УТВЕРЖДЕН
СЮИК.466216.001 РЭ-ЛУ

# УСТРОЙСТВО ХРАНЕНИЯ ИНФОРМАЦИИ ЗАЩИЩЕННОЕ МОБИЛЬНОЕ "МЕРКУРИЙ"

**Руководство по эксплуатации**
СЮИК. 466216.001РЭ

## Содержание

Настоящее руководство по эксплуатации (РЭ) распространяется на устройство хранения информации защищенное мобильное (далее по тексту УХИ "Меркурий") – устройство, выполняющее функции защищенного от несанкционированного доступа хранения информации (НСД) путем шифрования по ГОСТ 28147-89, хранения информации в области аппаратно защищенной от записи и контроля целостности информации путем вычисления значения хеш-функции по СТБ 1176.1-99.

Данный документ является объединенным эксплуатационным документом, удостоверяющим гарантированные предприятием-изготовителем основные параметры и технические характеристики УХИ «Меркурий» и содержащим сведения по эксплуатации и ремонту.

Руководство по эксплуатации адресовано специалистам, которые занимаются организацией защиты информации на предприятии и имеют знания в области защиты информации программными методами.

Руководство по эксплуатации описывает следующее:

- принцип работы УХИ «Меркурий»;
- порядок хранения и транспортирования УХИ «Меркурий»;
- порядок ввода в эксплуатацию УХИ «Меркурий»;
- описание аварийных ситуаций.

При записи в документе не допускаются записи карандашом, смывающимися чернилами и подчистки.

Неправильная запись должна быть аккуратно зачеркнута и рядом записана новая, которую заверяет лицо, ответственное за эксплуатацию ПЭВМ. После подписи проставляют фамилию и инициалы ответственного лица (вместо подписи допускается проставлять личный штамп исполнителя).

**Внимание! Не извлекайте устройство из разъема USB, не отключив его от ПЭВМ логически!**

**Помните: до ввода пароля зашифрованная область выглядит как неотформатированное пространство. Если Вы решите отформатировать ее – информация, хранящаяся в ней, будет навсегда утеряна!**

**Вам поставляется инициализированное устройство с транспортными ключами. При первом же включении выполните инициализацию устройства и смените пароль доступа в соответствии с 2.3.2.7.**

**По умолчанию устройство блокирует работу в сети. Для снятия блокировки необходимо выполнить п. 2.4.6.4.**

# 1 Описание и работа УХИ «Меркурий»

## 1.1 Назначение

1.1.1 УХИ "Меркурий" является персональным устройством и предназначено для защиты информации ограниченного распространения при ее обработке и хранении, под управлением ОС семейства MS Windows 2000/XP/2003/Vista/7.

УХИ «Меркурий» обеспечивает выполнение следующих функций:

а) аутентификацию субъекта, зарегистрированного в УХИ «Меркурий» по паролю, при этом имя пользователя используется по умолчанию и не отображается;

б) смену ключевой информации в случае компрометации ключей;

в) защиту информации путем помещения ее в область, предназначенную только для чтения;

г) защиту данных пользователя путем шифрования по ГОСТ 28147-89 в области доступной для чтения и записи;

д) контроль пользователем целостности информации и периодическое тестирование УХИ «Меркурий»;

е) хранение ключей пользователя вне файловой системы (16 областей по 64 кБайт) с организацией доступа к ним через специальный программный интерфейс;

ж) ведения журнала действий пользователя (при работе с использованием режима к), журнал ведется средствами операционной системы);

з) введения ограничения на количество исполняемых при использовании УХИ «Меркурий» программ;

и) экстренного уничтожения хранимой информации,

к) использование в режиме, исключающем несанкционированный перенос незашифрованной информации на USB-накопителе за пределы ПЭВМ, работающей в локальной сети.

## 1.2 Основные сведения об изделии и технические данные

### 1.2.1 Основные сведения

Наименование изделия: "Устройство хранения информации защищенное мобильное «Меркурий». ТУ BY 100037461.005-2009".

Обозначение изделия СЮИК.466216.001

Дата изготовления _____

Изготовитель _____ЗАО "НТЦ КОНТАКТ"_____

220007 г. Минск, пер. Студенческий, 7_____

наименование и почтовый адрес предприятия-изготовителя

Заводской номер _____

### 1.2.2 Технические характеристики

1.2.2.1 УХИ «Меркурий» имеет следующие технические характеристики:

- габаритные размеры – не более 100×20×8 мм;
- масса – не более 0,1 кг;
- напряжения питания – плюс 5 В;
- объем накопителя не менее 1024 Мбайт;
- защита хранимой информации путем шифрования по ГОСТ 28147-89;
- контроль целостности информации по СТБ 1176.1 – 99;
- тип используемой шины ПЭВМ – USB 2.0;
- обмена с ПЭВМ не менее 5Мбайт/сек;
- время хранения информации в УХИ «Меркурий» при отключении питания – не менее 5 лет;
- средняя наработка на отказ – не менее 1000000 операций записи или 6000 ч;
- срок службы – не менее 10 лет.

### 1.2.3 Сведения о содержании драгоценных материалов и цветных металлов

1.2.3.1 Драгоценные металлы в УХИ «Меркурий» отсутствуют.

### 1.3 Комплектность

1.3.1 Состав УХИ «Меркурий» приведен в таблице 2.

Таблица 2

| Обозначение изделия | Наименование изделия | Кол-во (шт.) | Заводской номер | Приме-чание |
|---|---|---|---|---|
| - | Накопитель | 1 | | |
| СЮИК.00380.01 | Комплект программного обеспечения | 1 | | Компакт-диск |
| СЮИК.466216.001 РЭ | Руководство по эксплуатации | 1 | | Компакт-диск |

## 1.4 Устройство и работа УХИ «Меркурий»

### 1.4.1 Устройство

1.4.1.1 УХИ «Меркурий» состоит из:

- накопителя U3;
- комплекта программного обеспечения.

### 1.4.2 Принцип работы

1.4.2.1 УХИ «Меркурий» представляет собой внешнее устройство, подключаемое к шине USB, состоящее из двух областей: открытой и защищенной. Открытая область доступна только для чтения информации и предназначена для размещения ПО, защищенная область доступна для чтения и записи информации и предназначена для хранения данных в зашифрованном виде. Внешний вид накопителя U3 представлен на рисунке 1. Внешний вид накопителя зависит от производителя и может меняться от модели к модели.

Рисунок 1

При подключении устройства к шине USB пользователю доступна только область, защищенная от записи. Зашифрованная область в это время выглядит как неотформатированное

пространство и не защищена от записи или форматирования. Выполнение этих операций уничтожит информацию, находящуюся в данной области. После получения запрошенной информации программа подключает шифрующую файловую систему, которая монтирует защищенную область в виде внешнего устройства (накопителя). Эта область всегда остается зашифрованной – данные представляются в расшифрованном виде только в ОЗУ ПЭВМ, что гарантирует их защиту, даже если во время работы будет выключено питание. В случае же утери носителя информация, записанная на нем, будет недоступна нашедшему (или похитившему) этот носитель.

УХИ «Меркурий» может содержать в своем составе операционную систему, и в этом случае оно может обеспечивать создание мобильного изолированного рабочего места, обеспечивающего обработку конфиденциальной информации с гарантированным исключением возможности ее утечки.

Для шифрования информации в УХИ «Меркурий» используются ключи, которые формируются путем вычисления значения хеш-функции от введенного пароля и логического сложения полученного значения с числом длиной 32 байта, хранящимся на накопителе. При использовании функции исключения возможности несанкционированного переноса на накопителе обрабатываемой информации за пределы рабочего места составляющей частью его является секретное число, хранящееся на сервере в зашифрованном на ключе от пароля виде.

Ключи шифрования защищенной области не хранятся в накопителе, а вырабатываются в процессе аутентификации.

Ключи приложений пользователя хранятся в отдельном зашифрованном по ГОСТ 28147-89 средствами СПО разделе накопителя в 16 областях, каждая размером 64 кБайт.

При работе в режиме, исключающем несанкционированный перенос незашифрованной информации на USB-накопителе за пределы ПЭВМ, работающей в локальной сети, часть материала

ключа, используемого для шифрования информации, хранится на сервере в виде, зашифрованном на ключе, выработанном из пароля, и передается программе шифрования по запросу при аутентификации пользователя.

### 1.5 Средства измерения, инструмент и принадлежности

1.5.1 Специальных измерительных приборов, необходимых для работы и настройки УХИ «Меркурий» и выполнения работ по техническому обслуживанию, не требуется.

