменится на горящий ЗЕЛЕНЫЙ, а затем на постоянно горящий ГОЛУБОЙ индикатор, показывая, что режим "Только чтение" был успешно установлен.

15. Включить Чтение/Запись в режиме администратора

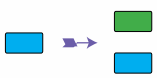
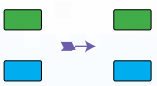
Чтобы включить "Чтение/Запись" на устройстве, сначала войдите в "Режим администратора", выполнив действия, описанные в разделе 7. Когда устройство перейдет в Режим администратора (горит ГОЛУБОЙ индикатор), выполните следующие действия.

1. В режиме администатора нажмите и удерживайте кнопки "**7 + 9**". (7=Чтение + 9=**З**апись)		Постоянно горящий ГОЛУБОЙ индикатор сменится на мигающие ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы
2. Отпустите кнопки "7 + 9" и нажмите кнопку "РАЗБЛОКИРОВАТЬ"		Комбинация мигающих ЗЕЛЕНОГО и ГОЛУБОГО сменится на горящий ЗЕЛЕНЫЙ, а затем на постоянно горящий ГОЛУБОЙ индикатор, показывая, что режим "Чтение/Запись" был успешно включен на устройстве.

16. Как создать саморазрушающийся PIN-код

Фукнция саморазрушения позволяет вам задать PIN-код, который может быть использован для стирания всех цифровых данных, хранящихся на устройстве. Если функция активна, то саморазрушающийся пароль **удалит все данные, PIN-коды администратора и пользователя,** а затем разблокирует устройство. Когда данная функция активируется, саморазрушающийся PIN-код автоматически становится новым PIN-кодом пользователя и устройство должно быть разбито на логические блоки и отформатировано перед тем, как записывать на него новые данные.

Для того, чтобы создать саморазрушающийся PIN-код сначала перейдите в "Режим администратора", выполнив действия, описанные в разделе 7. Когда устройство перейдет в Режим администратора (горит ГОЛУБОЙ индикатор), выполните следующие действия.

1. В режиме администатора нажмите и удерживайте кнопки "**РАЗБЛОКИРОВАТЬ + 6**".		Постоянно горящий ГОЛУБОЙ индикатор сменится на мигающий ЗЕЛЕНЫЙ и горящий ГОЛУБОЙ индикаторы
2. Создайте саморазрушающийся PIN-код из 7-15 цифр и нажмите кнопку "**РАЗБЛОКИРОВАТЬ**"		Комбинация мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов сменится одиночным миганием ЗЕЛЕНОГО индикатора, затем ЗЕЛЕНЫЙ индикатор продолжит мигать, а ГОЛУБОЙ будет гореть постоянно.
3. Повторно введите PIN-код пользователя и нажмите кнопку "**РАЗБЛОКИРОВАТЬ**"		ЗЕЛЕНЫЙ индикатор будет быстро мигать несколько секунд и сменится на постоянно горящий ГОЛУБОЙ индикатор, показывая, что саморазрушающийся PIN-код был успешно создан.

17. Как удалить самоуничтожающийся PIN-код

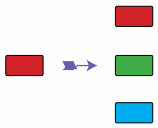
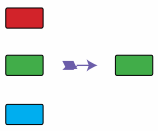
Для того, чтобы удалить самоуничтожающийся PIN-код сначала перейдите в “Режим администратора”, выполнив действия, описанные в разделе 7. Когда устройство перейдет в Режим администратора (горит ГОЛУБОЙ индикатор), выполните следующие действия.

1. В режиме администатора нажмите и удерживайте кнопки “**ПЕРЕКЛЮЧИТЬ + 6**”.		Горящий ГОЛУБОЙ индикатор сменится мигающим КРАСНЫМ индикатором
2. Повторно нажмите и удерживайте кнопки кнопки “**ПЕРЕКЛЮЧИТЬ + 6**”.		Мигающий КРАСНЫЙ индикатор сменится на горящий, а затем на постоянно горящий ГОЛУБОЙ, показывая, что самоуничтожающийся PIN-код был успешно удален.

18. Как разблокировать с помощью самоуничтожающегося PIN-кода

Если функция активна, то самоуничтожающийся пароль **удалит все данные, PIN-коды администратора и пользователя,** а затем разблокирует устройство. Когда данная функция активируется, самоуничтожающийся PIN-код автоматически становится новым PIN-кодом пользователя, а устройство должно быть разбито на логические блоки и отформатировано перед тем, как записывать на него новые данные.

Чтобы активировать механизм самоуничтожения необходимо перевести устройство в состояние ожидания (горит КРАСНЫЙ индикатор), а затем выполнить следующие действия.

1. В состоянии ожидания нажмите кнопку “**РАЗБЛОКИРОВАТЬ**”		Все индикаторы (КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ) начнут мигать
2. Введите ваш самоуничтожающийся PIN-код и нажмите кнопку “**РАЗБЛОКИРОВАТЬ**”		Мигающие КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы сменятся на поочередно мигающие ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы (будут мигать примеро 15 секунд), а затем загорится ЗЕЛЕНЫЙ индикатор

Важно: Если был активирован механизм самоуничтожения, все данные, ключ шифрования и PIN-коды администратора/пользователя будут удалены. **Самоуничтожающийся PIN-код автоматически станет новым PIN-кодом пользователя.** После активации механизма самоуничтожения PIN-код администратора больше не существует. Следует произести полный сброс настроек (см. раздел 28 на стр. 19 ‘Как выполнить полный сброс’) перед тем, как создать новый PIN-код администратора со всеми привилегиями, включая создание PIN-кода пользователя.

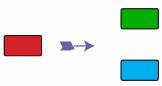
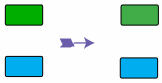
19. Как создать PIN-код администратора после атаки грубой силы или сброса

После атаки грубой силы или сброса настроек устройства требуется создать новый PIN-код администратора перед тем, как устройство может быть использовано. Если устройство было подвержено при атаке грубой силы или был выполнен полный сброс настроек, переведите его в состояние ожидания (горит КРАСНЫЙ индикатор), чтобы создать PIN-код администратора, выполнив следующие действия:

Требования к PIN-коду:

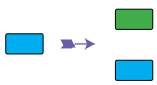
- Длина от 7 до 15 цифр
- Не должен состоять только из повторяющихся цифр. Пример: (3-3-3-3-3-3-3)
- Не может содержать только последовательные цифры. Пример: (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

Примечание: Кнопка "ПЕРЕКЛЮЧИТЬ" может использоваться для задания дополнительных комбинаций цифр. **ПЕРЕКЛЮЧИТЬ** + 1 это значение отличное от просто 1.
Чтобы создать PIN-код используя дополнительные комбинации нажмите и удерживайте кнопку **"ПЕРЕКЛЮЧИТЬ"** при вводе PIN-кода из 7-15 цифр. например: **ПЕРЕКЛЮЧИТЬ** + **26756498**.

1. В состоянии ожидания нажмите и удерживайте кнопки “ПЕРЕКЛЮЧИТЬ” + 1		Горящий КРАСНЫЙ индикатор сменится сочетанием мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов
2. Введите НОВЫЙ пароль администратора и нажмите кнопку “**РАЗБЛОКИРОВАТЬ**”		Комбинация мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов сменится одиночным миганием ЗЕЛЕНОГО индикатора, затем ЗЕЛЕНЫЙ индикатор продолжит мигать, а ГОЛУБОЙ будет гореть постоянно.
3. Повторно введите НОВЫЙ пароль администратора и нажмите кнопку “**РАЗБЛОКИРОВАТЬ**”		Мигающий ЗЕЛЕНЫЙ и горящий ГОЛУБОЙ индикаторы сменятся на быстро мигающий ГОЛУБОЙ индикатор (будет мигать несколько секунд), а затем загорится ГОЛУБОЙ индикатор, показывать, что PIN-код администратора был успешно задан.