### 1.6 Маркировка

1.6.1 На накопитель УХИ «Меркурий» нанесена маркировка, содержащая следующие данные:

- наименование и обозначение накопителя;
- заводской номер накопителя по системе нумерации предприятия-изготовителя.

### 1.7 Упаковка

1.7.1 Все компоненты УХИ «Меркурий» и эксплуатационный документ РЭ помещены в запаянный полиэтиленовый мешок согласно 1.3.1. В полиэтиленовый мешок вложен упаковочный лист и силикагель технический.

## 2 Использование по назначению

### 2.1 Эксплуатационные ограничения

2.1.1 Для работы всех компонентов функционирующих с УХИ «Меркурий», необходимо выполнение следующих условий:

- совместимая ПЭВМ, работающая под управлением ОС семейства MS Windows 2000/XP/2003/Vista/7. Тип операционной системы и её разрядность заранее уточняются Заказчиком, поскольку для каждого типа операционной системы требуется своя версия драйвера.
- наличие свободного разъема USB на ПЭВМ.

2.1.2 Для работы с УХИ «Меркурий» пользователь должен быть зарегистрирован в УХИ «Меркурий», для чего ему необходимо

определить:

- пароль и возможность его смены (при необходимости);
- дополнительные меры безопасности (время жизни пароля, период времени, когда пользователю разрешен вход в систему).

После процедуры регистрации, выполняемой администратором безопасности, о ней делается соответствующая запись в реестре учета носителей информации за подписью пользователя.

2.1.3 При работе в режиме, исключающем несанкционированный перенос на накопителе обрабатываемой информации за пределы рабочего места, ключ шифрования формируется из трех составляющих:

– значения хеш-функции по СТБ 1176.1-99, вычисленной от пароля, введенного оператором;

– некоторого числа, хранящегося на накопителе;

– секретной последовательности, хранящейся на сервере в зашифрованном на хеше, вычисленном от пароля, введенного оператором.

2.1.4 При попытке аутентификации пользователя в режиме п.2.1.3 на рабочем месте, отключенном от локальной сети, в которой находится сервер, хранящий часть ключа, будет выведено сообщение об ошибке.

2.1.5 Работа в режиме, исключающем несанкционированный перенос на накопителе обрабатываемой информации за пределы рабочего места, предполагает предварительную настройку рабочего места и сервера для применения УХИ «Меркурий».

2.1.6 На рабочем месте пользователя должно быть установлено программное обеспечение доступа к серверу, хранящему необходимую часть ключа, и оно должно загружаться и исполняться до начала работы с УХИ. На сервере также должно быть установлено соответствующее программное обеспечение и сформирован файл настроек, содержащий номер накопителя, как

поисковую характеристику, и зашифрованный на хеше от пароля секрет.

2.1.7 Для эксплуатации и эффективного применения УХИ «Меркурий», поддержания необходимого уровня защищенности ПЭВМ и информационных ресурсов требуется:

- соблюдение правил хранения УХИ «Меркурий»;
- строгое выполнение требований настоящей инструкции;
- учет носителей информации.

2.1.8 Условия эксплуатации УХИ «Меркурий»:

- температура окружающего воздуха от плюс 10 до плюс 30 °С;
- относительная влажность окружающего воздуха до 80 % при температуре окружающего воздуха плюс 25 °С;
- атмосферное давление от 84 до 107 кПа (630 до 800 мм.рт.ст).

## 2.2 Подготовка УХИ «Меркурий» к использованию

2.2.1 Перед началом работы необходимо внимательно изучить настоящее РЭ.

2.2.2 УХИ «Меркурий» обеспечивает электрическую, механическую и пожарную безопасность персонала в соответствии с требованиями ГОСТ 25861-83 и ГОСТ 30326-95 (МЭК 950-86).

2.2.3 Материалы, применяемые для изготовления УХИ «Меркурий», а также меры обеспечения пожарной безопасности соответствуют требованиям ГОСТ 12.1.004-91, ГОСТ 12.2.006-87 (МЭК 65-85) и ГОСТ В 20.39.308-76.

2.2.4 Необходимо убедиться в отсутствии механических повреждений накопителя.

## 2.3 Установка программного обеспечения УХИ «Меркурий»

### 2.3.1 Подготовка к процессу установки

2.3.1.1 Процесс установки программного обеспечения представляет собой последовательность действий, осуществляемую пользователем для приведения программной части УХИ «Меркурий» на ПЭВМ в работоспособное состояние.

2.3.1.2 Перед тем, как проводить установку, необходимо тщательно ознакомиться с настоящим документом для получения полного представления о требованиях, предъявляемых к рабочему месту и непосредственно к процессу установки.

2.3.1.3 Необходимо удостовериться, что ПЭВМ удовлетворяет всем требованиям, указанным в 2.1.

2.3.1.4 Необходимо четко сформулировать и запомнить пароль доступа к шифруемой информации.

### 2.3.2 Процесс установки

2.3.2.1 После проведения подготовки, описанной в 2.3.1, можно приступить к установки программного обеспечения УХИ «Меркурий».

Установка драйвера устройства для **Windows 2000/XP/2003/Vista/7** выполняется автоматически после первого подключения накопителя к ПЭВМ, при условии наличия у пользователя полномочий администратора ПЭВМ. Если полномочий администратора пользователь не имеет, то перед началом работы с устройством на ПЭВМ должен быть установлен драйвер устройства. В процессе установки драйвера на экран будут выведены сообщения об этом, не требующие вмешательства оператора.

2.3.2.2 Для начала процесса установки программной части УХИ «Меркурий» необходимо включить питание ПЭВМ, загрузить

ОС и вставить накопитель в свободный разъем USB, после чего перейти в папку **Мой компьютер** и на диске **U3** запустить программу **DCMGR**. На экране монитора отобразится сообщение в соответствии с рисунком 2.

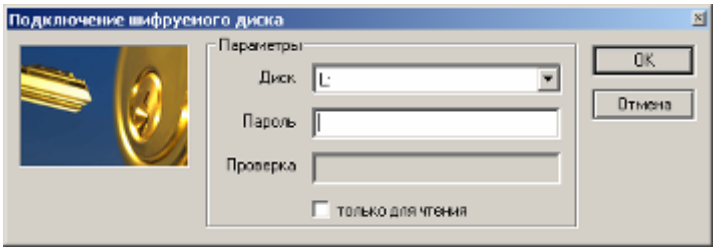


Рисунок 2

При этом на панели задач компьютера в правом нижнем углу экрана появится ярлык, выглядящий как показанный на рисунке 3. Он будет отображаться до того момента, пока накопитель не будет логически или физически отключен от ПЭВМ.

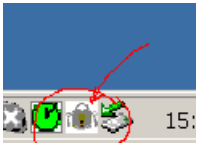

Рисунок 3

2.3.2.3 Для подтверждения выбора логического диска (рисунок 2) необходимо нажать кнопку ОК. Для отмены выбора нажать кнопку "Отмена", при этом окно, показанное на рисунке 2, будет закрыто.

2.3.2.4 Для возврата к состоянию, приведенному на рисунке 2, нужно мышкой выбрать накопитель U3 в окне "Мой компьютер" или, нажав правую кнопку мыши выбрать строку "Подключить диск".

2.3.2.5 С момента подсоединения накопителя к ПЭВМ в окне "Мой компьютер" появляются два новых накопителя: "U3" и "Съемный диск". Однако при попытке открыть съемный диск до

логического подключения в зависимости от ОС будет выдаваться сообщение, приведенное на рисунке 4 или 5, поскольку до логического подключения диска он зашифрован и рассматривается ОС как неформатированное пространство.

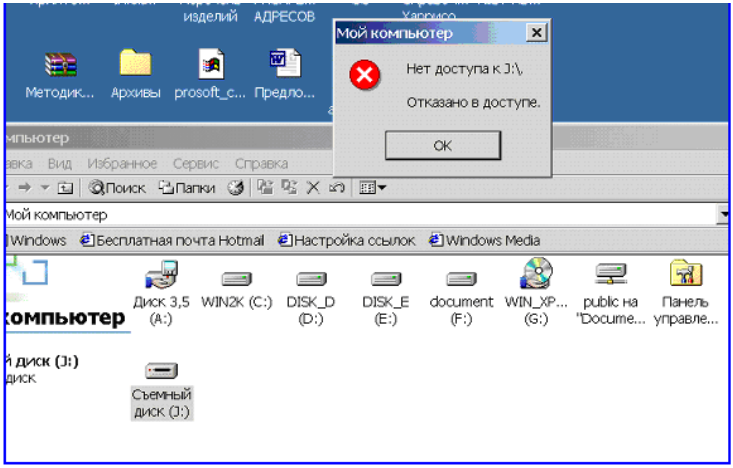


Рисунок 4

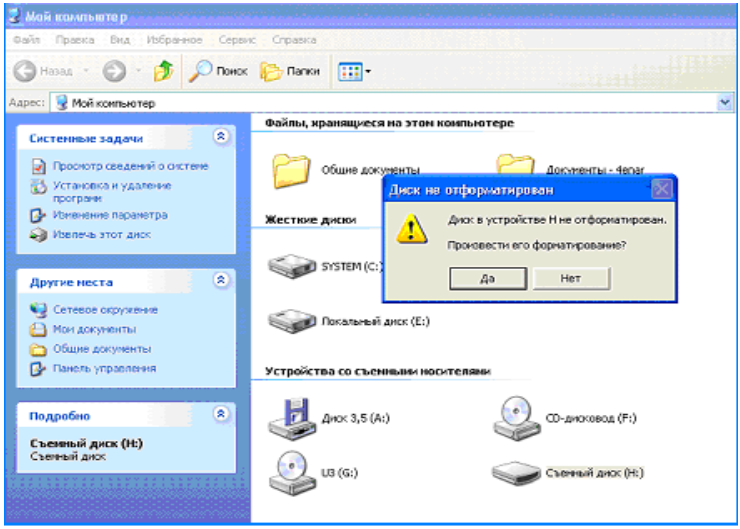


Рисунок 5

Для его закрытия необходимо нажать на клавиатуре клавишу "Ввод" или мышкой кнопку Нет.

2.3.2.6 Если доступ к диску выполняется в первый раз, то перед использованием накопителя следует произвести его инициализацию. Если инициализация выполняется не в первый раз, перед ее проведением следует сохранить данные, находящиеся на зашифрованном диске, а после завершения инициализации переписать их обратно. Для начала инициализации следует дважды нажать левую кнопку мыши, установив курсор на иконку, расположенную в правом нижнем углу (рисунок 3). На экране появится окно, приведенное на рисунке 6.

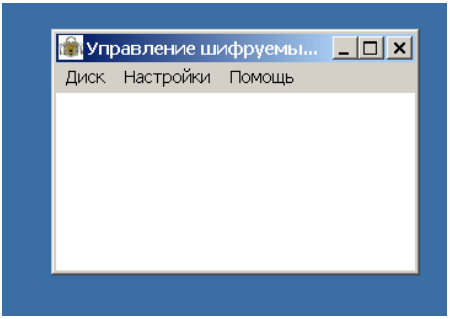


Рисунок 6

2.3.2.7 Затем, выбрать в меню позицию **Диск**, как показано на рисунке 7, и в открывшемся меню - **Инициализировать шифруемый диск,** после чего откроется окно, показанное на рисунке 8.

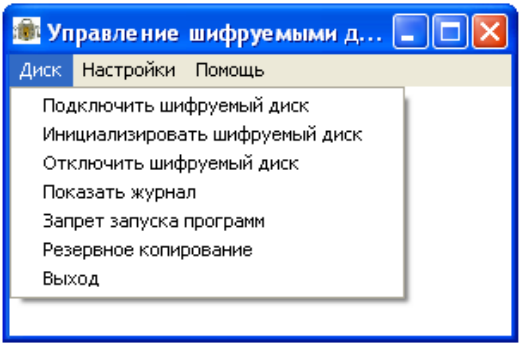

Рисунок 7

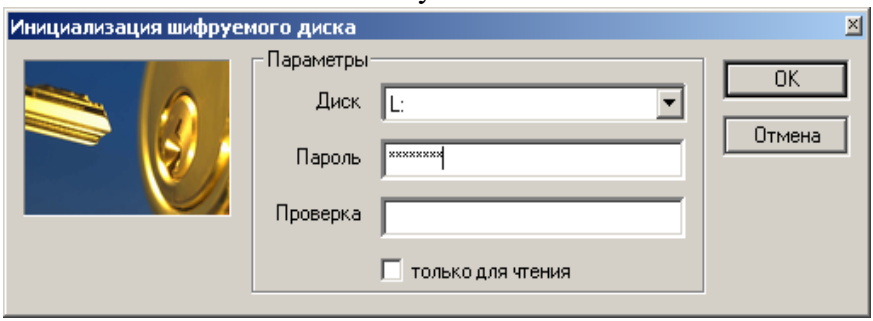


Рисунок 8

2.3.2.8 Далее следует ввести в поле **Пароль** - пароль, который будет использоваться для выработки ключа шифрования диска, а в поле **Проверка** повторить его. При вводе пароля вместо вводимых символов будут отображаться звездочки (*). Длина пароля должна быть не менее 8 символов, в пароле должны использоваться латинские и русские символы, а также цифры (см. Приложение А).

2.3.2.9 Если пароль в двух полях не совпадет, будет выдано сообщение, приведенное на рисунке 9.

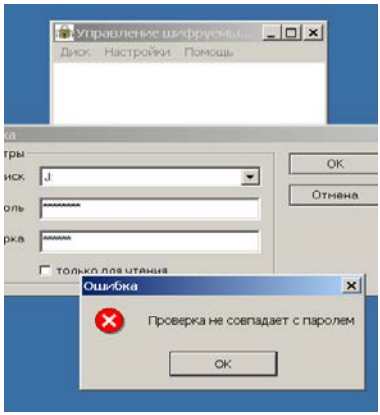


Рисунок 9

В ответ необходимо нажать кнопку ОК и повторить операцию, введя правильный пароль и его повторение, что приведет к

появлению на экране монитора окна, показанного на рисунке 10.

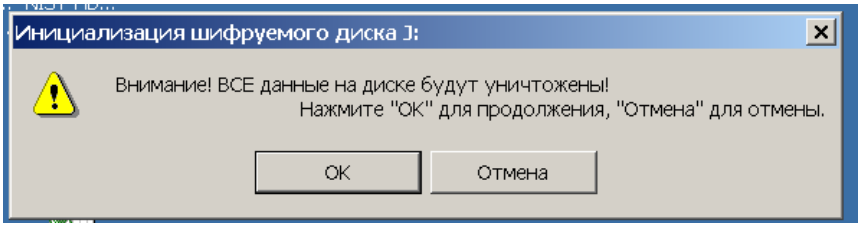


Рисунок 10

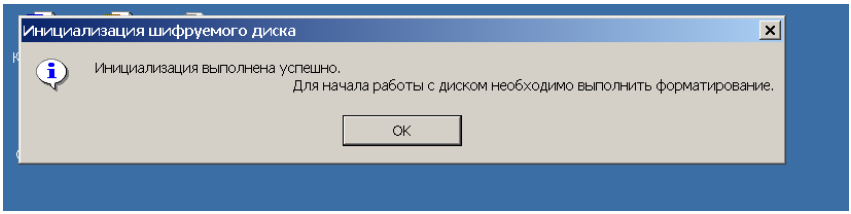


Рисунок 11

Поскольку, после выбора действия будет произведено форматирование накопителя, выберите необходимое продолжение. Если будет выбрано продолжение (ОК), то на экран будет выведено следующее сообщение (рисунок 11) и можно будет перейти к процессу форматирования, нажав кнопку ОК, что приведет к появлению на экране монитора стандартного окна форматирования накопителя, показанного на рисунке 12.

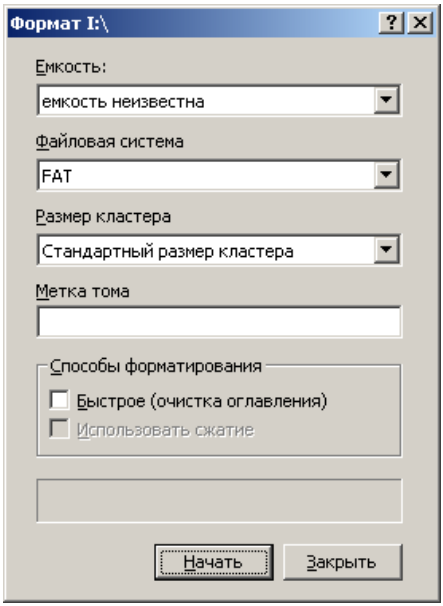


Рисунок 12

2.3.2.10 Процесс форматирования описан в документации на операционную систему. Для его выполнения следует ввести емкость форматируемого накопителя или его части, тип файловой системы, метку тома (может быть пустой) и выбрать способ форматирования – полное, при этом метка **Быстрое** не установлена и будет выполнено форматирование накопителя с проверкой всех кластеров, или быстрое - метка **Быстрое** установлена, - при этом будет выполнена только очитка оглавления накопителя без проверки кластеров.