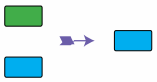
20. Настройка таймера автоблокировки

В целях защиты от несанкционированного доступа устройство оснащено функцией таймера автоблокировки. Если носитель находится в разблокированном состоянии, он может быть автоматически заблокирован через заданный промежуток времени. По умолчанию таймер автоблокировки выключен. Интервал доступных временных промежутков таймера: от 5 до 99 минут.
Для того, чтобы настроить таймер автоблокировки сначала перейдите в “Режим администратора”, выполнив действия, описанные в разделе 7. Когда устройство перейдет в Режим администратора (горит ГОЛУБОЙ индикатор), выполните следующие действия.

1. В режиме администратора нажмите и удерживайте кнопки “РАЗБЛОКИРОВАТЬ **+ 5**”		Горящий ГОЛУБОЙ сменится на сочетание мигающего ЗЕЛЕНОГОи горящего ГОЛУБОГО индикаторов
2. Введите значение времени для таймера автоблокировки. Минимальный промежуток: 5 минут, максимальный: 99 минут (5-99 минут). Например, введите: **05 для 5 минут** **20 для 20 минут** **99 для 99 минут**		
3. Нажмите кнопку “ПЕРЕКЛЮЧИТЬ”		Комбинация мигающих ЗЕЛЕНОГО и ГОЛУБОГО сменится на горящий ЗЕЛЕНЫЙ, а затем на постоянно горящий ГОЛУБОЙ индикатор, показывая, что таймер автоблокировки был успешно настроен.

21. Выключение таймера автоблокировки

Для того, чтобы выключить таймер автоблокировки сначала перейдите в “Режим администратора”, выполнив действия, описанные в разделе 7. Когда устройство перейдет в Режим администратора (горит ГОЛУБОЙ индикатор), выполните следующие действия.

1. В режиме администратора нажмите и удерживайте кнопки “РАЗБЛОКИРОВАТЬ **+ 5**”		Горящий ГОЛУБОЙ сменится на сочетание мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов
2. Введите цифры “**00**” и нажмите кнопку “**ПЕРЕКЛЮЧИТЬ**”		Комбинация мигающих ЗЕЛЕНОГО и ГОЛУБОГО сменится на горящий ЗЕЛЕНЫЙ, а затем на постоянно горящий ГОЛУБОЙ индикатор, показывая, что таймер автоблокировки был успешно выключен.

22. Как проверить таймер автоблокировки

Администратор имеет возможность проверить включен ли таймер автоблокировки и определить, какой временной промежуток в нем задан наблюдая за последовательностью сигналов световых индикаторов, ориентируясь на приведенную ниже таблицу.

Для того, чтобы проверить таймер автоблокировки сначала перейдите в “Режим администратора”, выполнив действия, описанные в разделе 7. Когда устройство перейдет в Режим администратора (горит ГОЛУБОЙ индикатор), выполните следующие действия.

1. В режиме администратора нажмите и удерживайте кнопки **ПЕРЕКЛЮЧИТЬ** (⬆) + **5**”		Горящий ГОЛУБОЙ сменится на сочетание мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов

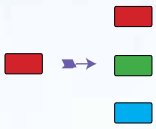
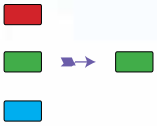
2. Нажмите кнопку “**РАЗБЛОКИРОВАТЬ**”, должно произойти следующее:

а. Все индикаторы (КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ) загорятся на 1 секунду.
б. Каждое мигание КРАСНОГО индикатора означает **десять** (10) **минут**.
в. Каждое мигание ЗЕЛЕНОГО индикатора означает **одну** (1) **минуту**.
г. Все индикаторы (КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ) загорятся на 1 секунду.
д. Загорится ГОЛУБОЙ индикатор.

В таблице ниже показано поведение световых индикаторов при проверке таймера автоблокировки. Например, если вы установили таймер устройства на **26** минут, КРАСНЫЙ индикатор мигнет два (**2**) раза, а ЗЕЛЕНЫЙ индикатор мигнет шесть (**6**) раз.

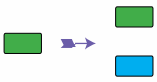
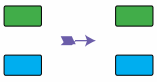
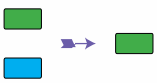
Время таймера	**КРАСНЫЙ**	**ЗЕЛЕНЫЙ**
8 минут	0	8 миганий
15 минут	1 мигание	5 миганий
26 минут	2 мигания	6 миганий
40 минут	4 мигания	0

23. Как разблокировать устройство при помощи PIN-кода пользователя

1. В состоянии ожидания (горит КРАСНЫЙ индикатор) нажмите кнопку “**РАЗБЛОКИРОВАТЬ**”		Все индикаторы (КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ) начнут мигать
2. Введите PIN-код пользователя и нажмите кнопку “**РАЗБЛОКИРОВАТЬ**”		Мигающие КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы сменятся на поочередно мигающие ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы (будут мигать примерно 15 секунд), а затем загорится ЗЕЛЕНЫЙ индикатор, показывая, что привод успешно разблокирован в режиме пользователя.

24. Изменение PIN-кода пользователя в режиме пользователя

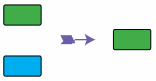
Чтобы изменить **PIN-код пользователя** сначала разблокируйте устройство при помощи PIN-кода пользователя как описано выше в разделе 23. Когда устройство перейдет в **Режим пользователя** (горит ЗЕЛЕНЫЙ индикатор) выполните следующие действия:

1.В режиме пользователя нажмите и удерживайте кнопки “**РАЗБЛОКИРОАТЬ + 4**”		Горящий ЗЕЛЕНЫЙ индикатор сменится на сочетание мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов
2. Введите новый PIN-код пользователя и нажмите кнопку “**РАЗБЛОКИРОВАТЬ**”		Сочетание мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов сменится одиночным миганием ЗЕЛЕНОГО индикатора, а затем ЗЕЛЕНЫЙ индикатор будет продолжать мигать, а ГОЛУБОЙ вновь загориться.
3. Поторно введите новый PIN-код пользователя и нажмите кнопку “**РАЗБЛОКИРОВАТЬ**”		Сочетание мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов сначала сменится на быстро мигающий, а затем на постоянно горящий ЗЕЛЕНЫЙ индикатор, показывая, что PIN-код пользователя был успешно изменен.

25. Установка "Только чтение" в режиме пользователя

Важно: Если данные были только что скопированы на устройство, следует сначала отключить его правильным образом от операционной системы кликнув 'Безопасно изъять аппаратное средство/изъять' перед повторным подключением и установкой режима 'Только чтение/Защита от записи'.

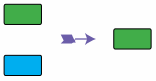
Для того, чтобы установить "Только чтение" сначала перейдите в "Режим пользователя", как описано в разделе 23. Когда устройство перейдет в Режим пользователя (горит ЗЕЛЕНЫЙ индикатор), выполните следующие действия.

1. В режиме пользователя нажмите и удерживайте кнопки "**7 + 6**". (7=**Т**олько + 6=**Ч**тение)		Горящий ЗЕЛЕНЫЙ индикатор сменится на сочетание мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов
2. Отпустите кнопки "7 + 6" и нажмите кнопку "РАЗБЛОКИРОВАТЬ"		Сочетание мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов сменится на постоянно горящий ЗЕЛЕНЫЙ индикатор, показывая, что режим "Только чтение" был успешно установлен.

Примечания: 1. Данная установка будет актирована при следующей разблокировке носителя.
2. Если "Только чтение" установил пользовал, администратор может сбросить эту установку, включив "Чтение/Запись" в режиме администратора.
3. Если администратор установил "Только чтение", пользователь не может установить "Чтение/Запись".

26. Включить Чтение/Запись в режиме пользователя

Для того, чтобы включить "Чтение/Запись" сначала перейдите в "Режим пользователя", как описано в разделе 23. Когда устройство перейдет в Режим пользователя (горит ЗЕЛЕНЫЙ индикатор), выполните следующие действия.