После завершения форматирования будет выдано соответствующее сообщение (рисунок 13) и откроется экран с пустым отформатированным диском.

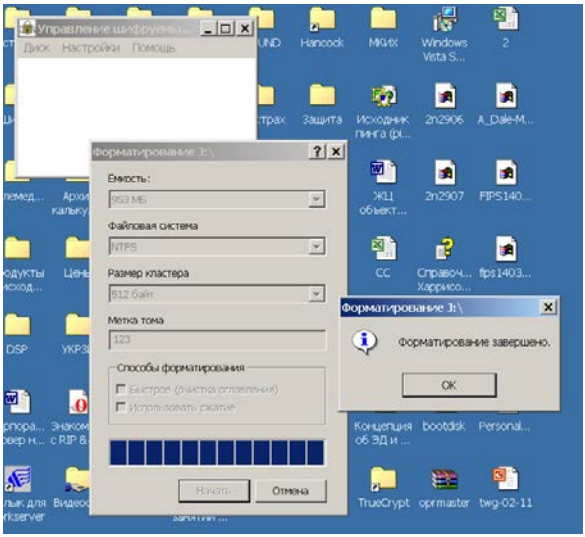


Рисунок 13

Процедура инициализации накопителя может быть выполнена в любое время. При этом следует помнить, что ее выполнение приведет к полному уничтожению хранимой на накопителе информации – она будет удалена, а диск накопителя перешифрован, и **восстановление уничтоженной информации будет невозможно**. Поэтому для обеспечения сохранности информации **перед инициализацией накопителя ее следует скопировать на другой носитель, а после инициализации записать обратно**.

2.3.2.11 При использовании устройства в режиме, исключающем несанкционированный перенос незашифрованной информации на USB-накопителе за пределы ПЭВМ, работающей в локальной сети, необходимо установить дополнительное программное обеспечение, поставляемое по специальному заказу и включающее:

- серверную часть, работающую на сервере, хранящем зашифрованный материал ключа пользователей;
- серверную часть, работающую на каждой из машин, где будут использоваться устройства;

– программу инициализации устройств на машине администратора безопасности

Данное программное обеспечение необходимо настроить в соответствии с приложением Г.

Инициализация устройств в этом случае производится только администратором с помощью специального программного обеспечения с сохранением данных материала ключа в локальном файле, имеющем расширение .ini. Данные из этого файла должны быть перенесены администратором в файл secrets.ini на сервере и удалены из локального файла.

**Внимание! Если Вы не удалили записи из локального файла, они будут записаны на сервер при очередном переносе и приведут к задваиванию записей, т.е. к нарушению работы рабочих мест пользователей.**

## 2.4 Использование УХИ «Меркурий»

### 2.4.1 Подключение инициализированного накопителя

2.4.1.1 Подключение накопителя, не содержащего в своем составе операционной системы, проводится в два этапа. Первый – физическое подключение к разъему порта USB, после чего на экране монитора должно появиться окно, приведенное на рисунке 2 (буква наименования диска может быть иной). При этом информация на диске остается недоступной пользователю. Второй – логическое подключение, в процессе которого производится ввод пароля, выработка из него ключа шифрования, активизация программы, производящей чтение зашифрованных кластеров с накопителя, их расшифрование в ОЗУ ПЭВМ с использованием ключа, полученного из пароля, передача расшифрованных кластеров программам обработки и отображения.

**Замечание**

1. Поскольку при использовании пароля в качестве источника для выработки ключа возникает угроза подбора пароля, при

применении УХИ «Меркурий» для обработки и хранения информации высокой конфиденциальности, в том числе секретной, должны использоваться дополнительные носители для хранения ключевой информации, которая совместно с информацией, полученной из пароля, составит ключ необходимой стойкости.

2. При обработке секретной информации накопитель УХИ «Меркурий» должен содержать операционную систему и программы обработки данных так, чтобы исключить применение других устройств хранения и связи, и, в связи с этим, возможности утечки информации.

3. Для пользователей, которые предполагают использовать одно приложение для работы с УХИ «Меркурий», возможна предустановка его в УХИ «Меркурий» и настройка файла автозагрузки так, что пользователю после завершения процедуры аутентификации будет открыто это приложение в состоянии, готовом к применению. Для этого используется файл DCMGR.ini, в который записывается запускаемая программа в соответствии с правилами оформления **.bat** или **.cmd** файлов.

4. После аутентификации пользователя все сетевые подключения блокируются и восстанавливаются после отключения накопителя, либо извлечения устройства из разъема, либо после отключения этой возможности (п. 2.4.6).

5. Для работы с устройством пользователя с правами, отличными от прав Администратора, необходимо убедиться, что для него установлено право форматировать и извлекать съемные носители. Для установки этих прав в Windows XP необходимо выполнить следующие действия:

– выбрать Пуск / Панель управления / Администрирование / Локальная политика безопасности / Параметры безопасности / Устройства: Разрешено форматировать и извлекать съемные носители – установить в состояние «Администраторам и интерактивным пользователям»;

– перезагрузить ПЭВМ.

2.4.1.2 При вводе пароля количество попыток ограничено. При исчерпании попыток работа УХИ «Меркурий» блокируется.

2.4.1.3 В случае правильного логического подключения зашифрованная информация, хранящаяся на накопителе, становится доступной пользователю ПЭВМ. При этом на накопителе она всегда находится в зашифрованном состоянии.

2.4.1.4 Следует помнить, что, поскольку часть информации в процессе работы хранится в ОЗУ ПЭВМ, выключение питания или физическое отключение накопителя без выполнения процедуры логического отключения может привести к утере информации.

2.4.1.5 При использовании накопителя в режиме, исключающем возможность несанкционированного переноса на накопителе обрабатываемой информации за пределы рабочего места, следует установить и настроить дополнительное программное обеспечение (см. Приложение Г).

### 2.4.2 Отключение инициализированного накопителя

2.4.2.1 Отключение устройства должно производиться в следующем порядке – логическое отключение, затем физическое – отключение от разъема или выключение питания.

2.4.2.2 Логическое отключение необходимо производить в следующем порядке:

- закрыть выполняющиеся прикладные программы;

**Внимание!** Если до физического отключения прикладные программы не будут завершены, доступ к защищаемой области сохранится. При попытке извлечь накопитель до завершения прикладной программы Вы можете уничтожить обрабатываемую прикладной программой информацию;

- вызвать окно, приведенное на рисунке 7;
- выбрать позицию меню Отключить шифруемый диск;
- если подключено несколько накопителей, получить сообщение, приведенное на рисунке 14;

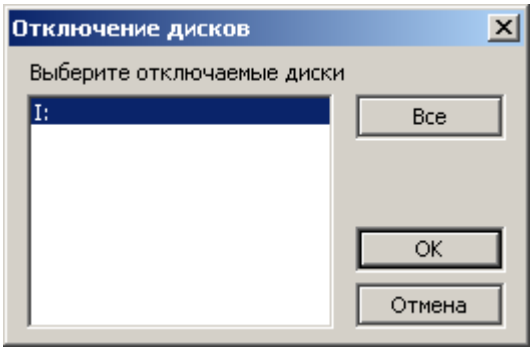


Рисунок 14

- выбрать отключаемый диск;
- появление сообщения приведенного на рисунке 15 говорит о завершении логического отключения накопителя, и его можно извлечь из разъема.

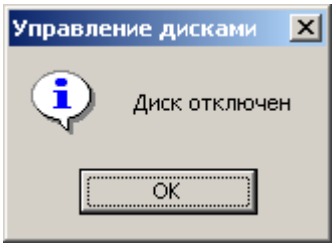


Рисунок 15

2.4.2.3 Если по какой-либо причине понадобится вновь логически подключить диск, то это можно сделать, вызвав окно, приведенное на рисунке 7, и выбрав в меню строку **Подключение шифруемого диска,** перейти к окну, приведенному на рисунке 2, и ввести пароль, что позволит начать работу с защищенными данными.

2.4.2.4 Подключение УХИ «Меркурий» с установленной на нем операционной системой отличается тем, что оно может быть использовано без загрузки установленной ОС, и тогда его использование производится в соответствии с 2.4.1 и 2.4.2, либо с загрузкой установленной на нем ОС.

2.4.2.5 Для загрузки установленной на накопитель ОС необходимо в программе SETUP BIOS ПЭВМ, на которой будет происходить загрузка, установить в разделе Advanced Setup опцию 1st Boot Device USB или 1st Boot Device USB FDD.

2.4.2.6 В этом случае после включения питания, нажатия кнопки **Сброс** или **Ctrl-Alt-Del** начнется начальная загрузка ОС с накопителя устройства.

### 2.4.3 Работа с подключенным накопителем

2.4.3.1 Работа с подключенным накопителем с точки зрения пользователя ничем не отличается от работы с обыкновенным флеш-диском.

### 2.4.4 Формирование ключей, их хранение и смена

2.4.4.1 Генерация ключей из пароля и их передача программе обработки производится каждый раз при логическом подключении диска. Его уничтожение в памяти ПЭВМ происходит при логическом отключении диска.

**Замечание**

В случае физического отключения диска без логического отключения ключ шифрования остается в памяти и может оказаться доступным злоумышленнику. Поэтому нарушение порядка отключения **строжайше запрещено**. Если отключение питания произошло не по Вашей вине, необходимо выключить и вновь включить питание ПЭВМ, загрузить ОС.

### 2.4.5 Работа с журналом устройства

При работе устройства ведется защищенный журнал работы. Для его просмотра следует в окне, приведенном на рисунке 7, выбрать закладку **Просмотр журнала.** При этом следует учитывать, что данная операция доступна пользователю только в том случае, если он идентифицирован с правами **Администратора.** При выборе закладки **Просмотр журнала** отобразится окно, как показано на рисунке 16. Следует помнить, что журнал становится доступным

только после аутентификации пользователя.

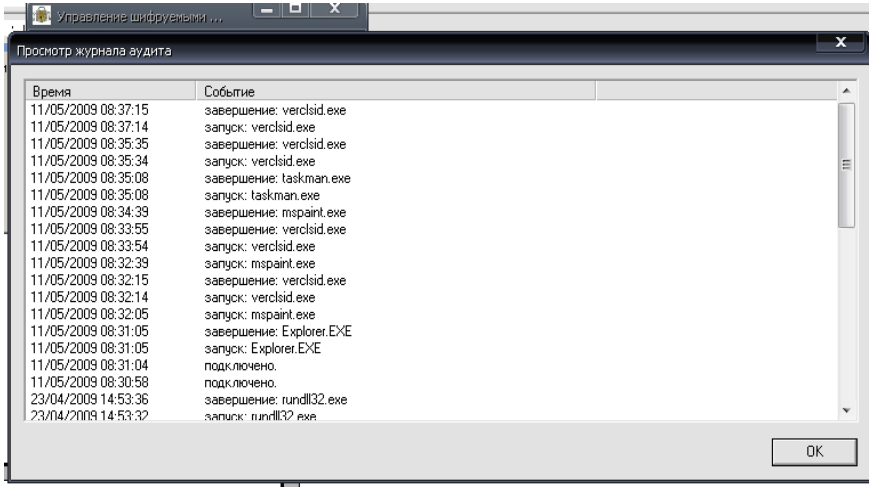


Рисунок 16

В журнале приводится информация о дате, времени и характере действия, произведенного пользователем (запуск/завершение), а также наименование приложения. При использовании возможности п.1.1.1. перечисление к), журнал ведется средствами ОС.

### 2.4.6 Установка разрешения на работу приложений

2.4.6.1 При использовании устройства может быть введено ограничение на работу приложений при подключенном накопителе устройства. Для этого пользователю, идентифицированному с правами **Администратора,** необходимо вызвать окно, приведенное на рисунке 7, и выбрать **Диск/Запрет запуска программ.** После этого откроется окно, приведенное на рисунке 17.

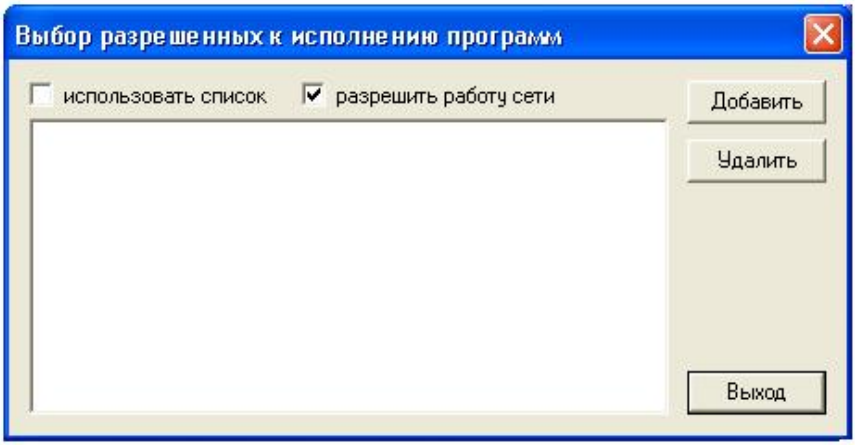


Рисунок 17

2.4.6.2 С помощью кнопок «Добавить» и «Удалить» в список добавляются и из списка исключаются программы, разрешенные к исполнению.

**Внимание!** Помните, что **все программы, не включенные в список,** не будут загружаться для исполнения.

2.4.6.3 Программы, включенные в список, начинают контролироваться только после того, как установлен признак **«использовать список».**

2.4.6.4 Работа УХИ «Меркурий» в сети возможна только после того, как установлен признак **«разрешить работу сети».**

### 2.4.7 Резервное копирование

2.4.7.1 Для реализации возможности копирования информации аутентифицированному пользователю необходимо вызвать окно, приведенное на рисунке 7, и выбрать **Диск/Резервное копирование.** После этого откроется окно, приведенное на рисунке 18, в котором можно выбрать папку для копирования и создать требуемую копию.

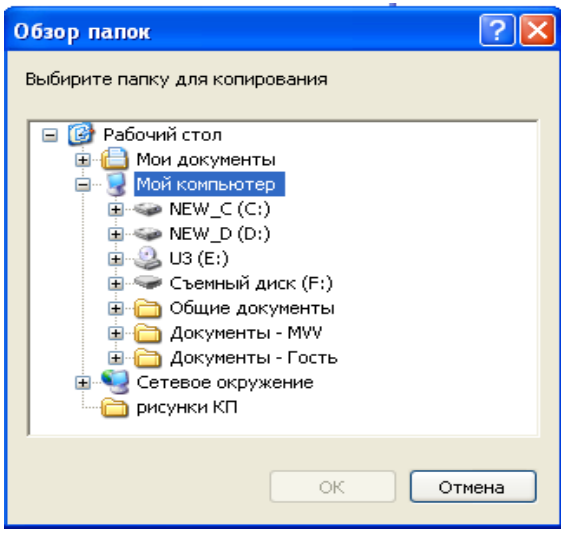


Рисунок 18

### 2.4.8 Завершение работы с УХИ «Меркурий»

2.4.8.1 Для завершения работы с УХИ «Меркурий» необходимо вызвать окно, приведенное на рисунке 7, и выбрать **Диск/Выход.** После этого откроется окно, приведенное на рисунке 19, в котором можно, нажав кнопку «ОК», завершить работу. Извлечение УХИ «Меркурий» из ПЭВМ аналогично извлечению обычного флеш-накопителя.

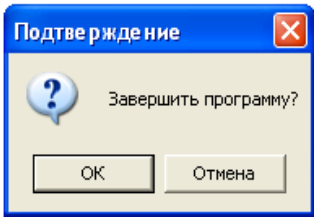


Рисунок 19

2.4.8.2 Также для завершения работы можно выполнить пункт 2.4.2.

### 2.5 Действия в экстремальных ситуациях

2.5.1 На случай стихийного бедствия (пожар, затопление помещения и т.п.) должны быть разработаны и утверждены руководством предприятия специальные инструкции, в которых предусматривается порядок вызова администрации, должностных лиц, очередность и порядок спасения имущества.

2.5.2 В случае возгорания ПЭВМ следует немедленно обесточить цепи питания и принять меры по ликвидации очага возгорания имеющимися средствами пожаротушения.