1. В режиме пользователя нажмите и удерживайте кнопки "**7 + 9**". (7=**Ч**тение + 9=**З**апись)		Горящий ЗЕЛЕНЫЙ индикатор сменится на сочетание мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов
2. Отпустите кнопки "7 + 9" и нажмите кнопку "РАЗБЛОКИРОВАТЬ"		Сочетание мигающего ЗЕЛЕНОГО и горящего ГОЛУБОГО индикаторов сменится на постоянно горящий ЗЕЛЕНЫЙ индикатор, показывая, что режим "Чтение/Запись" был успешно активирован.

Примечания: 1. Данная установка будет актирована при следующей разблокировке носителя.
2. Если "Только чтение" установил пользовал, администратор может сбросить эту установку, включив "Чтение/Запись" в режиме администратора.
3. Если администратор установил "Только чтение", пользователь не может установить "Чтение/Запись".

27. Защита от грубой силы

Если неверный PIN-код был введен 15 (3 по 5 PIN-кластеров) раз подряд, в таком случае все PIN-коды, ключ шифрования и **все данные будут удалены без возможности восстановления**. Для того, чтобы использовать устройство снова, его следует разбить на логические блоки и отформатировать.

1. Если PIN-код был введен неверно 5 (пять) раз подряд, все световые индикаторы - КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ подсветятся и будут гореть.

2. Переместите переключатель питания в положение **ВЫКЛ,** а затем снова во **ВКЛ** для получения пяти дополнительных попыток ввода PIN-кода. Если PIN-код был введен неверно еще 5 раз, (всего 10 - 5 в шаге 1 и 5 в шаге 2), все индикаторы - КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ подсветятся и будут гореть.

3. Переместите переключатель питания в положение **ВЫКЛ**, затем удерживая кнопку "**ПЕРЕКЛЮЧЕНИЕ**" снова включите питание устройства.

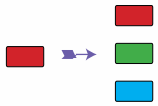
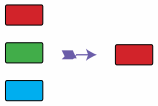
4. Когда загорятся все индикаторы введите код "**47867243**" нажмите кнопку "**РАЗБЛОКИРОВАТЬ**", чтобы получить пять последних попыток ввода пароля.

ВНИМАНИЕ: После 15 неудачных попыток ввода PIN-кода активируется механизм защиты от грубой силы, удаляя все PIN-коды, ключ шифрования и данные. Потребуется создание нового PIN-кода, процесс которого описан в разделе 19 на странице 15 'Как создать PIN-код администратора после атаки грубой силы или сброса", а само устройство будет нужно разбить на логические блоки и отформатировать.

28. Как выполнить полный сброс настроек

Чтобы выполнить полный сброс настроек, переведите привод в состояние ожидания (горит КРАСНЫЙ индикатор). После сброса настроек устройства все PIN-коды (администратора и пользователей), ключи шифрования и все даные будут удалены без возможности восстановления, а само устройство потребуется разбить на логические блоки и отформатировать.

Чтобы сбросить настройки устройства выполните следующие действия:

1. В состоянии ожидания нажмите и удерживайте кнопку"**0**" пока все индикаторы не мигнут попеременно.		Горящий КРАСНЫЙ индикатор сменится на поочередное мигание всех индикаторов (КРАСНОГО, ЗЕЛЕНОГО и ГОЛУБОГО)
2. Нажмите и удерживайте кнопки "**2 + 7**" пока все индикаторы не подсветятся на 1 секунду, а затем загорится КРАСНЫЙ индикатор.		Попеременно мигающие КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы подсветятся на 1 секунду, а затем снова загорится КРАСНЫЙ индикатор, показывая, что сброс настроек устройства был успешно произведен.

ВАЖНО: После полного сброса настроек устройства потребуется создание нового PIN-кода, процесс которого описан в разделе 19 на странице 15 'Как создать PIN-код администратора после атаки грубой силы или сброса", а само устройство будет нужно разбить на логические блоки и отформатировать.

29. Инициализация и форматирование устройства

После ‘атаки грубой силы’ или полного сброса настроек устройства будут удалены все данные, ключ шифрования, а также настройки разбивки на логические блоки. Перед дальнейшим использованием устройства вам требуется выполнить его инициализацию и форматирование. Для этого выполните следующие действия:

1. Подключите устройство к компьютеру.

2. Создайте новый PIN-код администратора. Смотрите раздел 19 на странице 15 ‘Как создать PIN-код администратора после атаки грубой силы или сброса настроек’.

3. Убедишись, что устройство в состоянии ожидания (КРАСНЫЙ индикатор) введите новый PIN-код администратора, чтобы разблокировать его (ЗЕЛЕНЫЙ индикатор).

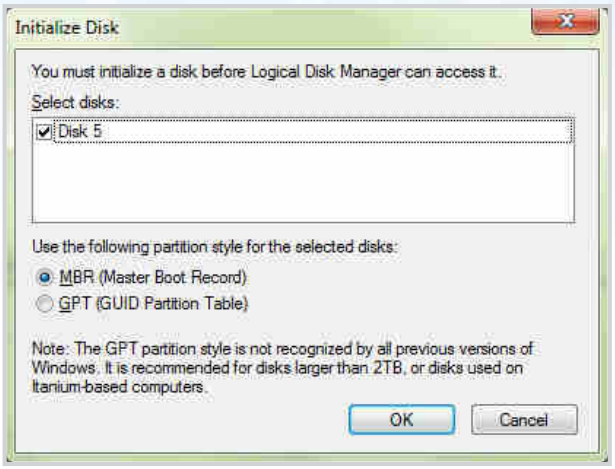
4. **Windows 7:** Кликнуть правой кнопкой мыши на **Компьютер,** затем **Управление,** затем выбрать **Управление дисками**
Windows 8: Кликнуть правой кнопкой мыши в левом верхнем углу рабочего стола и выбрать "Управление дисками"
Windows 10: Кликнуть правой кнопкой мыши на кнопке "Пуск", затем выбрать **Управление дисками.**

5. В диалоговом окне "Упрвление компьютером" кликните на **Управление дисками**. В диалоговом окне "Управление дисками" diskAshur DT² будет отображен как неизвестное устройство, которое не инициализировано и не разбито на логические блоки.

Примечание: Если откроется диалоговое окно "Запустить Disk Wizard", кликните на **Отмена.**

6. Кликните правой кнопкой мыши на "Неизвестный диск", выберите пункт "Инициализировать диск".

7. В диалоговом окне "Инициализировать диск" нажмите **OK**.



8. Кликните правой кнопкой мыши на пустой области и выберите "Новый простой том". Откроется диалоговое окно "Добро пожаловать в New Simple Volume Wizard".

9. Нажмите **Далее**.

10. Если вам нужен только один логический блок примите его размер по умолчанию и нажмите **Далее**.

11. Назначьте приводу букву или путь и нажмите **Далее**.

12. Создайте метку тома, выберите "Выполнить быстрое форматирование" и нажмите **Далее**.

13. Нажмите **Завершить**.

14. Подождите, пока закончится процесс форматирования. После этого устройство будет распознано и готово к использованию.

30. Установка устройства на платформе Mac OS

Привод diskAshur DT² был отформатирован в файловой системе NTFS для использования в ОС Windows. Чтобы переформатировать устройство под файловую систему, совместимую с Mac выполните описанные ниже действия.

После разблокировки устройства выберите пункт Disk Utility из списка Applications/Utilities/Disk Utilities.

Чтобы отформатировать diskAshur DT² нужно:

1. Выбрать diskAshur DT² в списке дисков и томов. Каждое устройство в этом списке отображается с указанием объема, производителя и наименования изделия, например 'iStorage diskAshur DT² Media' либо 232.9 diskAshur DT².

2. Кликните на кнопке 'Erase' (рис. 1).

Рис. 1

3. Введите название устройства (рис. 2). По умолчанию используется название Untitled. Название устройства будет отображаться на рабочем столе.