2.5.3 При необходимости экстренного уничтожения информации, хранящейся на накопителе, необходимо одновременно нажать клавиши **Ctrl+Alt+Del+PgDn.**

**Внимание!** При уничтожении информации с использованием **Ctrl+Alt+Del+PgDown** уничтожается 32-байтовое число, участвующее в формировании ключа, а также логическая структура накопителя. Для восстановления работоспособности устройства следует обратиться к поставщику изделия. При этом может быть восстановлена работоспособность устройства, но уничтоженная информация будет утеряна навсегда.

## 3 Техническое обслуживание

3.1 УХИ «Меркурий» в процессе эксплуатации является необслуживаемым изделием.

## 4 Текущий ремонт

4.1 УХИ «Меркурий» не требует текущих ремонтов. В случае нарушения работоспособности необходимо обратиться к разработчику УХИ «Меркурий».

## 5 Хранение

5.1 УХИ «Меркурий» не содержит в своем составе веществ и материалов, опасных для жизни и здоровья человека и окружающей среды, и не требует принятия специальных мер предосторожности

при хранении.

5.2 УХИ «Меркурий» хранят в упаковке изготовителя в складских помещениях.

5.3 Не допускается хранение УХИ «Меркурий» совместно с испаряющимися жидкостями, кислотами и другими веществами, которые могут вызвать коррозию.

5.4 Условия хранения УХИ «Меркурий» – 1 (Л) по ГОСТ 15150-69:

- температура окружающего воздуха в помещении хранения от плюс 5 до плюс 40 °С;
- относительная влажность окружающего воздуха – не более 80 % при температуре окружающего воздуха плюс 25 °С.

Гарантийный срок хранения УХИ «Меркурий» – не более 24 мес.

## 6 Транспортирование

6.1 УХИ «Меркурий» не содержит в своем составе веществ и материалов, опасных для жизни и здоровья человека и окружающей среды, и не требует принятия специальных мер предосторожности при транспортировании. Транспортирование УХИ «Меркурий» производится в подборной таре любым видом транспорта на любое расстояние в соответствии с правилами перевозок, действующими на каждом виде транспорта.

6.2 Способ крепления упакованных УХИ «Меркурий» при транспортировании должен предотвращать их перемещение.

6.3 Условия транспортирования УХИ «Меркурий» по ГОСТ 21552-84 Е:

- температура окружающего воздуха от минус 50 до плюс 50 °С;
- относительная влажность окружающего воздуха – не более 98 % при температуре окружающего воздуха плюс 25 °С;
- атмосферное давление от 84 до 107 кПа.

6.4 В транспортных средствах, где перевозится УХИ «Меркурий», не должно быть паров кислот, щелочей и других химически активных веществ, пары или газы которых могут вызвать коррозию.

## 7 Утилизация

7.1 УХИ «Меркурий» не содержит в своем составе ядовитых и вредных веществ и материалов, опасных для жизни и здоровья человека, а также представляющих опасность для окружающей среды, и не требует специальных мер предосторожности при утилизации.

7.2 Утилизацию УХИ «Меркурий» проводят после окончания срока службы и заключения комиссии о нецелесообразности дальнейшей эксплуатации УХИ «Меркурий».

7.3 Мероприятия по подготовке и отправке на утилизацию разрабатываются согласно распоряжению руководителя предприятия в соответствии с порядком утилизации, установленным на предприятии.

## 8 Ресурсы, сроки службы и хранения, гарантии изготовителя (поставщика)

### 8.1 Ресурсы, сроки службы и хранения

Ресурсные показатели долговечности для УХИ «Меркурий» не устанавливаются.

Средний срок службы до списания (полный) – не менее 10 лет.

Ресурс изделия до первого ремонта – наработка на отказ не менее 1000000 операций записи, или 6000 ч в течение срока службы 10 лет, в том числе срок хранения – 2 года в отапливаемых и вентилируемых складах, хранилищах с кондиционированием воздуха в упаковке изготовителя.

Указанные ресурсы, сроки службы и хранения действительны при соблюдении потребителем требований настоящего РЭ.

### 8.2 Гарантии изготовителя

Предприятие-изготовитель (поставщик) гарантирует соответствие УХИ «Меркурий» требованиям технической документации при соблюдении пользователем правил и условий эксплуатации, хранения, транспортирования и монтажа, установленной документацией на УХИ «Меркурий».

Гарантийный срок службы изделия – **12 мес.** со дня реализации предприятием-изготовителем.

Гарантийный срок хранения изделия – **12 мес.** с момента приемки на предприятии-изготовителе.

Гарантийное обслуживание УХИ «Меркурий» осуществляется за счет предприятия-изготовителя по договору между изготовителем или другой организацией, имеющей с предприятием-изготовителем соответствующее соглашение, и потребителем.

Потребитель лишается права на гарантийное обслуживание при нарушении условий эксплуатации УХИ «Меркурий».

## 9 Свидетельство об упаковывании

Устройство хранения информации защищенное мобильное «Меркурий»

**СЮИК.466216.001 №** _____
заводской номер

Упакован(а)_____ЗАО "НТЦ КОНТАКТ"_____
наименование или код изготовителя

согласно требованиям, предусмотренным в действующей технической документации.

_____ _____ _____
должность личная подпись расшифровка подписи

_____
год, месяц, число

## 10 Свидетельство о приемке

Устройство хранения информации защищенное мобильное «Меркурий»

**СЮИК.466216.001 №** _____
заводской номер

изготовлен(а) и принят(а) в соответствии с обязательными требованиями государственных стандартов, действующей технической документации и признан (а) годным(ой) для эксплуатации.

Начальник ОТК

МП _____ _____ _____
личная подпись расшифровка подписи год, месяц, число

## 11 Движение изделия при эксплуатации

Сведения о движении УХИ «Меркурий» должны заноситься в таблицу 3.

Таблица 3

| Дата установки | Где установлено | Дата снятия | Наработка | | Причина снятия | Подпись лица, проводившего установку |
|---|---|---|---|---|---|---|
| | | | с начала эксплуатации | после последнего ремонта | | |
| | | | | | | |

## 12 Аварийные ситуации

12.1 При работе УХИ «Меркурий» возможна выдача на экран монитора соответствующих сообщений, приведенных в таблице 4.

Таблица 4 – Перечень сообщений

| Текст сообщения | Описание события | Порядок действия |
|---|---|---|
| Неверный пароль | Попытка входа в систему с неверным паролем | Ввести верный пароль и повторить вход |
| Подтверждение не совпадает с паролем | Пароль в поле "Подтверждение" не совпадает с паролем в поле "Пароль" | Ввести правильный пароль |

## Приложение А
(справочное)
## Перечень принятых сокращений

В настоящем руководстве по эксплуатации приняты следующие сокращения:

НСД – несанкционированный доступ
ОЗУ – оперативное запоминающее устройство
ОС – операционная система
ПЭВМ – персональная электронно-вычислительная машина
РЭ – руководство по эксплуатации

## Приложение Б
(справочное)
## Требования к паролям

Порядок работы (генерации, ввода, изменения, удаления) с паролями должен быть изложен в соответствующих инструкциях по формированию и ведению паролей.

**Общие требования к паролям пользователей**

Общие требования к паролям пользователей следующие:

- идентификатор (имя) и пароль должны выдаваться каждому пользователю под роспись в «карточке учета паролей»;
- при входе в систему идентификатор и пароль вводятся самим пользователем;
- пароли пользователей должны периодически меняться в сроки, предусмотренные регламентом;
- пароль должен иметь длину не менее восьми символов, в состав которых должны входить буквы латинского алфавита, цифры и специальные знаки (подчеркивание, тильда и др.); ввод паролей, не отвечающих этим требованиям, блокируется системой;
- пароли должны отличаться друг от друга не менее чем тремя символами и не должны иметь более двух повторяющихся символов;
- пользователям запрещается передавать свои пароли друг другу и записывать пароль на чем-либо.

**Требования к системе ведения паролей**

Процедура системы ведения паролей должна быть тщательно отработана пользователями:

- пароль должен вводиться согласно требованиям инструкций по формированию и ведению паролей;
- запрещается осуществлять ввод пароля в присутствии посторонних лиц;
- должна быть предусмотрена процедура смены паролей в случае несанкционированного доступа к информации и в других нештатных ситуациях;
- при компрометации пароля необходимо срочно принять меры по смене пароля;

**Требования к пользователю при работе с паролями**

Пользователь обязан:

- выполнять требования эксплуатационной документации на встроенные средства защиты информации при работе со своим паролем;
- сохранять пароль в тайне и следить за конфиденциальностью ввода пароля с клавиатуры;
- в неясных или нештатных случаях обращаться за помощью к администратору безопасности,

**Прочие требования по организации ведения паролей**

- пользователь должен быть ознакомлен с перечисленными выше требованиями и предупрежден об ответственности за невыполнение своих обязанностей, а также за разглашение паролей;
- ответственность за своевременное формирование и распределение (выдачу) паролей пользователям возлагается на администратора безопасности;
- конверты с паролями должны быть опечатаны, при необходимости может быть заведена резервная копия «карточки учета паролей» каждого пользователей (на случай утраты основной);

- внеплановая смена (блокирование) личного пароля любого пользователя в случае прекращения его полномочии (увольнение, переход на другую работу и т.п.), либо компрометирующих действий должна производиться немедленно после окончания последнего санкционированного сеанса работы данного пользователя. Необходимо производить внеплановую смену паролей всех пользователей при выявлении несанкционированного доступа;
- в случае компрометации (разглашения) пароля пользователя должно проводиться служебное расследование.

**Методика определения необходимой длины пароля**

Оценка необходимой длины пароля требуется для того, чтобы правильно выбрать период действия (смены) паролей. Данный период действия паролей определяется вероятностью подбора пароля, при этом предполагается, что подбор пароля осуществляется непрерывным тестированием ПЭВМ в течение определенного периода времени.

Взаимосвязь между длиной пароля и периодом времени для его подбора в результате непрерывного тестирования ПЭВМ определяется формулой:

$$4{,}32 \times 10^4 \times \mathrm{K} \times \left( \frac{\mathrm{M}}{\mathrm{P}} \right) \leq \mathrm{A}^{\mathrm{Z}} \qquad (1),$$

где К – количество попыток подбора пароля в минуту (мин-1);

М – период времени непрерывного тестирования ПЭВМ для подбора пароля в месяцах (месяц);

Р – заданная вероятность подбора пароля;

А – количество символов, из которых составляется пароль (базовая длина алфавита);

z – длина пароля.

Формула (1) позволяет определить необходимую длину пароля, если задана вероятность подбора пароля при непрерывном

тестировании ПЭВМ в течение какого-либо определенного промежутка времени.

Например, пусть заданная вероятность подбора пароля в результате месячного непрерывного тестирования ПЭВМ не должна превышать 0,0001 ($P \le 0{,}0001$).

Для составления пароля используется английский алфавит ($A = 26$).

Длина пароля ($z = 8$).

Выясним соответствие длины пароля и заданных условий по его подбору, при этом будем полагать, что время на одну попытку подбора пароля составляет 5 секунд (то есть, что $K = 60/5 = 12$).

Имеем:

$$4{,}32 \times 10^4 \times 12 \times \left( \frac{1}{0{,}0001} \right) \le 26^8$$

или

$$5{,}2 \times 109 \le 208{,}8 \times 109$$

То есть, длина пароля с 8 символов достаточна для выполнения заданных условий, а именно – если будет выбран пароль длиной в 8 символов, то в течение месяца при осуществлении непрерывных попыток его подбора вероятность подбора будет не выше 0,0001.

Если требуется вычислить вероятность подбора пароля при осуществлении непрерывных попыток его подбора в течение месяца при следующих условиях, то:

$K = 12$ (мин-1);

$M = 1$ (мес.);

$A = 26$ (символов);

$z = 8$ (символов).

Подставив данные значения в формулу (1), получим:

$$4,\ 104 \times 12 \times \left( \frac{1}{P} \right) \le 208{,}8 \times 109$$

или

$$0{,}00052 \times 109 \times \left(\frac{1}{P}\right) \leq 208{,}8 \times 109$$

то есть, вероятность подбора пароля не превысит 2,5 × 10-6.

Пароль, в котором используется хотя бы одна цифра, спецсимвол, а также буквы различных алфавитов или регистров, называется сложным. Если при составлении пароля использовать буквы русского алфавита (прописные и строчные), буквы латинского алфавита (прописные и строчные), цифры и спецсимволы, то базовая длина алфавита составит A = 161 символ.

В этом случае вероятность подбора пароля при осуществлении непрерывных попыток его подбора в течение месяца не превысит 2,5 × 10-14.

Таким образом, при использовании сложного пароля вероятность его подбора крайне низка и, кроме того, исключается возможность его подбора методом "словаря".

Следовательно, для обеспечения надежной защиты информации, хранящейся на носителе, рекомендуется менять пароль не реже одного раза в месяц.

## Приложение В
(справочное)
## Организационные мероприятия по обеспечению безопасности при работе с УХИ «Меркурий»

Для хранения НКИ в помещениях должны устанавливаться надежные металлические хранилища, оборудованные внутренними замками. Использовать НКИ необходимо только по назначению, совместно с программными компонентами ПС КЗИ и ЭЦП. В случае утери НКИ или подозрении на компрометацию криптографических ключей необходимо немедленно сообщить об этом Администратору безопасности ИИС ЭОТ и исключить дальнейшее использование данных криптографических ключей.

Узлы и блоки оборудования средств вычислительной техники (СВТ), к которым в процессе эксплуатации программных компонент ПС КЗИ и ЭЦП доступ не требуется, должны быть закрыты и опечатаны. Опечатывание производится в соответствии с конструктивными особенностями данных СВТ и должно исключать возможность несанкционированного вскрытия оборудования.

Для обеспечения защиты от несанкционированного доступа и разграничение доступа к ресурсам СВТ, защиты от несанкционированных модификаций и контроля целостности программ и данных на которых обрабатывается информация хранящаяся на УХИ «Меркурий» рекомендуется использовать программно-аппаратные комплексы защиты информации от НСД.

Для исключения возможности внедрения «закладок», «компьютерных вирусов», несанкционированного изменения действующего программного обеспечения (ПО) рекомендуется использовать только лицензионное системное и прикладное ПО и только необходимое по технологии работы. Любое изменение (реконфигурирование, дополнение и т.д.) ПО должно быть согласовано с Администратором безопасности соответствующего уровня или специально выделенным ответственным лицом.

При проведении ремонтных и профилактических работ УХИ «Меркурий», должны приниматься организационные меры и использоваться технические средства для исключения утечки защищаемой информации;

Осмотр и ремонт СВТ представителями сторонних организаций должен проводиться только под наблюдением специально выделенного ответственного лица.

Передача СВТ для ремонта в сторонние организации производится только после демонтажа накопителя на жестком магнитном диске (НЖМД) и адаптера НКИ (платы защиты от НСД, при ее наличии) с обязательном отражением в учете.

Защита информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок, акустических и виброакустических каналов, несанкционированного доступа за счет скрытно установленных устройств съема информации, а также защита от «компьютерных вирусов» должна осуществляться на основании руководящих документов, действующих в Республике Беларусь, а также рекомендаций ОАЦ.

**Приложение Г**
(справочное)
**Порядок установки и настройки программного обеспечения при работе с УХИ «Меркурий» в режиме, исключающем возможность несанкционированного переноса на накопителе обрабатываемой информации за пределы рабочего места**

**Состав и назначение программного обеспечения**

1. Папка Admin not use secret содержит программу для инициализации чистых, непроинициализированных U3 флеш-дисков. Перед инициализацией администратор запускает программу DCMGR.exe и вводит стандартный транспортный пароль для доступа к флеш-диску (12345678) как показано на рисунке Г1.

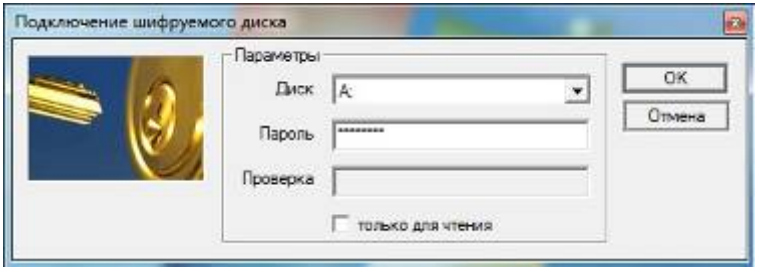


Рисунок Г1

Для инициализации диска следует выбрать пункт меню «Диск -> Инициализация шифруемого диска», как показано на рисунке Г2. При инициализации администратор вводит новый пароль к флеш-диску (рисунок Г3) и проверку, после нажатия кнопки «Ok» запускается процесс инициализации (рисунок Г4). На выполнение процесса инициализации может потребоваться значительное количество времени, в течение которого извлекать накопитель категорически запрещается.