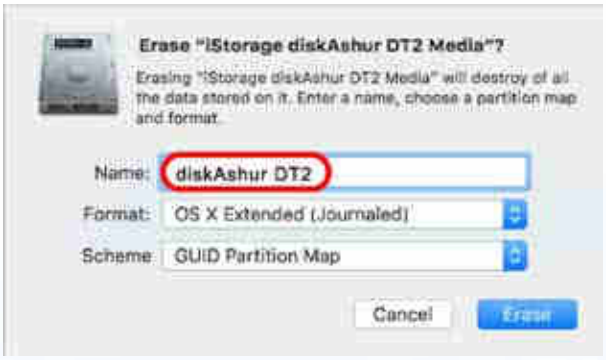


Рис. 2

4. Выберите схему и формат тома, который будет использоваться. В выпадающем меню Volume Format (рис. 3) перечислены все доступные форматы, совестимые с платформой Mac. Рекомендуемый формат: 'Mac OS Extended (Journaled).' В выпадающем меню Scheme format отображаются доступные схемы (рис. 4). Мы рекомендуем использовать схему 'GUID Partition Map' для устройств с объемом более чем 2TB.

Рис. 3

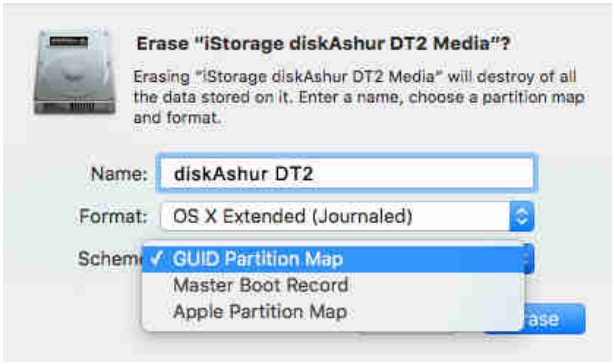


Рис. 4

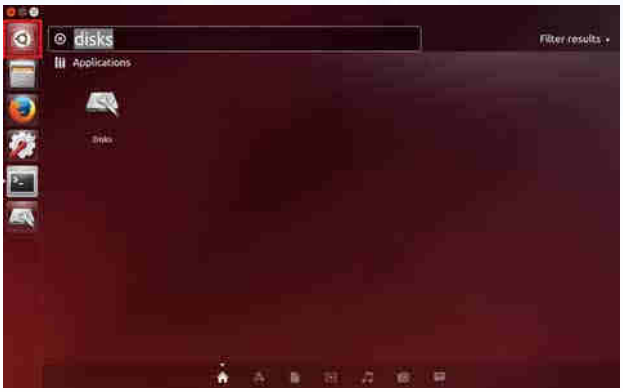
5. Нажмите 'Erase'. Программа Disk Utility отключит том от рабочего стола, сотрет данные и снова подключит его к рабочему столу.

31. Установка устройства на платформе Linux (Ubuntu 14.04)

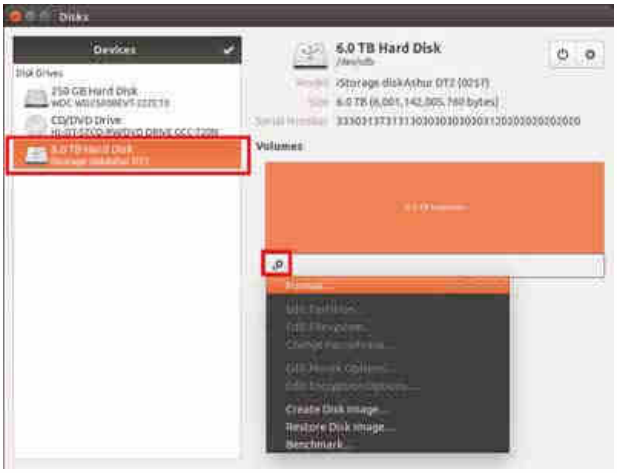
Если ваше устройство было инициализировано и отформатировано в файловой системе NTFS для Windows, вы сразу можете использовать его на платформе Ubuntu. Если возникли проблемы, выполните действия, приведенные ниже.

Чтобы отформатировать diskAshur DT² в файловой системе FAT:

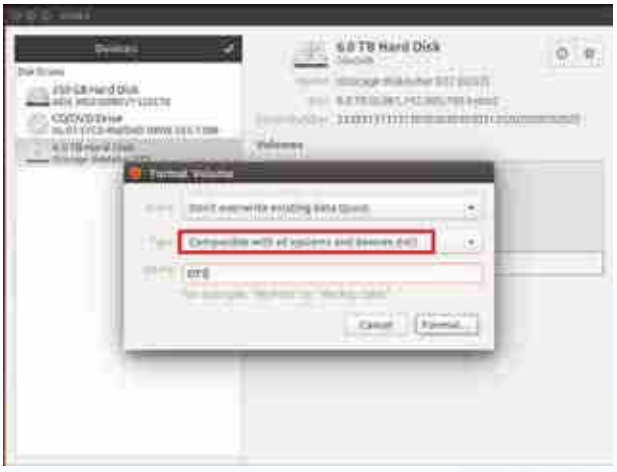
1. Откройте '**Unity Dash**' и наберите '**Disks**' в строке поиска. Выберите диспетчер 'Disks', когда он отобразится.



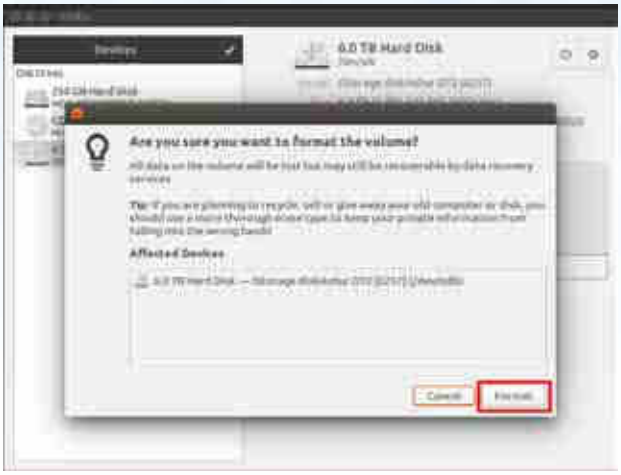
2. Кликните на названии устройства (6.0 TB Hard Disk), чтобы выбрать его в разделе 'Devices'. Затем кликните на иконке с шестеренками под разделом 'Volumes', а затем выберите '**Format**'.



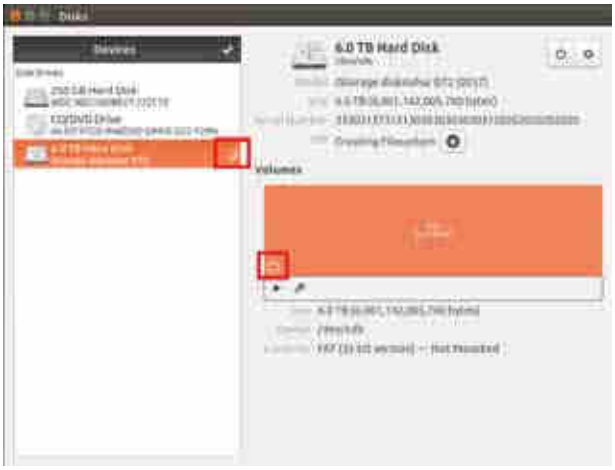
3. Выберите опцию '**Compatible with all systems and devices(FAT)**' в поле 'Type'. Затем введите название устройства, например: diskAshur DT². Затем снова нажмите кнопку '**Format**'.



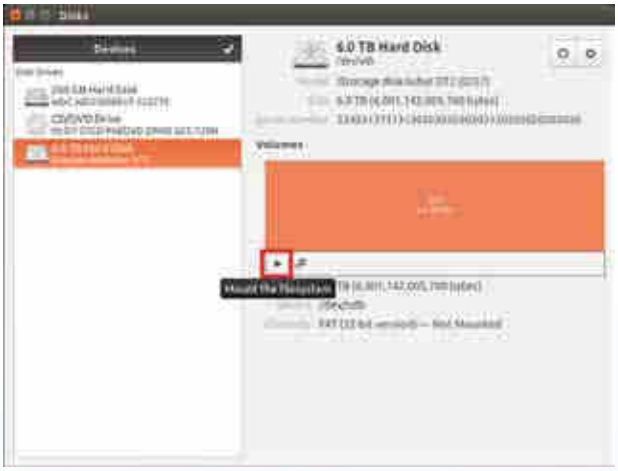
4. Еще раз нажмите '**Format**'.



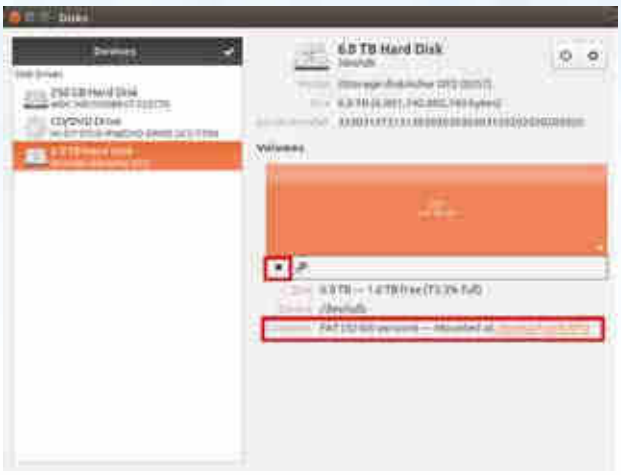
5. Запустится процесс форматирования устройства.



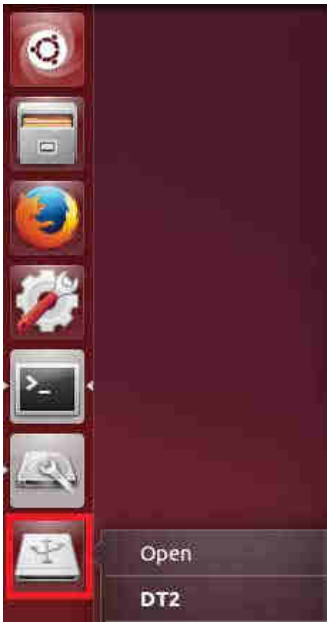
6. После того, как процесс форматирования завершится, кликните на ▶ , чтобы подключить устройство к системе.



7. Теперь привод должен быть подключен к Ubuntu и готов к использованию.



8. Отобразится иконка диска как показано на иллюстрации ниже.
Кликните на эту иконку, чтобы получить доступ к данным, хранящимся на носителе.



Блокировка устройства на Linux (Ubuntu 14.04)

Настоятельно рекомендуется извлекать (блокировать) устройство посредством клика правой кнопкой мыши на '**Safely remove**' на рабочем столе ОС, в особенности если производилась запись или удаление данных.

32. Спящий режим, приостановка или выход из операционной системы

Убедитесь в том, что вы сохранили и закрыли все файлы, расположенные на diskAshur DT² перед тем, как операционная система перейдет в спящий режим, будет приостановлена ее работа или вы осуществите выход из системы.

Рекомендуется блокировать устройство вручную, перед тем как операционная система перейдет в спящий режим, будет приостановлена ее работа или вы выполните выход из нее.

Чтобы выполнить блокировку просто нажмите кнопку 'БЛОКИРОВАТЬ' на самом устройстве либо кликнув на иконку 'Безопасно изъять аппаратное средство/Изъять' в вашей операционной системе.

ВНИМАНИЕ: Чтобы обеспечить сохранность своих данных, если вы отлучаетесь от компьютера блокируйте diskAshur DT²

33. Как проверить прошивку в режиме администратора

Чтобы проверить ревизионный номер прошивки устройства сначала перейжите в "**Режим администратора**", выполнив действия, описанные в разеле 7. Если Режим администратора активен (горит ГОЛУБОЙ индикатор) выполните следующие действия.

1. В режиме администратора нажмите и удерживайте кнопки "3 + 8" пока ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы не мигнут синхронно.		Горящий ГОЛУБОЙ индикатор сменится мигающими ЗЕЛЕНЫМ и ГОЛУБЫМ индикаторами

2. Нажмите кнопку "**РАЗБЛОКИРОВАТЬ**" и произойдет следующее:

a. Все индикаторы (КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ) загорятся на 1 секунду.
б. Мигания КРАСНОГО индикатора означают целую часть ревизионного номера.
в. Мигания ЗЕЛЕНОГО индикатора означают дробную часть ревизионного номера.
г. Все индикаторы (КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ) загорятся на 1 секунду.
д. Загорится ГОЛУБОЙ индикатор.

Например, если ревизионный номер прошивки '1.2', то КРАСНЫЙ индикатор мигнет один (1) раз, а ЗЕЛЕНЫЙ индикатор мигнет два (2) раза. Как только последовательность сигналов завершится, КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы мигнут синхронно, а затем загорится ГОЛУБОЙ индикатор.

34. Как проверить прошивку в режиме пользователя

Чтобы проверить ревизионный номер прошивки устройства сначала перейжите в “**Режим пользователя**”, выполнив действия, описанные в разеле 23. Если Режим администратора активен (горит ЗЕЛЕНЫЙ индикатор) выполните следующие действия.

1. В режиме пользователя нажмите и удерживайте кнопки “3 + 8” пока ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы не мигнут синхронно.		Горящий ЗЕЛЕНЫЙ индикатор сменится мигающими ЗЕЛЕНЫМ и ГОЛУБЫМ индикаторами

2. Нажмите кнопку “**РАЗБЛОКИРОВАТЬ**” и произойдет следующее:

a. Все индикаторы (КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ) загорятся на 1 секунду .
б. Мигания КРАСНОГО индикатора означают целую часть ревизионного номера.
в. Мигания ЗЕЛЕНОГО индикатора означают дробную часть ревизионного номера.
г. Все индикаторы (КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ) загорятся на 1 секунду.
д. Загорится ЗЕЛЕНЫЙ индикатор.

Например, если ревизионный номер прошивки ‘1.2’, то КРАСНЫЙ индикатор мигнет один (1) раз, а ЗЕЛЕНЫЙ индикатор мигнет два (2) раза. Как только последовательно сигналов завершится, КРАСНЫЙ, ЗЕЛЕНЫЙ и ГОЛУБОЙ индикаторы мигнут синхронно, а затем загорится ГОЛУБОЙ индикатор.

35. Техническая поддержка

Компания iStorage предоставляет вам следующие полезные информационные ресурсы:

Официальный сайт iStorage: https://www.istorage-uk.com E-mail для связи: support@istorage-uk.com
Техническая поддержка нашего технического отдела: +44 (0) 20 8991-6260.
Специалисты технического отдела iStorage работают с 9:00 до 17:30 (время Гринвича) с понедельника по пятницу.

Поддержка на территории России, Украины и Казахстана осуществляет компания Dataway Security

www.datawaysecurity.ru и www.datawaysecurity.com.ua
E-mail: support@datawaysecurity.com

36. Информация по гарантии и RMA

Двухлетняя гарантия:

iStorage предоставляет 2-летнюю гарантию на диск iStorageAshur DT2 на возможные дефекты материалов и производства при условии соблюдения всех правил его эксплуатации. Гарантийный срок наступает с даты покупки либо непосредственно у производителя, либо у его авторизованного торгового представителя.

Отказ от ответственности и условия гарантии:

ГАРАНТИЯ ДЕЙСТВУЕТ С ДАТЫ ПОКУПКИ И ДОЛЖНА БЫТЬ ПОДТВЕРЖДЕНА ЧЕКОМ ИЛИ СЧЕТОМ-ФАКТУРОЙ, ГДЕ УКАЗАНА ДАТЫ ПРОДАЖИ ТОВАРА. ISTORAGE БЕЗ ДОПОЛНИТЕЛЬНЫХ ЗАТРАТ ДЛЯ ПОКУПАТЕЛЯ ВЫПОЛНИТ РЕМОНТ ИЛИ ЗАМЕНУ БРАКОВАННЫХ ДЕТАЛЕЙ НОВЫМИ ЛИБО ОТРЕМОНТИРОВАННЫМИ И ГОТОВЫМИ К ЭКСПЛУАТАЦИИ ДЕТАЛЯМИ. ВСЕ ДЕТАЛИ И ЗАПЧАСТИ ТОВАРА, ЗАМЕНЕННЫЕ В СООТВЕТСТВИИ С НАСТОЯЩЕЙ ГАРАНТИЕЙ, СТАНОВЯТСЯ СОБСТВЕННОСТЬЮ ISTORAGE. НАСТОЯЩАЯ ГАРАНТИЯ НЕ РАСПРОСТРАНЯЕТСЯ НА ТОВАР, НЕ ПРИОБРЕТЕННЫЙ НАПРЯМУЮ У ПРОИЗВОДИТЕЛЯ ЛИБО У ЕГО АВТОРИЗОВАННОГО ТОРГОВОГО ПРЕДСТАВИТЕЛЯ, ЛИБО В СЛУЧАЕ: 1.ПОВРЕЖДЕНИЯ, НЕПРАВИЛЬНОЙ ЭКСПЛУАТАЦИИ, ОТКАЗА ИЛИ НЕВОЗМОЖНОСТИ СОБЛЮДАТЬ РЕКОМЕНДАЦИИ, ПРЕДУСМОТРЕННЫЕ В НАСТОЯЩЕМ РУКОВОДСТВЕ ПО ЭКСПЛУАТАЦИИ: 2. ИСПОЛЬЗОВАНЯ ЗАЧАСТЕЙ, НЕ ИЗГОТОВЛЕННЫХ НА ЗАВОДЕ ПРОИЗВОДИТЕЛЯ; 3. МОДИФИКАЦИИ ТОВАРА; ИЛИ 4. В РЕЗУЛЬТАТЕ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ ИЛИ РЕМОНТА ЛИЦАМИ, НЕ АВТОРИЗОВАННЫМИ ISTORAGE. ДАННАЯ ГАРАНТИЯ НЕ РАСПРОСТРАНЯЕТСЯ НА ЕСТЕСТВЕННЫЙ ИЗНОС. КОМПАНИЯ ISTORAGE НЕ ДАЕТ НИКАКИХ ДРУГИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ ЛЮБЫЕ ГАРАНТИИ ПРИГОДНОСТИ ДЛЯ КОНКРЕТНЫХ ЦЕЛЕЙ, В ОТНОШЕНИИ ТОВАРА И ЕГО УСТАНОВКИ, ИСПОЛЬЗОВАНИЯ, ЭКСПЛУАТАЦИИ, ЗАМЕНЕ И РЕМОНТУ. ПО УСЛОВИЯМ НАСТОЯЩЕЙ ГАРАНТИИ ПРОИЗВОДИТЕЛЬ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБОЙ СЛУЧАЙНЫЙ, УМЫШЛЕННЫЙ ИЛИ КОСВЕННЫЙ УЩЕРБ (В ТОМ ЧИСЛЕ, ПОТЕРЯ ДАННЫХ), СВЯЗАННЫЙ С ИСПОЛЬЗОВАНИЕМ ИЛИ ФУНКЦИОНИРОВАНИЕМ ДАННОГО ТОВАРА.

Приложение A

Директива безопасности iStorage #1 – Функции безопасности и безопасное обращение

Данная директива iStorage обеспечивает поддержку продукта для использования коммерческими, общественными и государственными учреждениями, а также продуктов iStorage (дисков с высокой степенью защиты данных), с применением положений нормативного документа NCSC CESG , таких как:

CPA Обеспечение безопасности и шифрование аппаратных носителей данных Версия 1.2, апрель 2012 г.

Директива безопасноти №1 представляет собой описание функций обеспечения безопасности информации, используемых в аппаратных средствах хранения данных производства iStorage, а также набор наиболее важных рекомендаций по защите чувствительной и конфиденциальной информации, хранимой на приводах iStorage, как при использовании в рабочем помещении, так и вне его, а также в процессе транспортировки устройств хранения данных iStorage.

Функции безопасности устройств в сочетании с практическими рекомендациями по защите данных способны существенно снизить риск физических атак или кражи данных, а также возможности скомпрометировать активы данных, хранящиеся на дисках iStorage, чтобы лишить возможности несанкционированного доступа к защищенному содержимому.

Риски: безопасные устройства хранения данных от iStorage относятся к ценным и привлекательным объектам, которые могут содержать секретную коммерческую, государственную или персональную информацию и являться целью для физических и логических атак в виде кражи и повреждения данных будучи:

- Оставленными без присмотра
- Видимыми в людных местах
- Оставленными на открытой местности
- Недостаточно защищенными при транспортировке
- Не заданы необходимые настройки безопасности для особо важных данных

В данной директиве №1 мы приводим наиболее эффективные программные и практические меры по предовращению любых возможных атак.

Меры по обеспечению безопасности данных: Все функции безопасности, а также меры предосторожности, которые необходимо соблюдать при транспортивке, хранении и эксплуатации устройств хранения данных, приведены в **Таблице 1** ниже. Наш подход базируется на ключевых принципах безопасности CIA+A (Конфиденциальности, Целостность, Доступность + Учетность), которые признаны эффективными согласно стандарту ISO/IEC 27001, а также упоминавшегося нормативного документа NCSC CESG.

Таблица 1 – Принципы – Функции устройства - Меры безопсности при эксплуатации

Принцип	NCSC (CESG) CPA	Риск	Рекомендации
1 Целостность Доступность Учетность	DEP.M311 DEP.1.M26	В дороге	Никогда не оставляйте устройство на виду и без присмотра в транспортном средстве. Если устройство необходимо оставить без присмотра, убедитесь, что оно не на виду и что транспортное средство закрыто на замок. Если вы используете привод iStorage в процессе деловой активности, отправляя его пользуйтесь услугами только отслеживаемых и проверенных курьерских служб. Устройства хранения данных поставляются в запечатанной защитной коробке. Если при получении печать безопасности повреждена, либо видны признаки попыток еее повреждения, немедленно сообщите об этом в нашу службу поддержки по номеру: +44 (0) 20 8991-6260 Либо на e-mail: support@istorage-uk.com

Принцип	NCSC (CESG) CPA	Риск	Рекомендации
Конфиденциальность Целостность Доступность	DEP.M1 DEP.M701	Несакционированный доступ	Чтобы минимизировать угрозу повреждения данных на устройствах хранения от iStorage: Никогда не оставляйте устройство без присмотра с авторизованной открытой рабочей сессией Чтобы избежать попыток несанкционированного доступа, всегда блокируйте устройства, когда не работаете с ними Настройте таймер автоблокировки привода iStorage, чтобы устройство автоматически заблокировалось через указанный промежуток времени (процесс настройки описан в данном руководстве) Если устройство не используется, убедитесь, что оно отключено от компьютера и помещено в сейф с замком. Регулярно выполняйте резервное копирование данных на случай попыток несанкционированного доступа или непредвиденных сбоев в работе устройства.
3 Конфиденциальность Учетность	DEP.M703	Утеря, кража, повреждение	Удостоверьтесь, что руководство оповещено про факт кражи, утери или повреждении данных на устройстве хранения iStorage В случае, если на диске iStorage находилась особо важная, либо представляющая государственную тайну информация, обратитесь в соответствующую службу или орган. Убедитесь, что данные были защифрованы на момент их утери или кражи (устройство хранения не находилось в режиме открытой сессии), что не позволит повредить чувствительную информацию или другие формы связанных с ней данных.
4 Целостность	DEP.1.M26	Защита от несанкциониро-ванного доступа	Устройства iStorage оснащены защитой от несанкционированного доступа. Проводите регулярную проверку внешнего футляра устройства iStorage на предмет наличия признаков попытки несанкционированного проникновения. **Примечание 1:** Если были выявлены признаки несанкционированного вскрытия, немедленно сообщите об этом в компетентные структуры.
5 Конфиденциальность Целостность	DEP.2.M12 DEP.2.M283 DEP.2.M285 DEP.2.M617	Строгое управление паролем	Пароль никогда не отображается при вводе. Всегда устанавливайте сложные пароли администратора и пользователя, чтобы максимально обезопасить устройство хранения данных от логических атак Несмотря на то, что привод позволяет использовать пароль из 7 символов, мы настоятельно рекомендуем пользователям устанавливать пароль более высокой сложности, например: 8 символов с комбинацией кнопки **ПЕРЕКЛЮЧИТЬ** и цифры Используйте конструкцию пароля, которую было бы крайне непросто подобрать.

Принцип	NCSC (CESG) CPA	Риск	Рекомендации
			Избегайте использования одинакового пароля в разных системах с различным уровнем безопасности Никогда не записывайте пароли на бумаге Никому не сообщайте пароль Следите за тем, чтобы никто не подсматривал, когда вы вводите пароль в публичном месте Если вы подозреваете, что ваш пароль был скомпромитирован, смените его при первой возможности Если существует необходимость зафиксировать пароль на жестком носителе, делайте это с максимальной осторожностью. **Примечание 2:** Существует специальное программное обеспечение для безопасного хранения паролей, либо можно использовать специальный запечатанный конверт с особыми средствами защиты от физического проникновения.
6 Конфиденциальность Целостность	**DEP.2.M281**	**Управление паролем администратора**	Устройство хранения данных iStorage оснащено функционалом администратора, который обладает привилегированным уровнем доступа к данным. Только авторизованные и аутентифицированные администраторы могут добавлять или отзывать учетные записи.
7 Конфиденциальность	**DEP.2.M277**	**Социальная инженерия**	Помните о потенциальной косвенной угрозе атак, целью которых может быть кража вашего пароля и других деловых или личных данных с помощью методов социальной инженерии.
8 Конфиденциальность Целостность	**DEP.2.M280**	**Распространение данных учетной записи**	Никогда не сообщайте и не передавайте какие-либо конфиденциальные данные по одному и тому же каналу связи либо в комплекте с устройством iStorage. **Примечание 3:** В тех случаях, когда есть необходимость передать данные учетной записи третьим лицам, это должно быть сделано вне сетей публичного доступа (например, голосом, текстом, по защищенной электронной почте)
9 Целостность	**DEP.4.M348** **DEP.1.M348**	**Авторизация обновлений**	Никаких автообновлений. Только подтвержденные пользователем обновления для продуктов iStorage будут выполняться в рамках внутренней политики iStorage SDLC по управлению уязвимостями.

Принцип	NCSC (CESG) CPA	Риск	Рекомендации
10 Конфиденциальность Учетность		**Классификация данных**	Убедитесь, что ценность данных, хранящихся на защищенном диске iStorage, классифицирована или имеет защитную маркировку, соответствующую их использованию и / или хранению.
11 Конфиденциальность		**Доступ для проверенных сотрудников**	Убедитесь, что те, кому предоставлен доступ к данным, хранящимся на защищенном диске iStorage, обладают четким пониманием и соответствуют степени ценности и секретности материалов с защитной маркировкой, хранящихся на нем.

Приложение B

Директива безопасности iStorage №2 – Санитарная обработка и безопасная утилизация

Данная директива iStorage обеспечивает поддержку данного продукта для использования коммерческими, общественными и государственными учреждениями, а также других продуктов iStorage. Данная директива безопасности iStorage №2 содержит рекомендции по процессам санитарной обработки и безопасной утилизации устройств хранения данных.

В этой директиве также содержатся рекомендации по повторному выпуску защищенных дисков в целях снижения риска повреждения данных, хранящихся на защищенных дисках iStorage при их повторном выпуске.

Риск: Если безопасность каких-либо данных, хранящихся на диске iStorage, не контролируется в процессе переработки или утилизации по окончании срока эксплуатации, такие данные могут подвергаться рискам, затрагивающим безопасность организации, и обязательным элементам защиты, таким как GDPR. Например:

- Эксфильтрация и передача конфиденциальных данных несанкционированным внешним субъектам
- Случайное разглашение
- Раскрытие защищенных или государственных секретных данных

Цель: Несмотря на то, что носители iStorage обеспечивают защиту хранящихся на них данных с помощью надежной системы шифрования, тем не менее, наилучшей практикой безопасности является обеспечение того, чтобы в случаях, когда защищенные диски iStorage передаются другим сторонам, хранителям, отделам или когда они утилизируются по истечении сроков эксплуатации, чтобы устройства подвергались процессам, гарантирующим надежную очистку и полное удаление любых остатков ранее хранившихся данных с этого диска, снижая тем самым вероятность компрометации этих данных.

CPA Обеспечение безопасности и шифрование аппаратных носителей данных Версия 1.2, апрель 2012 г.

В этой директиве безопасности iStorage №2 мы описываем наиболее эффективные и действенные меры, которые следует предпринять в целях предотвращения компрометации важных данных.

Меры по обеспечению безопасности данных: Все функции безопасности, а также меры предосторожности, которые необходимо соблюдать при транспортивке, хранении и эксплуатации устройств хранения данных, приведены в **Таблице 1** ниже. Наш подход базируется на ключевых принципах безопасности CIA+A (Конфиденциальности, Целостность, Доступность + Учетность), которые признаны эффективными согласно стандарта ISO/IEC 27001, а также упоминавшегося нормативного документа NCSC CESG.

Процесс: На **Рис. 1** ниже представлен высокоуровневый поток данных, относящийся к:

- Безопасной утилизации
- Санитарной обработке
- Особо охраняемым данным и данным государственной важности
- Повторному выпуску устройств хранения данных iStorage

Рис. 1 – Процесс санитарной обработки и утилизации

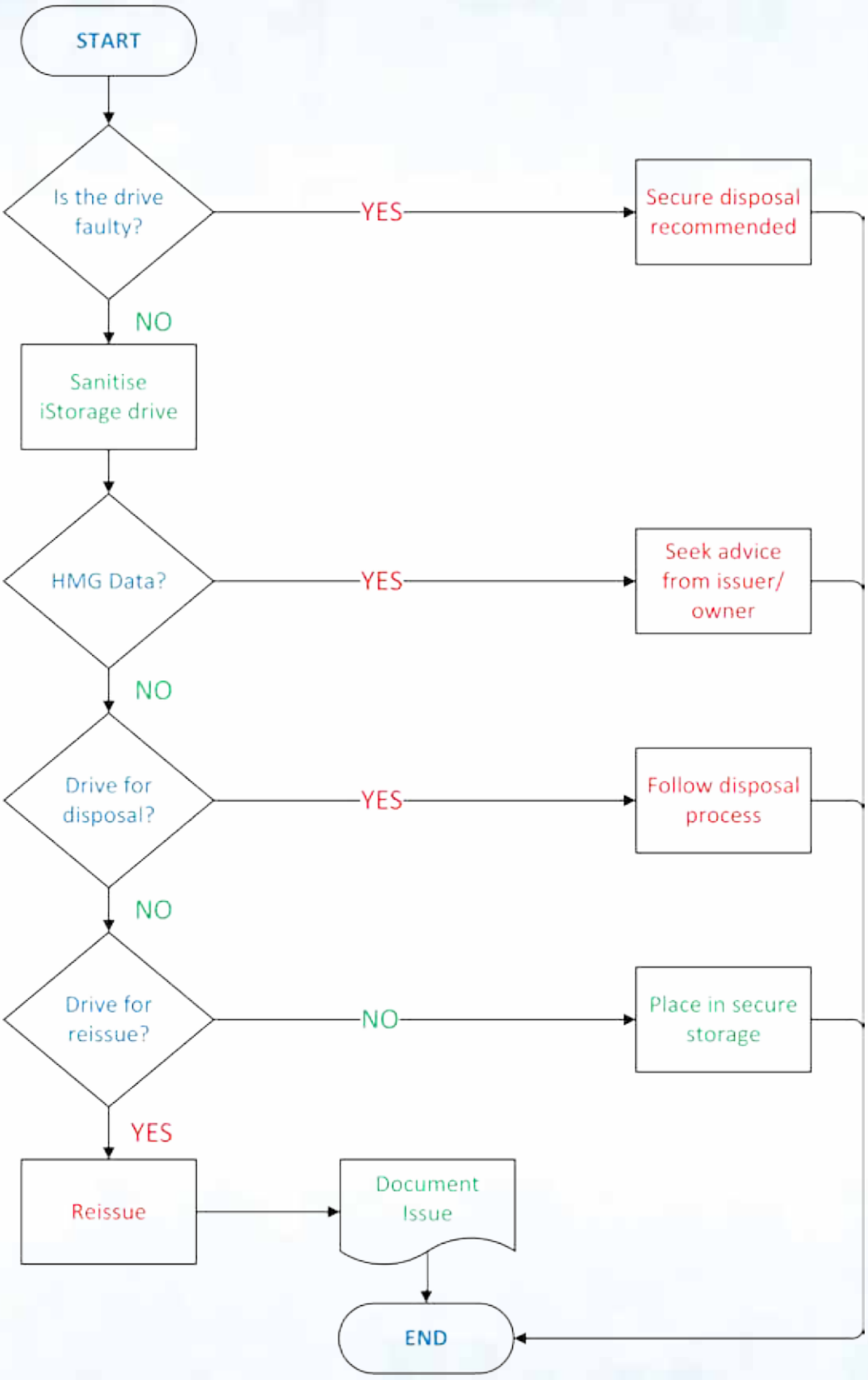


Таблица 1 – Меры безопсности - Санитарная обработка и безопасная утилизация

Принцип	NCSC (CESG) CPA	Риск	Рекомендации
1 Конфиденциальность Учетность	DEP.M1	**Хранение**	Убедитесь, что все устройства iStorage, ожидающие санитарной обработки или безопасной утилизации, полностью документированы и учтены, а также, что они хранятся на защищенном объекте, оснащенном надежными механизмами и процедурами контроля доступа и безопасности. **Примечание 1:** В зависимости от количества устройств, ожидающих обработки, это может быть хорошо запертая комната либо кабинет безопасности.
2 Конфиденциальность Учетность	DEP.M311	**В дороге**	Никогда не оставляйте устройство на виду без присмотра в транспортном средстве. Если устройство необходимо оставить без присмотра, убедитесь, что оно не на виду и что транспортное средство закрыто на замок. Все усройства iStorage, предназначенные для обработки средствами безопасного уничтожения, должны сопровождаться только надежной логистической или курьерской службой. В тех случаях, когда на устройствах iStorage хранятся данные, отмеченные защитной маркировкой либо секретные данные государственной важности, следует обратиться за консультацией в соответствующий орган или агентство, чтобы удостовериться, есть ли требование применять дополнительные средства контроля (например, транзитная связь при контакте с экстренными службами или резервное транспортное средство)
3 Конфиденциальность Учетность		**Защитная маркировка**	В тех случаях, когда на устройствах iStorage хранятся защищенные маркировкой данные, относящиеся к государственным секретным данным, следует обратиться в соответсвущую структуру за рекомендациями относительно требований к учету и безопасной утилизации защищенных носителей.
4 Конфиденциальность Учетность		**Учетность**	Все носители iStorage, ожидающие санитарной обработки или безопасной утилизации, должны быть обязательно учтены в реестре с указанием: • Серийного номера • Владельца/Отдела • Даты получения • Классификации активов данных или защитной маркировки • Любых специальных предупреждений • Даты отправки на обработку **Примечание 2:** В тех случаях, когда диск iStorage прошел санитарную обработку для перевыпуска, он должен быть внесен в отдельный реестр устройств, ожидающих передачи новому владельцу / хранителю / отделу.

Принцип	NCSC (CESG) CPA	Риск	Рекомендации
5 Доступность		**Непрерывность работы**	Перед тем, как любое устройство iStorage будет подвергнуто санитарной обработке или безопасной утилизации, необходимо запросить подтверждение того, что все хранящиеся на нем данные учтены и скопированы в соответствии с требованиями, в целях избежания непреднамеренного удаления операционных данных, хранимых на носителе.
6 Конфиденциальность Учетность	**DEP.M137**	**Методы санитарной обработки**	Методы санитарной обработки, которые используются при обработке любых носителей данных iStorage, должны сопровождаться документированными процедурами очистки и процедурами операционной безопасности (SyOps); Такие процедуры должны выполняться после соответствующих процессов, относящихся к конкретному типу носителя, различной защитной маркировке или другой государственной классификации актива данных, подвергаемого санитарной обработке для обеспечения соответствия минимальным стандартам HMG. Выбранный исполнитель работ должен подтвердить, что все эти процедуры выполняются на практике. Рекомендации NCSC (частично GCHQ) доступны по ссылке: https://www.ncsc.gov.uk/index/topic/164
7 Целостность	**DEP.M137**	**Санитарная обработка и утилизация**	Санитарная обработка и утилизация всех продуктов iStorage должны выполняться в соответствии с документированными операционными процедурами производителя, руководствами пользователя и любыми другими опубликованными нормами безопасности. Персонал или команда специалистов, которые проводят санитарную обработку или безопасную утилизацию, должны быть обучены правильному использованию соответствующего оборудования. Должны быть предусмотрены мероприятия по проверке того, что оборудование используется правильно и в соответствии с рекомендациями производителей.
8 Конфиденциальность Учетность		**Перевыпуск устройства для хранения данных**	В тех случаях, когда устройство iStorage было подвергнуту санитарной обработке для перевыпуска и передачи новому пользователю, хранителю или отделу, перед его передачей необходимо провести проверку, чтобы убедиться, что носитель полностью пуст. Руководство пользователя устройства хранения данных iStorage должно быть выдано пользователю-получателю и содержать четкие инструкции по его безопасному использованию. Выпуск безопасного носителя данных iStorage должен быть полностью задокументирован и внесен в реестр активов.

Принцип	NCSC (CESG) IAS5	Риск	Рекомендации
9 Конфиденциальность Учетность	**DEP.M703**	**Утеря, кража, повреждение**	Удостоверьтесь, что руководство оповещено про факт кражи, утери или повреждения данных на устройстве хранения iStorage В случае, если на диске iStorage находилась особо важная, либо представляющая государственную тайну информация, обратитесь в соответствующую службу или орган. Убедитесь, что данные были защифрованы на момент их утери или кражи (устройство хранения не находилось в режиме открытой сессии), что не позволит повредить чувствительную информацию или другие формы связанных с ней данных.
10 Конфиденциальность	**MIT003**	**Доступ для проверенных сотрудников**	Убедитесь, что те, кому предоставлен доступ к данным, хранящимся на защищенном диске iStorage, обладают четким пониманием и соответствуют степени ценности и секретности материалов с защитной маркировкой, хранящихся на нем.

iStorage®

iStorage Limited, iStorage House, 13 Alperton Lane
Perivale, Middlesex. UB6 8DH, England
Tel: +44 (0) 20 8991 6260 | Fax: +44 (0) 20 8991 6277
e-mail: info@istorage-uk.com | web: www.istorage-uk.com