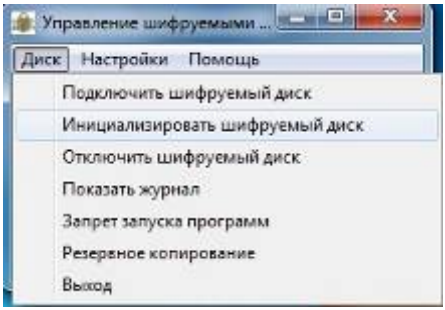


Рисунок Г2

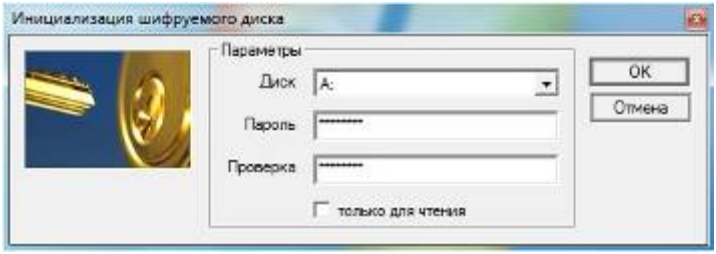


Рисунок Г3

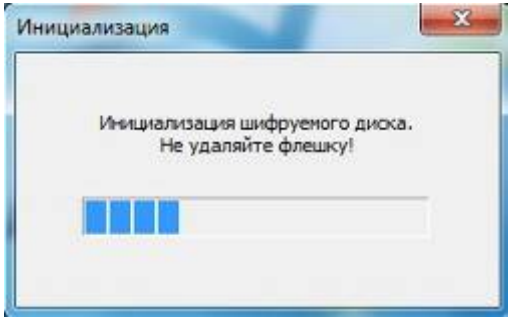


Рисунок Г4

Если процесс инициализации прошёл успешно, программа выдаст сообщение, показанное на рисунке Г5.

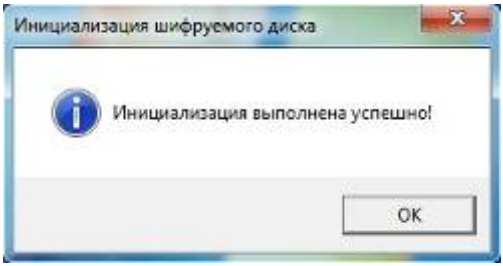


Рисунок Г5

В процессе инициализации вырабатывается секрет, а также ключ на основе пароля и секрета. Секрет, зашифрованный на хеше от пароля, сохраняется в папке с программой в файле secrets.ini (рисунок Г6).

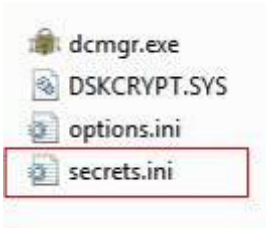


Рисунок Г6

Данный файл необходимо будет перенести на сервер в папку с программой Remote Server и удалить эту информацию из локального файла.

2. Папка Admin use secret содержит программу для инициализации проинициализированных ранее U3 флеш-дисков. Последовательность действий, необходимых для инициализации накопителя, а также внешний вид окон программы идентичны рассмотренным в предыдущем пункте. Перед инициализацией администратор вводит пароль для доступа к флеш-диску, после чего происходит запрос секрета от удаленного сервера и получение доступа к устройству. Для инициализации диска следует выбрать пункт меню «Диск -> Инициализация шифруемого диска». При

инициализации администратор вводит новый пароль к флеш-диску, после чего вырабатывается секрет и вырабатывается ключ на основе пароля и секрета. Секрет, зашифрованный на хеше от пароля, сохраняется в файле secrets.ini. Данный файл необходимо будет перенести на сервер в папку с программой Remote Server.

3. Папка Local server содержит программу-посредника. Данная программа служит для взаимодействия между пользователем/администратором и удаленным сервером, на котором хранится список секретов для доступа к U3 флеш-дискам. Программа устанавливается на ПЭВМ пользователей/администраторов, она должна быть настроена и запущена перед началом работы с U3 флеш-диском. Иконка запущенной программы отображается в трее, как показано на рисунке Г7.

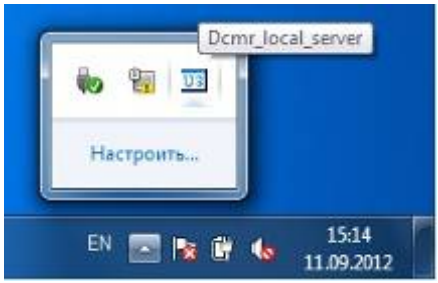


Рисунок Г7

4. Папка Remote Server содержит программу-сервер. Данная программа служит для приема клиентских запросов от Local server, поиска по списку секрета и возврата его клиентскому приложению. Список секретов загружается из файла secrets.ini. Файл формируется с помощью программ из папок «Admin not use secret» и «Admin use secret» во время инициализации U3 флеш-дисков. Иконка запущенной программы отображается в трее, как показано на рисунке Г8.

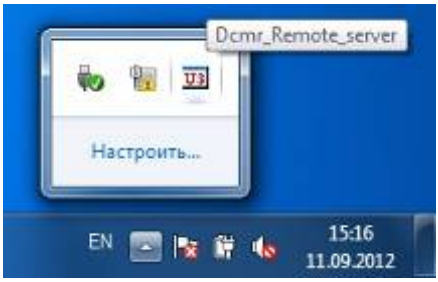


Рисунок Г8

5. Папка USB Client содержит программу и файл настроек, записываемые на U3 флеш-диск.

**Способ установки программного обеспечения**

Программное обеспечение устанавливается путем копирования папок с файлами в выбранное свободное место на жестком диске и выполнения процедуры настройки. Настройка осуществляется вводом или корректировкой записей в .ini файле.

**Настройки программного обеспечения**

Ниже приведены примеры настроек и их описания.

**Внимание! В настройках следует применять значения, определяемые в Вашей конкретной системе.**

Программы (1) и (2) ставятся на компьютере администратора. В папках с программами находится файл Options.ini. Данный файл содержит параметры, указанные в таблице 5:

Таблица 5 – Содержимое файла Options.ini программ (1) и (2)

| Параметр | Описание |
|---|---|
| UseInitMenu = 1 | Разрешить наличие пункта меню «Инициализировать шифруемый диск» в меню «Диск» программы dcmgr.exe (0 – убрать пункт меню, 1- оставить. По умолчанию = 1) |
| UseSecretForInitialize = 1 | Генерировать секрет при инициализации (1 – |

| | |
|---|---|
| | используя секрет и пароль, 0 - только на основе пароля) |
| UseSecret = 1 | Запрашивать секрет для получения доступа к флэш диску |
| Use_driver_opt = 1 | Использовать заданный путь для загрузки драйвера |
| Driver = | Путь к драйверу, например, "E: \dskcrypt\ dskcrypt.sys" |
| Use_CD_opt = 1 | Использовать заданную в настройках букву CD-Rom диска ( 0 – нет, 1 - использовать) |
| CD = | Буква CD-Rom диска, например, "H" |

Так как программы (1) и (2) запускаются с жесткого диска компьютера администратора, то необходимо в настройках указывать путь к файлу драйвера и букву диска, которую назначает операционная система для подключаемых U3 флеш-дисков.

Программа (3) устанавливается на ПЭВМ клиентов/администратора. В папке с программой находится файл Options.ini. Данный файл содержит параметры, указанные в таблице 6:

Таблица 6 – Содержимое файла Options.ini програмы (3)

| Параметр | Описание |
|---|---|
| remoteport = | Порт удалённого сервера для запроса секрета, например, 51010 |
| remotehost = | IP адрес удалённого сервера для запроса секрета, например, 127.0.0.1 |

Программа (4) устанавливается на сервере. В папке с

программой находится файл Options.ini. Данный файл содержит параметры, указанные в таблице 7:

Таблица 7 – Содержимое файла Options.ini програмы (4)

| Параметр | Описание |
|---|---|
| port = | Прослушиваемый порт, например, 51010 |

В папке с программой также должен находиться файл secrets.ini, генерируемый программами (1) и (2). Файл содержит список секретов и серийных номеров U3 флеш-дисков. Для того, чтобы новый файл секретов вступил в силу, следует перезапустить программу (4).

| Лист регистрации изменений | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Изм | Номера листов (страниц) | | | | Всего листов (страниц) в докум. | № докум. | Входящий № сопроводительного докум. и дата | Подп | Дата |
| | измененных | замененных | новых | аннулированных | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |