

CyberSafe® для Windows

Руководство пользователя



Содержание

Общая информация о программе CyberSafe	1
Что нового в CyberSafe версии 2.0	5
Условные обозначения, используемые в этом Руководстве	7
Для кого предназначен этот документ	8
Лицензионное соглашение на использование изделия	8
Термины и определения	8
Предмет соглашения	8
Авторские права	8
Условия использования	9
Срок действия соглашения	9
Ответственность	9
Гарантии изготовителя (поставщика)	9
Лицензионные положения и условия, замечания и информация третьих сторон	10
Помощь по работе с программой	12
Дополнительная информация о продукте	13
Контактная информация	13
CyberSafe. Основы	2
Терминология и основные функции CyberSafe	14
Терминология CyberSafe	14
Основные функции программы	15
Симметричная и асимметричная криптография	16
Подробнее о криптографии	16
Первое использование CyberSafe	16
Установка CyberSafe	3
Перед установкой	18
Системные требования	18
Установка и настройка CyberSafe	18
Установка программы	19
Создание сертификата и настройка программы	20
Деинсталляция CyberSafe	21
Перемещение CyberSafe с одного компьютера на другой	22
Пользовательский интерфейс CyberSafe	4
Доступ к основным функциям CyberSafe	24
Главное окно программы	24
Работа с ключами CyberSafe	5
Просмотр ключей	26
Создание ключевой пары	26
Использование паролей	27
Защита закрытого ключа	27
Меры, предпринимаемые для защиты ключей	28
Создание резервной копии ключей	28
Что, если закрытый ключ утерян?	29
Распространение открытого ключа	29
Публикация на сервере	30
Добавление открытого ключа в e-mail сообщение	31
Экспорт открытого ключа в файл	31
Получение открытого ключа от других пользователей	31
Скачивание открытого ключа с сервера ключей	31
Импорт ключей и сертификатов	32
Работа с серверами ключей	32

Хранение ключей CyberSafe на токенах	6
О токенах	34
Использование флеш-накопителя в качестве токена	35
Защита E-mail сообщений	7
Шифрование почты при помощи CyberSafe	38
Экспорт сертификата в формате PFX	38
Работа с Microsoft Outlook	39
Работа с Mozilla Thunderbird	45
Работа с The Bat!	48
Шифрование файлов при помощи CyberSafe	8
О шифровании файлов программой CyberSafe	52
Шифрование файлов и папок	52
Шифрование на основе сертификатов (ключей)	52
Шифрование паролем	55
Создание зашифрованных zip-архивов	56
Дополнительные настройки шифрования	58
Прозрачное шифрование помощи CyberSafe	9
О прозрачном шифровании	62
Преимущества прозрачного шифрования	62
Прозрачное шифрование на локальном компьютере	61
Прозрачное шифрование сетевых папок	65
Резервное копирование зашифрованных файлов	67
Система доверенных приложений	68
Меры безопасности при использовании прозрачного шифрования	69
Защита дисков при помощи CyberSafe	10
О шифровании дисков программой CyberSafe	68
В чем отличие шифрования логического диска от создания виртуального диска?	69
Подготовка диска к шифрованию	69
Типы дисков, поддерживающие шифрование	69
Алгоритмы шифрования, используемые для шифрования дисков	70
Проверка работоспособности диска перед шифрованием	70
Расчет продолжительности шифрования	70
Обеспечение бесперебойного питания в процессе шифрования	71
Тестирование на совместимость программного обеспечения	71
Шифрование дисков и разделов	71
Шифрование логического диска/раздела	72
Создание виртуальных дисков	74
О виртуальных дисках CyberSafe	74
Создание нового виртуального диска	76
Использование виртуальных дисков	77
Удаление виртуального диска	78
Особые меры безопасности, предпринимаемые CyberSafe	78
Стирание пароля	78
Защита виртуальной памяти	78
Защита ключа шифрования	79
Другие меры безопасности	79
Скрытие информации при помощи CyberSafe	11
О скрытии информации на персональном компьютере	81
Скрытие файлов и папок	82

Скрытие логических дисков	83
Шифрование ключами КристоПРО CSP	12
О криптопровайдере КристоПРО CSP	85
Реализуемые алгоритмы	85
Шифрование файлов при помощи криптопровайдера КристоПРО CSP	86
Создание сертификата КристоПРО	86
Экспорт КристоПРО ключей в файл	88
Шифрование файлов и цифровая подпись ключами КристоПРО	88
Работа с паролями и ключевыми фразами	13
Что использовать: пароль или ключевую фразу?	90
Индикатор надежности пароля	91
Создание надежных паролей	91

1

Общая информация о программе CyberSafe

CyberSafe – программное обеспечение, использующее средства криптографии для защиты данных от несанкционированного доступа.

Программа предназначена для создания сертификатов и ключей шифрования, предоставляемый ею набор инструментов и функций применяется в таких сферах работы с информацией как: шифрование файлов и папок, защита электронной почты посредством использования сертификатов шифрования на почтовых клиентах, создание цифровой подписи, работа в качестве Цента Сертификации.

CyberSafe была протестирована и подтвердила надежность работы на всех операционных системах семейства Windows для ПК.

Программа шифрует информацию при помощи наиболее распространенных алгоритмов (AES, 3DES, ГОСТ, RSA, BlowFish) в зависимости от требуемой степени секретности. Кроме того, в своей работе CyberSafe использует библиотеки трех криптопровайдеров (OpenSSL, OpenPGP, Крипто-Про), благодаря чему отличается высокой гибкостью в работе.

Для более полного понимания работы программы рекомендуем вам ознакомиться с разделом *“Используемые термины”* и *“Симметричная и асимметричная криптография”*.

В этой главе

Что нового в CyberSafe версии 2.0.....	5
Условные обозначения, используемые в этом Руководстве	7
Для кого предназначен этот документ	8
Лицензионное соглашение.	8
Помощь по работе с программой.	12

Что нового в CyberSafe версии 2.0

Версия программы CyberSafe 2.0 сочетает в себе все основные функции и качества предыдущей версии, а также имеет ряд улучшений и новых дополнительных возможностей. Вместе с этим, был полностью изменен пользовательский интерфейс программы, что позволяет сделать работу с CyberSafe еще более простой, понятной и удобной.

История версий программы

Версия 2.0.0.21 от 12.09.2013

- Добавлен выбор всех сертов по умолчанию для шифрования.
- Исправлено, установка статуса "Not available." для Revocation при установке доверия "Trusted by user custom policy."

Версия 2.0.0.20 от 11.09.2013

- Исправлено, создание и установка корневого сертификата по ГОСТ КриптоПро.
- Установка корневого сертификата ГОСТ без прав администратора.
- Исправлено, ошибка отправки информации о сертификате на сервер с пробелами в имени сертификата.
- Добавлен экспорт сертификата КриптоПро.
- Добавлен импорт сертификата КриптоПро.

- Изменение алгоритма установки доверия сертификата.
- Исправлено, пустой список сертификатов для шифрования после импорта и дешифрации.
- Исправлено, не создается сертификат КriptoПро при перезаписи существующего.

Версия 2.0.0.19 от 23.08.2013

- Исправлено, сертификаты работают в Outlook и iPhone.
- Добавлено создание и установка корневого сертификата по ГОСТ.

Версия 2.0.0.18 от 09.08.2013

- Исправлена ошибка генерации и размещения в хранилище сертификата КП.
- Изменена структура базы данных для возможности хранения серийного номера сертификата КП.
- Реализована возможность хранения и получения информации о сертификате КП на сервере по серийному номеру.
- Добавлена проверка сертификата по базе по серийному номеру (Check Now).

Версия 2.0.0.17 от 06.08.2013

- Изменен код подтверждения публикации на 5-ти значный и изменен вид диалога ввода кода.
- Обеспечение работы сертификата в Outlook для подписи и шифрования.

Версия 2.0.0.16 от 05.08.2013

- Подробный прогресс создания сертификата.
- Переименованы комбобоксы на форме шифрования КП.
- Добавлен запрос на перезапись сертификата при импорте.
- Добавлена реализация Help-Home page.
- Исправлена ошибка отсутствия пгп файлов при экспорте чужих сертификатов.
- Исправлена ошибка: активная кнопка "Next" после расшифровки.
- Исправлена ошибка: кнопка Delete должна быть доступна только при выделении Родителя в TreeList, а не нодов.
- Исправлена ошибка: при расшифровке не показывается расшифрованный файл в папке.
- Убраны ненужные пункты в назначении сертификата.
- Добавлены точки в конце сообщений.
- Исправлена ошибка: сообщение об ошибке после прерывания создания сертификата.

Версия 2.0.0.15 от 12.07.2013

- Добавлена эмуляция мышки и клавиатуры для биологического датчика Кripto Про.

Версия 2.0.0.14 от 11.07.2013

- Добавлено проверка подписи Кripto-Про.
- Добавлено удаление сертификата Кripto-Про.
- Исправлена ошибка сортировки сертификатов.

Версия 2.0.0.13 от 09.07.2013

- Добавлена проверка наличия сертификата для шифрования.
- Добавлено создание подписи Кripto-Про.
- Изменен прогресс для добавления файлов и шифрования.

Версия 2.0.0.12 от 08.07.2013

- Исправлена ошибка доступа после нескольких операций шифрования и расшифровки.
- Добавлен хинт для "укороченных" надписей по ключу подписи.
- Добавлен прогресс при добавлении файлов на шифрование.
- Сделан более понятный прогресс при расшифровке.

- Добавлены точки в сообщениях.
- Исправлена ошибка доступности кнопки "Delete" в списке файлов.
- Сделан активным первый серт в списке для шифрования.
- Исправлен баг: при публикации после импорта теряются ключи ПГП.

Версия 2.0.0.11 от 05.07.2013

- Добавлено шифрование и расшифровка файлов Кripto Про.

Версия 2.0.0.10 от 04.07.2013

- Добавлен сервис для выполнения команд с правами администратора.
- Добавлено создание сертификата Кripto-Про.
- Добавлено изменение списка сертификатов для шифрования, в зависимости от провайдера.
- Кнопка "More Options" доступна только для шифрования OPGP.

Версия 2.0.0.9 от 03.07.2013

- Добавлена проверка целостности файла.
- Добавлен вывод информации по подписи, если сертификат не найден в базе и на сервере.

Версия 2.0.0.8 от 02.07.2013

- Добавлен признак Trusted (доверенный) для OPGP сертификата.
- Добавлена проверка на сервере - Отозван ли сертификат.
- Исправлен баг: ошибка при расшифровке файла, если нет нужного сертификата.
- Исправлен баг: ошибка при удалении сертификата после расшифровки и проверки подписи.

Версия 2.0.0.7 от 01.07.2013

- Исправлено: Прокрутка вправо при размере окна по умолчанию в окне сертов.
- Исправлено: Куда подевался KeyTreeList? Нельзя менять контролы после написания тестов!
- Исправлено: При проверке кода активации email в парсере лишние пробелы. Человек может случайно скопировать с лишними пробелами. Поэтому игнорировать пробелы до и после кода.
- Исправлено: Непонятный tmp файл при расшифровке написан.
- Исправлено: Конец расшифровки Access violation.
- Исправлено: Dir already Exists если по умолчанию расшифровывать. А должен быть запрос на перезапись.
- Исправлено: Directory doesn't exist если ввести вручную папку которой нет. А должно создавать и расшифровывать.
- Исправлено: Нельзя нажать More Options.
- Исправлено: Добавление многих файлов подвисает гуи.
- Исправлено: Должен быть прогресс распаковки файлов.
- Убрана горизонтальная прокрутка в списке сертификатов.

Версия 2.0.0.2 от 14.06.2013

- Добавлено шифрование файлов.

Версия 2.0.0.1 от 07.06.2013

- Прототип\Альфа.

Условные обозначения, использующиеся в Руководстве

Примечания. Дополнительные, но важные сведения, которые обращают Ваше внимание на важные моменты в работе с программой. Читая их, вы сможете использовать Cyber Safe более эффективно.

Предупреждения. Указывают на возможность потери данных либо на незначительные нарушения безопасности. Предупреждения расскажут вам о ситуациях, в которых могут возникнуть проблемы, если не принять необходимые меры предосторожности. Уделите этим пунктам должное внимание.

Предостережения. Указывают на возможность значительной потери данных или возникновения серьезной брешы в безопасности, а также сообщают о существенных проблемах, которые могут возникнуть в том случае, если не будут предприняты своевременные меры по их предотвращению. Отнеситесь к Предостережениям очень серьезно.

Для кого предназначен этот документ

Это Руководство адресовано всем, кто намерен использовать CyberSafe для защиты данных на персональных компьютерах, работающих под управлением ОС Windows.

Примечание. Если ранее вы не были знакомы с криптографией, ознакомьтесь с разделами *Симметричная* и *ассиметричная криптография*, а также *Дополнительные сведения о криптографии*.

Лицензионное соглашение на использование изделия

Настоящее Лицензионное соглашение является общей офертой ООО "КиберСофт" и Пользователем – физическим или юридическим лицом. Настоящее Лицензионное соглашение в случае согласия, выраженного в форме молчания в течении 7 дней с момента приобретения Изделия, в соответствии со ст. 433 ГК РФ, имеет силу договора.

Термины и определения

- Под Изделием понимается комплекс программ для ЭВМ, включая носители и документацию, который является объектом авторского права и охраняется законом.
- Везде в тексте под словом "документация" подразумеваются печатные материалы и носители, содержащие документацию в электронном виде. Документация является неотъемлемой частью Изделия.
- Данное Изделие (программный продукт), включая носители и печатные материалы, передается на условиях Лицензионного соглашения.
- Дальнейшая установка Изделия рассматривается как согласие с условиями Лицензионного соглашения и вступление его в законную силу.
- В случае несогласия с каким-либо из условий Лицензионного соглашения в течение семи дней со дня получения продукта, Пользователь должен вернуть полный комплект Изделия, включая печатные материалы и упаковку с носителями, в компанию, предоставившую данное Изделие.

Предмет соглашения

- Предметом настоящего Лицензионного соглашения является возмездная передача Пользователю прав пользования и владения на Изделие.
- Все условия, оговоренные далее, относятся как к Изделию в целом, так и ко всем его компонентам в отдельности.

Авторские права

- Изделие и его компоненты являются интеллектуальной собственностью разработчика и защищаются законодательством об авторском праве © 2013 КиберСофт (ООО).

- Право использования Изделия предоставляется только конечному Пользователю как владельцу, и никаким иным третьим лицам, если нет письменного согласия ООО "КиберСофт" на обратное.

Условия использования

- Пользователь может хранить, установить и использовать только определенное количество экземпляров Изделия. Пользователь не имеет права хранить, устанавливать или использовать (в установленном или установленном виде) большее количество экземпляров Изделия, чем предоставлено ему и определено в соответствующих документах на право использования Изделия.
- Пользователь обязуется не распространять данное Изделие. Под распространением Изделия понимается предоставление доступа третьим лицам к воспроизведенным в любой форме компонентам Изделия путем продажи, проката, сдачи внаем, предоставления займа или иными другими способами отчуждения.
- Пользователь не имеет права осуществлять следующую деятельность:
 - допускать использование Изделия людьми, не имеющими прав на такое использование;
 - пытаться дизассемблировать, декомпилировать (преобразовывать объектный код в исходный текст) программы и другие компоненты Изделия;
 - вносить какие-либо изменения в объектный код программ за исключением тех, которые вносятся средствами, включенными в комплект Изделия и описанными в документации;
 - совершать относительно Изделия другие действия, нарушающие Российские и международные нормы по авторскому праву и использованию программных средств.

Примечание. Использование шифровальных средств криптографической защиты информации подлежит лицензированию в соответствии с действующим законодательством РФ.

Срок действия соглашения

- Настоящее Лицензионное соглашение вступает в силу с момента вскрытия упаковки с носителями CyberSafe 2 или установки программного обеспечения из комплекта Изделия и действует на протяжении всего срока использования Изделия.
- В случае нарушения условий Лицензионного соглашения или неспособности далее выполнять его условия, все компоненты Изделия (включая печатные материалы, магнитные носители, файлы с информацией, архивные копии) должны быть уничтожены. Пользователь обязан подтвердить факт уничтожения Изделия в письменном виде. Лицензионное соглашение при этом прекращает свое действие.

Ответственность

- Пользователь приобретает Изделие и несет ответственность за его использование в соответствии с рекомендациями, изложенными в эксплуатационной документации.
- Нелегальное использование, распространение, воспроизведение для третьих лиц, копирование программного обеспечения является нарушением Закона Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных" и преследуется по закону.
- В случае нарушения настоящего Лицензионного соглашения конечный Пользователь лишается права на использование Изделия, при этом гарантийные обязательства на обслуживание Изделия снимаются.

Гарантии изготовителя (поставщика)

- Изготовитель гарантирует работоспособность Изделия при соблюдении

требований эксплуатации, транспортирования и хранения, корректном его пользовании и использовании Изделия в "невирусной среде".

- В случае выявления дефектов в программах, не связанных с нарушением правил эксплуатации, транспортирования и хранения, изделие подлежит рекламации в 10-дневный срок с момента обнаружения, и изготовитель обязуется по получении уведомления о претензии в возможно короткий срок устранить дефекты своими силами и средствами вплоть до поставки экземпляров изделия.
- Гарантийный срок изделия устанавливается 12 месяцев.
- Начальной датой исчисления гарантийного срока изделия является дата поставки изделия, зафиксированная в формуляре.
- Изготовитель (поставщик) принимает претензии к качеству поставки Изделия в течение тридцати дней со дня поставки.
- Действие гарантийных обязательств прекращается по истечении гарантийного срока.

Лицензионные положения и условия, замечания и информация третьих сторон

- Лицензионное соглашение по данному продукту ссылается на содержащиеся в данном файле сведения относительно положения и условий, применимых к включенному в данный продукт программному коду третьих сторон, а также на определенные замечания и прочую информацию, которую ООО "КиберСофт" должно предоставить вам в соответствии со своей лицензией на тот или иной программный код. Соответствующие положения и условия, замечания и прочая информация либо ссылки на них приводятся ниже.

Пожалуйста, учтите, что все версии приведенных ниже лицензий, представленные на каких-либо языках помимо английского, не являются официальными и приводятся только для вашего удобства. Официальной версией приведенных ниже лицензий является их версия на английском языке, представленная как часть английской версии данного файла.

Невзирая ни на какие положения и условия любых иных соглашений, которые могут быть заключены между вами и ООО "КиберСофт" или любой из ее родственных или дочерних компаний (совместно именуемыми "КиберСофт"), указанный ниже программный код третьих сторон представляет собой "Исключенные компоненты" и является предметом следующих положений и условий:

- Исключенные компоненты предоставляются "как есть";
- "КиберСофт" отказывается от предоставления любых и всяких явных и подразумеваемых гарантий и условий в отношении исключенных компонентов, включая, но не ограничиваясь таковыми, гарантии соблюдения или ненарушения чьих-либо авторских прав, а также подразумеваемые гарантии относительно коммерческого использования или пригодности для каких-либо целей;
- "КиберСофт" не будет нести перед вами никакой ответственности и не будет возмещать вам никаких убытков ни по каким претензиям, связанным с Исключенными Компонентами; а также "КиберСофт" не будет нести никакой ответственности ни за какие прямые, косвенные, случайные и фактические убытки или штрафные санкции, связанные с Исключенными Компонентами.
- К Программе прилагается программное обеспечение, в настоящее время разрабатываемое группой The OpenSSL Project (<http://www.openssl.org/>). Инструментарий OpenSSL toolkit подпадает под две лицензии, то есть, к этому инструментарию применимы как условия Лицензии OpenSSL, так и условия оригинальной лицензии SSLeay. Фактические тексты сообщений смотрите ниже. В действительности, обе эти лицензии представляют собой BSD-лицензии на Открытый Исходный Код. По всем касающимся лицензии вопросам, связанным с OpenSSL, обращайтесь, пожалуйста, по адресу: openssl-core@openssl.org. "КиберСофт" получила большую часть программных средств OpenSSL на

основании положения и условий следующих лицензий:

- *Лицензия OpenSSL*. Copyright (c) 1998-2003 The OpenSSL Project. Все права защищены.

Вторичное распространение и использование в виде исходного и двоичного кода с модификацией или без таковой разрешается при условии, что будут соблюдены следующие условия:

- Вторичные дистрибутивы исходного программного кода должны сопровождаться приведенным выше замечанием об авторских правах, этим списком условий и приведенным ниже отказом от предоставления услуг и гарантий.
 - Вторичные дистрибутивы исходного программного кода в двоичном виде должны сопровождаться приведенным выше замечанием об авторских правах, этим списком условий и приведенным ниже отказом от предоставления услуг и гарантий в печатной документации и/или в прочих материалах, прилагаемых к дистрибутиву.
 - Во всех рекламных материалах, где говорится о компонентах или об использовании этой программы, должна содержаться следующая ссылка: "Данный продукт включает в себя программное обеспечение, разработанное группой The OpenSSL Project для использования в OpenSSL Toolkit. (<http://www.openssl.org/>)"
 - Не разрешается без предварительного письменного разрешения использовать названия "OpenSSL Toolkit" и "OpenSSL Project" для представления или продвижения на рынок продуктов, полученных на основе данной программы. За письменным разрешением, пожалуйста, обращайтесь по адресу: openssl-core@openssl.org.
 - При отсутствии предварительного письменного разрешения от The OpenSSL Project запрещается присваивать продуктам, полученным на основе данного программного обеспечения, имена "OpenSSL", а также использовать в их именах слово "OpenSSL".
 - Вторичные дистрибутивы, независимо от их формы, должны содержать следующую ссылку: "Данный продукт включает в себя программное обеспечение, разработанное группой The OpenSSL Project для использования в OpenSSL Toolkit (<http://www.openssl.org/>)"
 - The OpenSSL Project предоставляет данную программу "как есть", при отказе от любых явных и подразумеваемых гарантий, включая, но не ограничиваясь таковыми, подразумеваемые гарантии относительно ее коммерческого использования или пригодности для каких-либо целей. ни при каких обстоятельствах ни группа OpenSSL Project, ни ее участники не несут ответственности ни за какие прямые, косвенные, случайные и фактические убытки (включая, но не ограничиваясь таковыми, приобретение товаров-заменителей или услуг, потерю данных или прибыли, или перерывы в деловой жизни), которые были тем или иным способом вызваны использованием этой программы, даже в случае предварительного уведомления о возможности таковых, независимо от того, каким образом они были причинены и каков предполагаемый порядок наступления ответственности - непосредственно на основании контракта либо по деликту (включая случаи халатности и иные).
- *Оригинальная Лицензия SSLeay*. Copyright (C) 1995-1998 Eric Young (eyay@cryptsoft.com). Все права защищены.
Данный пакет представляет собой реализацию SSL, автором которой является Eric Young (eyay@cryptsoft.com). Эта реализация была написана так, чтобы обеспечить соответствие с Netscape SSL.
Эта библиотека предоставляется бесплатно для коммерческого и некоммерческого использования постольку, поскольку соблюдаются приведенные ниже условия. Приведенные ниже условия относятся ко всему коду, находящемуся в данном дистрибутиве, независимо от того, является ли этот код кодом RC4, RSA, lhash или DES, а не только к

коду SSL. На прилагаемую к данному дистрибутиву документацию по SSL распространяются те же положения об авторских правах, за исключением того, что правообладателем является Tim Hudson (tjh@cryptsoft.com).

Авторское право сохраняет за собой Eric Young, в связи с чем не разрешается удалять из кода соответствующие замечания об авторских правах (Copyright). Если данный пакет используется в каком-либо продукте, там должна содержаться ссылка с указанием на то, что Eric Young является автором частей используемой библиотеки. Эта ссылка может появляться в форме текстового сообщения при запуске программы либо она может быть дана в документации (в электронной или текстовой), прилагаемой к пакету.

Вторичное распространение и использование в виде исходного и двоичного кода с модификацией или без таковой разрешается при условии, что будут соблюдены следующие условия:

- Вторичные дистрибутивы исходного программного кода должны сопровождаться замечанием об авторских правах, этим списком условий и приведенным ниже отказом от предоставления услуг и гарантий.
- Вторичные дистрибутивы исходного программного кода в двоичном виде должны сопровождаться приведенным выше замечанием об авторских правах, этим списком условий и приведенным ниже отказом от предоставления услуг и гарантий в печатной документации и/или в прочих материалах, прилагаемых к дистрибутиву.
- Во всех рекламных материалах, где говорится о компонентах или об использовании этой программы, должна содержаться следующая ссылка: "Этот продукт содержит криптографическую программу, автором которой является Eric Young (eay@cryptsoft.com)" Слово 'криптографическую' можно опустить, если части используемой библиотеки не связаны с криптографией :-).
- Если вы включите в продукт какой-либо специальный код для Windows (или производный код такового) из каталога apps (код приложения), то вы должны будете дать следующую ссылку: "Данный продукт содержит программные средства, автором которых является Tim Hudson (tjh@cryptsoft.com)".
- Eric Young предоставляет данную программу "как есть", при отказе от любых явных и подразумеваемых гарантий, включая, но не ограничиваясь таковыми, подразумеваемые гарантии относительно ее коммерческого использования или пригодности для каких-либо целей. ни при каких обстоятельствах ни автор, ни прочие участники не несут ответственности ни за какие прямые, косвенные, случайные и фактические убытки (включая, но не ограничиваясь таковыми, приобретение товаров-заменителей или услуг, потерю данных или прибыли, или перерывы в деловой жизни), которые были тем или иным способом вызваны использованием этой программы, даже в случае предварительного уведомления о возможности таковых, независимо от того, каким образом они были причинены и каков предполагаемый порядок наступления ответственности - непосредственно на основании контракта либо по деликту (включая случаи халатности и иные).
- Нельзя изменять положения лицензии и положения о распространении ни для каких публично предоставляемых версий производных продуктов данного кода. То есть, нельзя просто скопировать этот код и распространить на него лицензию на другой дистрибутив, включая Общедоступную Лицензию GNU (GNU Public License).

Помощь по работе с программой

Для более подробного изучения продукта ознакомьтесь, пожалуйста, со

следующими разделами.

Дополнительная информация о программе

Для получения более подробной информации о Cyber Safe посетите сайт программы www.cybersafesoft.com. На сайте доступны детальные видео-уроки по работе с программой и использованию ее основных функций.

На форуме сайта можно задать интересующие вас вопросы, узнать о методах устранения ошибок, а также ознакомиться с опытом работы других пользователей.

Контактная информация

Для связи с технической поддержкой, отправьте письмо на адрес электронной почты support@cybersafesoft.com или воспользуйтесь контактной формой на сайте: <http://cybersafesoft.com/rus/contacts>. *Обращаем Ваше внимание, что техническая поддержка по e-mail возможна лишь для пользователей, использующих платную версию программы.*

Адрес компании: Российская Федерация, Москва, ул. Марксистская, 32
Тел.: 8 (800) 555-28-43

2

CyberSafe. Основы

В этом разделе описывается терминология и основные функциональные возможности CyberSafe , а также приводятся некоторые важные концептуальные понятия из области криптографии.

В этой главе

Терминология и основные функции CyberSafe.	14
Симметричная и асимметричная криптография	16
Первое использование CyberSafe.....	16

Терминология и основные функции CyberSafe

Для того, чтобы использовать CyberSafe максимально эффективно, вам следует ознакомиться с ее основными функциями, а также специальными терминами, о которых пойдет речь в этой главе.

Терминология CyberSafe

Прежде чем вы впервые приступите к работе с CyberSafe , вам следует ознакомиться со следующими терминами:

- **Шифрование.** Процесс кодирования информации, позволяющий защитить ее от несанкционированного доступа. Получить доступ к зашифрованной информации без наличия специального ключа дешифрования невозможно, поэтому даже если злоумышленнику удастся завладеть ею, он никак не сможет ею воспользоваться.
- **Дешифрование.** Процесс приема зашифрованных сообщений и их декодирование, в результате чего защищенные данные приобретают исходное состояние и становятся доступными для использования.
- **Цифровая подпись.** Данные, которые вы пересылаете другим пользователям, можно подписывать, создавая на них цифровую подпись при помощи закрытого секретного ключа. Получив файлы, пользователь проверяет цифровую подпись на них при помощи открытого ключа и эта проверка доказывает, что данные получены именно от вас, а не от кого-либо другого.
- **Проверка цифровой подписи.** Процесс, в результате которого при помощи открытого ключа можно определить, действительно ли при создании цифровой подписи использовался индивидуальный закрытый ключ конкретного отправителя.
- **Ключевая пара.** Комбинация закрытый/открытый ключ. Создавая “ключ” в CyberSafe вы, по сути, создаете ключевую пару. В дополнение к закрытому и открытому ключам, она включает в себя ваше имя и адрес электронной почты, что оказывается очень удобным. Ключевая пара является вашим идентификатором в цифровом мире, точно так же, как ваш паспорт или водительские права идентифицируют вас в физическом мире.
- **Открытый ключ.** Публичный общедоступный ключ, который вы отправляете другим пользователям для того, чтобы они могли отправлять вам сообщения, зашифрованные с его помощью (сообщения, которые могут быть расшифрованы лишь при помощи вашего индивидуального закрытого ключа), а также проверить вашу цифровую подпись. Открытые ключи предназначены для широкого распространения. Открытый и закрытый ключи связаны в математической зависимости, однако получить

закрытый ключ из открытого невозможно.

- **Закрытый ключ.** Ваш индивидуальный секретный ключ, который следует хранить в тайне. Лишь с его помощью вы сможете расшифровать данные, которые были зашифрованы при помощи открытого ключа. Также только используя закрытый ключ вы сможете создать цифровую подпись, которая проверяется при помощи открытого ключа.

Предупреждение. Не доверяйте ваш закрытый ключ и пароль никому! Храните закрытый ключ в полной безопасности.

- **Сервер ключей.** Место хранения ключей. Некоторые компании используют серверы ключей для хранения открытых ключей своих сотрудников, благодаря чему те могут находить открытые ключи друг друга и обмениваться зашифрованными сообщениями.
- **Смарт-карты и токены.** Портативные устройства, на которых вы можете создавать или на которые можете копировать свои ключевые пары. Создавая ключевую пару на смарт-карте или токене, вы тем самым повышаете уровень безопасности, поскольку для шифрования и дешифрования файлов, а также для создания цифровой подписи и ее проверки потребуется иметь при себе это портативное устройство. Поэтому если неавторизованный пользователь захочет проникнуть в ваш компьютер, хранящиеся на нем зашифрованные данные будут в полной безопасности, поскольку ваша ключевая пара хранится не на жестком диске компьютера, а смарт-карте или токене, которые находятся при вас. Копирование ключевой пары на смарт-карту или токен – хороший способ использовать ее без взаимодействия с операционной системой, создать резервную копию, а также распространить ваш открытый ключ.

Основные функции программы

CyberSafe – программное обеспечение, использующие криптографию для защиты ваших данных от несанкционированного доступа. Функциональные возможности CyberSafe позволяют решать самые разносторонние задачи в области защиты информации. Список основных функций программы приведен ниже.

- **Шифрование файлов и папок.** Функция, предоставляющая возможность зашифровать любой файл, папку либо несколько файлов и папок одновременно для хранения на персональном компьютере либо отправки другим пользователям. Шифрование может быть выполнено на основе инфраструктуры открытых ключей (PKI) либо при помощи пароля. Расшифровать файлы можно только на компьютере с установленным CyberSafe .
- **Создание зашифрованных zip-архивов.** Функция, позволяющая объединить любое количество файлов и папок в одном зашифрованном архиве для удобства передачи или резервного копирования. Zip-архив защищается паролем. Расшифровать архив можно на любом компьютере.
- **Работа в качестве центра сертификации.** В своем составе CyberSafe имеет специализированное приложение CyberSafe Certificate Authority, предназначенное для создания, хранения и работы с сертификатами, а также позволяющее программе работать в качестве Центра сертификации.
- **Шифрование электронной почты.** Функция по защите электронных сообщений, обмен которыми происходит через почтовые клиенты, такие как Outlook 2010, The Bat!, Thunderbird и другие. Благодаря этой функции вся ваша электронная корреспонденция будет надежно защищена от злоумышленников.
- **Цифровая подпись.** Функция по созданию цифровых подписей на файлах и папках при помощи закрытого ключа, а также обеспечение проверки подписи с использованием открытого ключа.

Симметричная и асимметричная криптография

Симметричная криптография получила свое название благодаря тому, что в процессе шифрования и дешифрования информации используется один и тот же секретный ключ. Также ее называют традиционной криптографией. Этот вид криптографии отлично подходит для защиты данных, которые не планируются для передачи другим пользователям. Однако если вы собираетесь отправлять зашифрованные данные кому-то еще, особенно людям, с которыми вы незнакомы, этот вид защиты данных не очень хорош. На практике доставка секретных ключей, особенно по незащищенным каналам связи, а также их обновление безопасным и надежным способом очень проблематичны.

Асимметричная криптография. В процессе шифрования и дешифрования информации используются разные ключи – открытый и закрытый. Поэтому этот вид шифрования данных также называют шифрованием на основе инфраструктуры открытых ключей (Public Key Infrastructure). Закрытый ключ – это ваш индивидуальный секретный ключ, который используется для расшифровывания сообщений и создания цифровых подписей. Как видно из его названия, этот ключ следует хранить в тайне от посторонних и в большой безопасности. Второй ключ – открытый или публичный. В соответствии с его названием, вы можете делиться им с другими пользователями. На самом деле, вы должны им делиться.

Асимметричная криптография работает следующим образом. Предположим, что вы хотите обмениваться зашифрованными сообщениями со своим другом из другого города. И у него, и у вас должен быть установлен CyberSafe. Прежде всего, каждый из вас должен создать свою ключевую пару, состоящую из открытого и закрытого ключей. Свой закрытый ключ вы держите в тайне, а открытый отправляете на общедоступный сервер ключей. То же самое делает ваш друг. После этого вы скачиваете с сервера открытый ключ своего друга, а он – ваш (для обмена открытыми ключами существуют и другие возможности; подробнее об этом можно прочитать в главе *Работа с ключами*). Теперь ваш друг может отправить вам сообщение, зашифрованное при помощи вашего открытого ключа. А расшифровать его можно лишь используя закрытый ключ, который есть только у вас. **Данные, зашифрованные открытым ключом, расшифровать можно лишь при помощи закрытого ключа.** Даже ваш друг не сможет расшифровать то сообщение, которое он зашифровал. Открытый и закрытый ключи связаны между собой по математической зависимости, однако получить закрытый ключ из открытого невозможно.

Подробнее о криптографии

Для получения более подробной информации о криптографии, посетите домашнюю страницу сайта CyberSafe, перейти на которую можно из главного меню программы.

Первое использование CyberSafe

При первом использовании CyberSafe рекомендуем вам следовать следующим этапам:

1 Установите CyberSafe на свой компьютер

Если вы корпоративный пользователь, ваш системный администратор может предложить вам специальные инструкции по установке или настройке конфигураций программы. Но, так или иначе, установка является первым шагом.

2 Следуйте дальнейшим рекомендациям программы

Для того, чтобы помочь вам начать работу с CyberSafe после установки, программа предложит вам пройти несколько этапов по:

- Созданию сертификата и генерации ключевой пары;
- Публикации вашего сертификата и открытого ключа на сервере;

В том случае, если мастер установки программы был настроен системным администратором, программа может предложить выполнение других задач.

3 Обмен открытыми ключами с другими пользователями

После того, как ключевая пара создана, вы можете обмениваться зашифрованными сообщениями с другими пользователями (предварительно обменявшись с ними открытыми ключами). Обмен открытыми ключами – первый и важный шаг. Для того, чтобы отправить пользователю зашифрованное сообщение, вам понадобится скопировать его открытый ключ, а для того, чтобы пользователь смог отправить зашифрованное сообщение вам, у него должен быть ваш открытый ключ. Если вы до этого не опубликовали свой открытый ключ на сервере CyberSafe, сделайте это сейчас. Если у вас нет открытого ключа того пользователя, которому вы хотите отправить зашифрованное сообщение, сервер CyberSafe – первое место для его поиска.

4 Проверьте открытые ключи, которые вы загрузили с ненадежных серверов

Если вы скачали открытый ключ с ненадежного сервера, постарайтесь убедиться в том, что он не был изменен, а также в том, что этот ключ действительно принадлежит тому пользователю, о котором идет речь. Для того, чтобы сделать это используйте CyberSafe и сравните уникальный электронный отпечаток вашей копии открытого ключа пользователя с электронным отпечатком подлинного открытого ключа (хороший способ сделать это – позвонить владельцу ключа по телефону и запросить информацию об электронном отпечатке, для того, чтобы вы смогли ее сверить). Открытые ключи, хранящиеся на доверенных серверах, таких как сервер CyberSafe уже были проверены.

5 Начните защищать свои файлы и электронную почту

После того, как была сгенерирована ключевая пара и вы обменялись открытыми ключами с другими пользователями, вы можете начать использовать функции по шифрованию, дешифрованию, цифровой подписи и ее проверке применительно к сообщениям электронной почты и файлам.

3

Установка CyberSafe

В этом разделе описывается процесс инсталляции CyberSafe на локальный компьютер, а также первые действия по работе с программой после ее установки.

В этой главе

Перед установкой	18
Установка и настройка CyberSafe	18
Деинсталляция CyberSafe	21
Перемещение CyberSafe с одного компьютера на другой	22

Перед установкой

Здесь говорится о минимальных системных требованиях, которые необходимы для успешной установки CyberSafe на локальный компьютер, работающий под управлением ОС Windows.

Системные требования

Перед началом установки программы убедитесь, что ваша операционная система удовлетворяет следующим минимальным требованиям:

- Microsoft Windows 2000 (Service Pack 4), Windows Server 2003 (Service Pack 1 и 2), Windows XP Professional 32-бита (Service Pack 2 или 3), Windows XP Professional 64-бита (Service Pack 2), Windows XP Home Edition (Service Pack 2 или 3), Microsoft Windows XP Tablet PC Edition 2005 (требующий подключения клавиатуры), Windows Vista (все 32- и 64-битные версии, включая Service Pack 1 и 2), Windows 7 (все 32- и 64-битные версии), Windows 8 (все 32- и 64-битные версии).

Примечание. Программа будет полностью совместима с перечисленными выше операционными системами лишь в том случае, если на них установлены все последние обновления Microsoft.

- 512 MB оперативной памяти
- 88 MB свободного пространства на жестком диске

Установка и настройка CyberSafe

В этом параграфе содержится информация о том, как правильно установить и настроить CyberSafe .

Установка программы

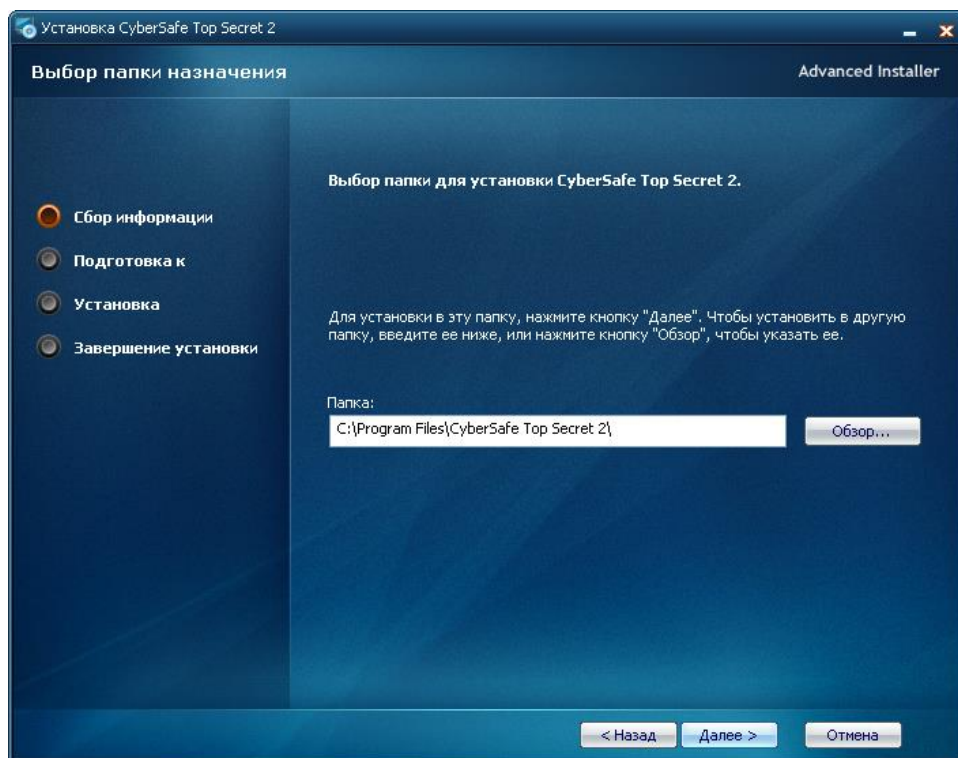
Примечание. Для того, чтобы установить CyberSafe вы должны обладать правами администратора. Перед началом установки рекомендуется закрыть все другие приложения и программы.

- **Для того, чтобы установить CyberSafe , выполните следующие действия:**

- 1 Найдите на своем компьютере инсталляционный дистрибутив с программой - файл с расширением *.exe.
- 2 Дважды кликните мышью на этом установочном файле.
- 3 Следуйте инструкциям на экране:

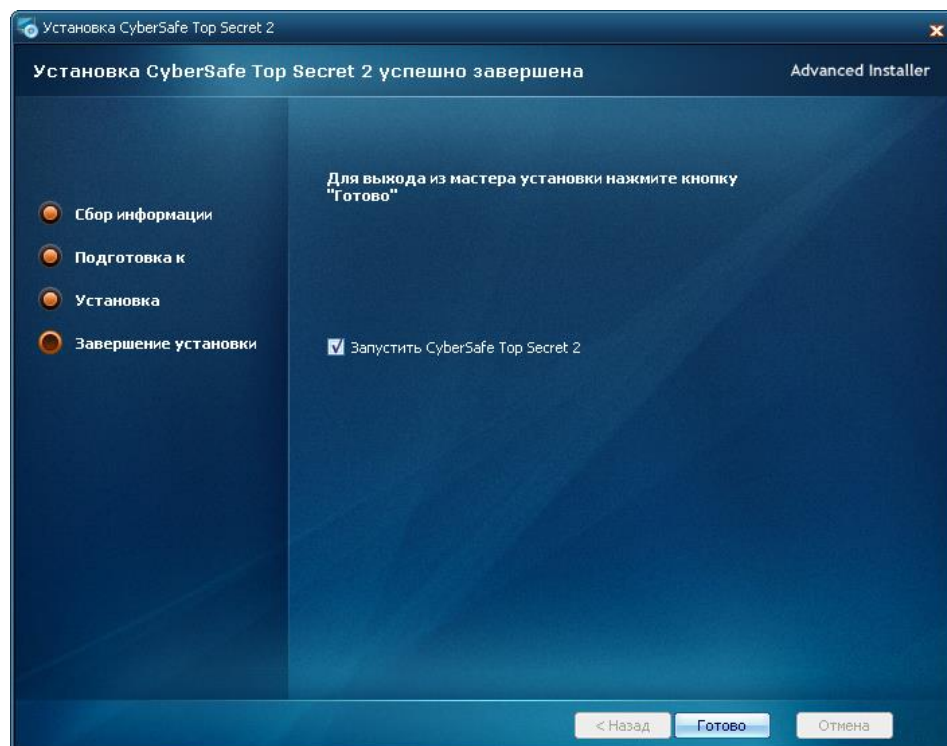
В открывшемся окне мастера установки CyberSafe Setup нажмите **Далее**.

По умолчанию путь к файлам с установленной программой будет следующим: **C:\Program Files\CyberSafe 2**. Если вы хотите выбрать другой каталог для установки, воспользуйтесь кнопкой **Обзор**. Нажмите **Далее**:



После завершения подготовки к установке нажмите кнопку **Установить**. Если вы решили изменить какую-то из настроек, вернитесь к предыдущим установкам, воспользовавшись кнопкой **Назад**.

Если установка прошла успешно, по ее завершению вы увидите следующее окно, в котором следует нажать кнопку **Готово**. Если вы хотите запустить программу сразу после установки, установите галочку в соответствующем чекбоксе:



- 4 В том случае, если программа установки предложит перезагрузить компьютер, сделайте это. Установка CyberSafe 2 завершена.

Создание сертификата и настройка программы

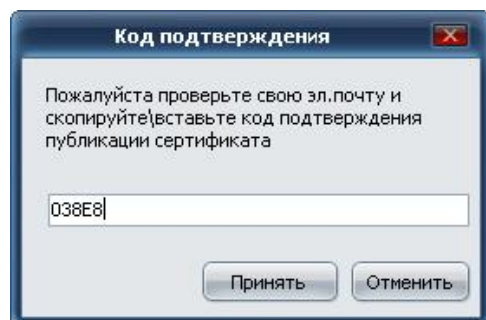
После того, как установка CyberSafe завершена и, при необходимости, выполнена перезагрузка компьютера, программа запустится автоматически. На экран будет выведено окно по созданию сертификата.

Поля, обязательные для заполнения, помечены символом *. В поле Email Address укажите свой действующий электронный адрес – на него будет выслан код, необходимый для публикации сертификата на сервере. Пароль должен состоять из латинских букв (желательно имеющих разный регистр) и цифр. Индикатор надежности пароля поможет оценить, насколько силен вводимый вами пароль (подробнее о создании сильных паролей см. в главе *Работа с паролями и ключевыми фразами*). В дальнейшем этот пароль понадобится вам в процессе работы с программой:

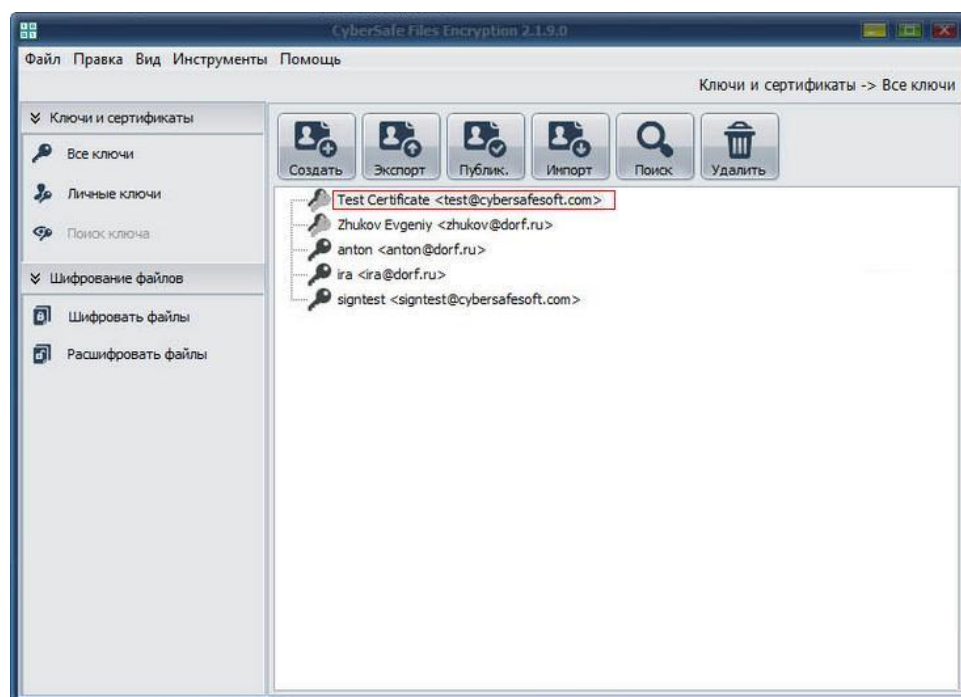


Рекомендуется заполнить и необязательные поля – эта информация будет присутствовать на вашем сертификате, в том числе и ваше фото. Укажите размер ключа шифрования в пределах от 1024 до 4096 бит, а также срок его действия. Галочка в чекбоксе *Опубликовать после создания* подразумевает автоматическую публикацию вашего сертификата на сервере – оставляем ее включенной и нажимаем кнопку **Далее**.

После этого пройдет процесс генерации ключей сертификата, по окончании которого на указанный вами e-mail будет выслан код, который потребуется ввести в соответствующее поле, после чего произойдет публикация вашего сертификата на сервере.



После успешного подтверждения процедура по созданию сертификата завершена. Результат можно увидеть в главном окне программы:



Создание сертификата завершено.

Деинсталляция CyberSafe

Удалить программу с локального компьютера можно при помощи стандартной функции Windows "Установка и удаление программ".

► **Для деинсталляции CyberSafe при помощи стандартной функции Windows выполните следующие действия:**

1. Перейдите в меню **Пуск > Панель управления > Установка и удаление программ**.

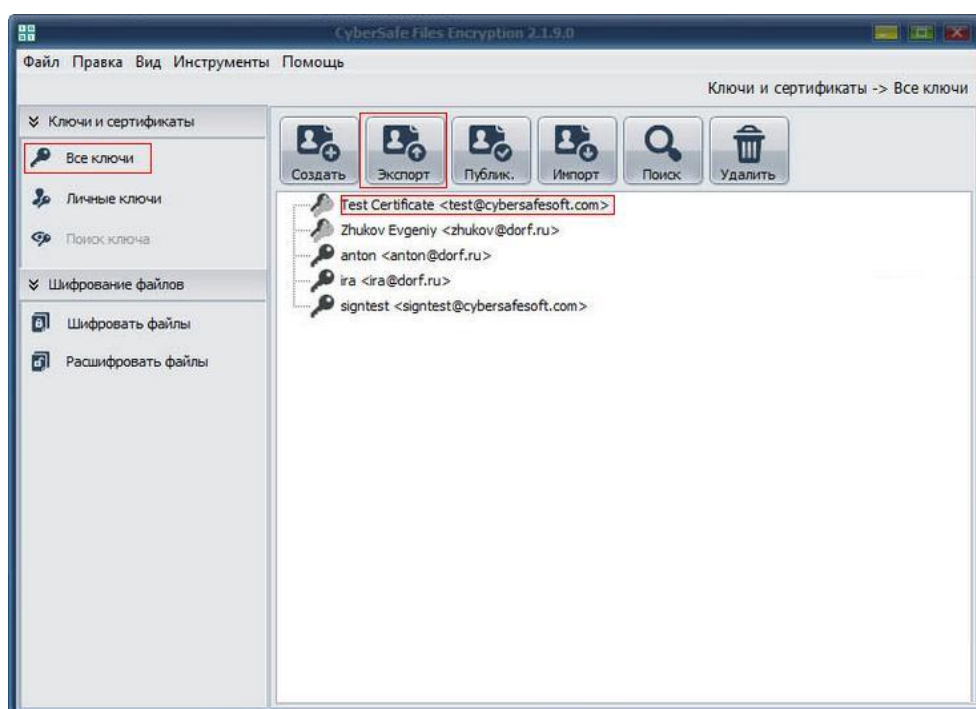
- 2 В списке с установленными программами найдите CyberSafe и нажмите **Удалить**. После появления системного диалогового окна, запрашивающего подтверждение на удаление программы, нажмите **Да**.

Перемещение CyberSafe с одного компьютера на другой

Перемещение CyberSafe с одного компьютера на другой – не сложный процесс. Основная задача заключается в правильном перемещении файла ключей, который потребуется экспортировать из базы данных программы, установленной на старом компьютере и импортировать в базу данных на новом.

- Для перемещения программы на другой компьютер выполните следующие действия:

- 1 Перейдите на вкладку **Все ключи**, выделите нажатием левой кнопки мыши имя свой сертификат и на верхней панели нажмите кнопку **Экспорт**. В открывшемся диалоговом окне введите свой пароль к данному сертификату.



- 2 Требуется экспортировать файл ключей, имеющий расширение *.id, поэтому в появившемся окне необходимо поставить галочку напротив пункта "Экспорт ID файла":



- 3 Укажите папку, в которую будут экспортированы выбранные файлы и

нажмите **Принять**. Произойдет экспорт файлов в указанную папку. Имя файла ключей совпадает с вашим e-mail и имеет расширение *.id. Копируем этот файл на новый компьютер и, при необходимости, удаляем CyberSafe со старого.

Примечание. Удаление программы с локального компьютера не ведет к удалению сертификатов и файлов ключей.

- 4 Установите CyberSafe на новый компьютер согласно инструкции, описанной выше.
 - 5 Перейдите на вкладку **Все ключи**, на верхней панели нажимаем кнопку **Импорт**, в проводнике Windows найдите файл ключей, указав то место, куда вы его скопировали, выделите его и нажмите кнопку **Открыть**. В появившемся окне введите свой пароль. Далее программа импортирует указанный файл ключей и создаст ваш сертификат.
- Перемещение CyberSafe на новый компьютер выполнено.

4

Пользовательский интерфейс CyberSafe

В этом разделе описывается пользовательский интерфейс CyberSafe .

В этой главе

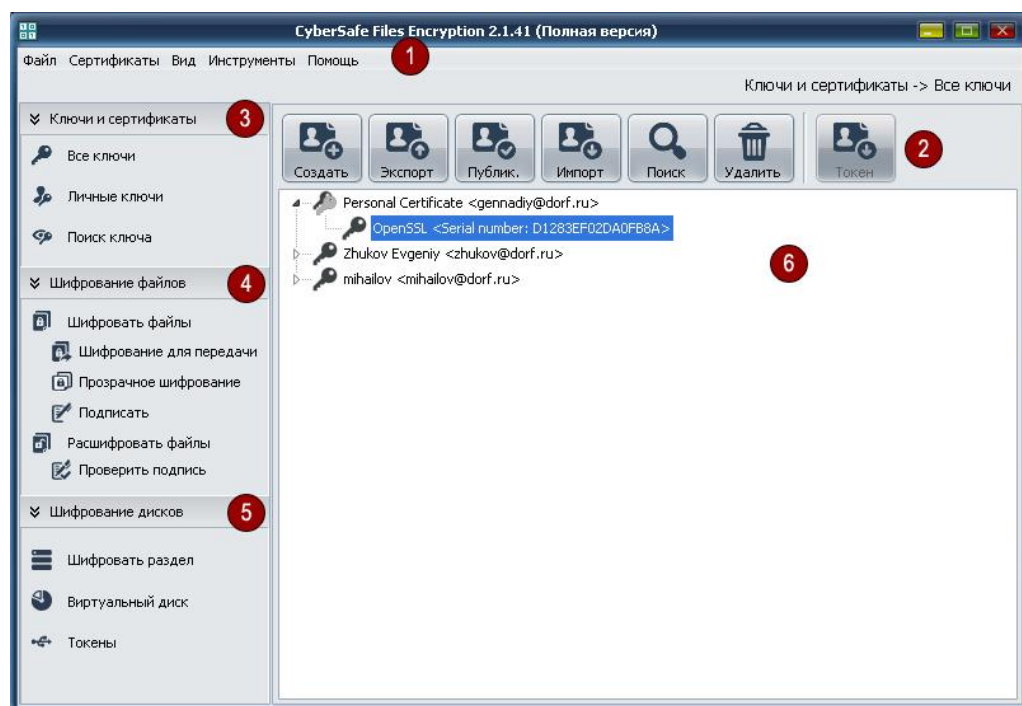
Доступ к основным функциям CyberSafe 24

Доступ к основным функциям Cyber Safe

Доступ к основным функциям программы осуществляется через ее главное окно, открыть которое можно либо дважды кликнув на ярлыке программы с расширением *.exe, либо перейдя **Пуск > Все программы > CyberSafe 2**.

Главное окно программы

Интерфейс главного окна программы содержит все ее основные функции.



Главное окно Cyber Safe содержит:

1	Основное меню. Предоставляет доступ к основным функциям программы. Пункты меню содержат дополнительные выпадающие вкладки, соответствующие выбранной категории.
2	Меню опций. Содержит опции создания, экспорта, импорта, публикации, поиска и удаления, все или некоторые из которых могут быть применены к файлам, папкам, дискам и сертификатам.
3	Ключи и сертификаты. Доступны вкладки "Все ключи", "Мой закрытый ключ", а также функция "Поиск ключей" (в результатах поиска выдаются данные основываясь на имени или электронном адресе пользователей).

4	Шифрование файлов. Доступ к функциям по шифрованию и дешифрованию файлов, созданию и проверки цифровой подписи.
5	Шифрование дисков. Доступ к функциям по шифрованию логических дисков и их разделов, созданию виртуальных зашифрованных дисков, а также хранению ключей на токенах.
6	Рабочая область Cyber Safe . Отображает информацию, а также действия, которые могут быть предприняты в соответствии с выбранным пунктом меню.

Все блоки вертикального меню под номерами 3, 4, 5 изначально отображаются в развернутом виде, но, с целью рационального использования рабочего пространства и экономии места могут сворачиваться. Для того, чтобы свернуть/развернуть блок используйте значок .

Пункты *Меню опций*, а также содержание *Рабочей области* меняется в зависимости от того, какой из пунктов в меню вы выбрали.

К примеру, при выборе функции **Шифрование файлов** в *Рабочей области* отобразится возможность выбора одного из двух вариантов шифрования (для личного пользования или пересылки другим пользователям), а в *Меню опций* будут доступны опции *Добавить папку*, *Добавить файл*, *Удалить* и *Показать*. А при выборе пункта меню **Все ключи** в *Рабочей области* отобразится список всех доступных ключей на вашей связке, а в *Меню опций* отобразятся опции *Создать*, *Экспорт*, *Публикация*, *Импорт*, *Поиск* и *Удалить*.

5

Работа с ключами CyberSafe

Под работой с ключами CyberSafe подразумевается создание и хранение ключевой пары, а также открытых ключей других пользователей.

В этом разделе описываются виды ключей, процесс создания ключевой пары, распространения вашего открытого ключа, а также получение открытых ключей других пользователей.

В этой главе

Просмотр ключей.	26
Создание ключевой пары.	26
Защита закрытого ключа.	27
Распространение открытого ключа.	29
Получение открытого ключа от других пользователей.	31
Импорт ключей и сертификатов.	32
Работа с серверами ключей.	32

Просмотр ключей

Для просмотра ключей на локальной связке, откройте CyberSafe и в пункте меню **Ключи и Сертификаты** (Keys and Certificates) выберите:

- **Все ключи** (All Keys). Будут отображены все ключи на вашей связке.
- **Личные ключи** (Private Keys). Будут отображены только закрытые ключи на вашей связке.
- **Поиск ключа** (Search for Keys). Поиск ключа на вашей связке исходя из указанных критериев.

Ваши **Личные ключи** имеют значок  и содержат ваш открытый и закрытый ключи. Ключи других пользователей, отображаемые на связке **Все ключи** вместе с вашими Личными ключами, имеют значок  и содержат только открытые ключи этих пользователей.

Создание ключевой пары

Возможно, вы уже создавали ключевую пару в CyberSafe самостоятельно после первого запуска программы, либо при работе с ее предыдущими версиями, но если нет, вам нужно сделать это сейчас, поскольку при использовании CyberSafe практически каждая операция связана с работой с ключевой парой.

Создание ключевой пары в CyberSafe происходит при создании сертификата, созданные ключи хранятся в базе данных программы и, при необходимости, могут быть экспортированы в отдельные файлы.

Предупреждение. Не следует постоянно создавать новые ключи и сертификаты. Сертификаты, используемые в CyberSafe подобны электронным паспортам или водительским удостоверениям; создавая их в большом количестве, вы в конечном итоге запутаете и себя, и тех пользователей, с которыми обмениваетесь зашифрованными сообщениями. Лучше всего иметь один сертификат и одну ключевую пару.

► Для создания ключевой пары

- 1 Убедитесь, что выбран пункт меню **Ключи и Сертификаты** (Keys and

Certificates).

- 2 В **Меню опций** выберите пункт **Создать** (Create). Пройдите процедуру по созданию сертификата, которая подробно описана в параграфе *"Создание сертификата и настройка программы"*.
Укажите **Размер ключа** (Key size) в диапазоне от 1024 до 4096 бит. Чем больше размер ключа, тем он надежнее, но тем дольше будет проходить его генерация.
Укажите **Срок действия** (Validity) ключа в днях. По умолчанию срок действия установлен 365 дней. По истечении установленного срока действия потребуется создать новую ключевую пару.
- 3 Убедитесь, что после создания сертификата он, а также созданные ключи отображаются на связке ключей в Рабочей области. Если вы не видите нового сертификата в списке, убедитесь, что в меню Ключи и Сертификаты выбран пункт **Все ключи** (All Keys) или **Личные ключи** (Private Keys).

Предупреждение. На этом этапе рекомендуется сделать резервную копию вашего закрытого ключа, сохранив ее в безопасном месте. Ваш закрытый ключ очень важен, а его потеря может иметь катастрофические последствия если вы уже использовали этот ключ для шифрования ценных для вас данных. Подробнее об этом смотрите в параграфе *"Защита закрытого ключа"*.

Использование паролей

Зашифровать файл, а потом оказаться неспособным его расшифровать – это болезненный урок, позволяющий понять, насколько важным является выбрать пароль, который вы всегда будете помнить.

Большинство приложений требуют создание пароля длиной от трех до восьми символов. Плохой идеей является использование в качестве пароля слова, которое можно найти в словаре. Этого делать не рекомендуется, поскольку такой пароль является уязвимым для атак, использующих подбор пароля из базы данных, составленной на основе словарей. Подход здесь заключается в том, что программа по взлому паролей перебирает по очереди все имеющиеся в словаре слова и их комбинации до тех пор, пока не определит ваш пароль. Такие программы способны находить массивы с паролями, даже если используемые в них термины были в большей или меньшей мере изменены по сравнению с их изначальной формой в словаре.

Для защиты от такого вида атак настоятельно рекомендуется создавать пароль, включающий комбинацию символов верхнего и нижнего регистра, цифры, знаки пунктуации и пробелы. Это обеспечит создание надежного пароля, однако усложнит его запоминание.

Стремление противостоять таким атакам приводит к тому, что вы создаете сложный пароль, который легко забыть. Это может привести к потере информации, потому что вы не сможете использовать его для расшифровывания своих собственных защищенных файлов.

Выбор пароля экспромтом скорее всего приведет к его полному забыванию. Постарайтесь использовать те фразы, которые уже прижились в вашей долговременной памяти. Это не должно быть чем-то, что вы недавно повторяли кому-то, а также это не должны быть известные цитаты, поскольку вы намереваетесь создать пароль, который будет трудно подобрать злоумышленникам.

Конечно, если вы будете настолько безрассудны, что запишите где-нибудь свой пароль, прикрепите его к монитору или положите в ящик стола, тогда будет совсем не важно, насколько трудную комбинацию вы выбрали.

Для получения более подробной информации по этому вопросу, см. параграф *"Работа с паролями"*.

Защита закрытого ключа

Компания "КиберСофт" настоятельно рекомендует вам выполнить следующие действия сразу же после того, как вы создадите свой сертификат и ключевую

пару.

Предупреждение. Если не воспользоваться приведенными ниже рекомендациями, в дальнейшем это может привести к потере ценных для вас данных.

- Создайте резервную копию вашего закрытого ключа в еще одном безопасном месте, в том случае если ваша основная копия еще не повреждена и не потеряна. Подробнее об этом см. в параграфе *"Создание резервной копии закрытого ключа"*.
- Посмотрите на выбранный пароль еще раз для того, чтобы убедиться, что вы его не забудете. Если вы в этом не уверены, измените пароль ПРЯМО СЕЙЧАС на тот, который вы не сможете забыть.

Ваш закрытый ключ очень важен, поскольку если данные были зашифрованы отправителем при помощи открытого ключа, расшифровать их можно лишь при помощи закрытого ключа получателя. Это также справедливо и для вашего пароля – утрата пароля или закрытого ключа приведет к тому, что вы не сможете расшифровывать данные, зашифрованные отправителем при помощи открытого ключа, а также данные, зашифрованные для вашего личного пользования.

Как только данные зашифрованы, никто, даже компания "КиберСофт", не сможет их расшифровать без вашего закрытого ключа и пароля. Это означает, что если вы зашифруете важную для вас информацию, а затем либо забудете пароль, либо утратите закрытый ключ, зашифрованные данные окажутся недоступными, непригодными к использованию и подлежащими восстановлению.

Меры, предпринимаемые для защиты ключей

Кроме создания резервных копий ваших ключей, вы также должны быть очень внимательны по отношению к тому, где храните свой закрытый ключ. Не смотря на то, что ваш закрытый ключ защищен паролем, который известен только вам, существует возможность, что кто-то узнает ваш пароль и тогда воспользуется вашим закрытым ключом для расшифровки ваших электронных писем или подделки цифровой подписи. Например, кто-то может запомнить сочетание клавиш, которое вы нажимаете при вводе пароля или даже перехватить его по локальной сети или через Интернет.

Для того, чтобы не позволить злоумышленникам, которые могли перехватить ваш пароль, воспользоваться вашим закрытым ключом, храните закрытый ключ только на своем компьютере. Если ваш компьютер подключен к локальной сети, убедитесь, что ваши файлы не входят в число тех, с которых создаются резервные копии, используя которые другие пользователи могут получить доступ к закрытому ключу.

Учитывая тот факт, что при подключении к локальной сети компьютеры становятся более уязвимыми, если вы работаете с очень ценной информацией, закрытый ключ можно хранить на дискете, которую вам потребуется использовать в качестве старомодного ключа всякий раз в случае возникновения необходимости прочитать или подписать секретную информацию.

Примечание. Изменение пароля на вашем ключе не ведет к изменению пароля на какой-либо из копий этого ключа (например, созданной при резервном копировании). Если вы подозреваете, что закрытый ключ вашего сертификата мог быть скомпрометирован, компания "КиберСофт" рекомендует вам удалить все предыдущие копии этого ключа и после создать сертификат снова.

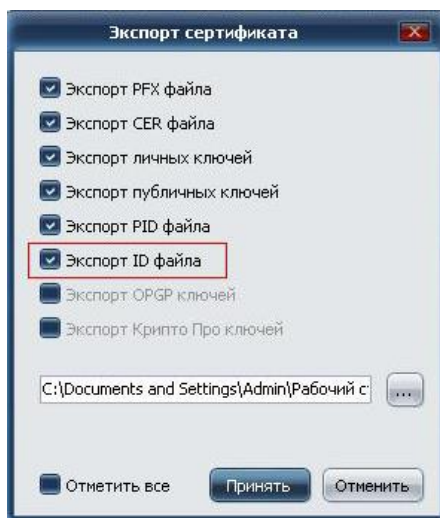
Создание резервной копии ключей

Ваш закрытый и открытый ключи хранятся в базе данных программы. Для того, чтобы создать их резервную копию с целью хранения в другом месте на жестком диске или съемном носителе, ключи нужно экспортировать из базы

данных.

► Для создания резервной копии ключей

- 1 В меню Ключи и Сертификаты выберите пункт **Личные ключи**.
- 2 В Рабочей области в списке ключей выделите нужный ключ и нажмите **Экспорт**. В открывшемся диалоговом окне ввода пароля введите свой пароль для данного ключа (сертификата).
- 3 В открывшемся диалоговом окне программы выберите **Экспорт ID файла** и укажите место на локальном компьютере или съемном носителе, куда будут экспортированы ключи. Нажмите **Принять**:



- 4 Экспортированный файл, содержащий ваш закрытый и открытый ключи, имеет расширение ***.id**. Если директория для экспорта отличалась от места, в котором вы хотите хранить вашу резервную копию ключей, найдите в экспортированных файлах файл с этим расширением и скопируйте его в безопасное место. Это может быть CD/DVD диск, другой персональный компьютер или USB-флеш накопитель, который вы храните в безопасном месте. Пожалуйста, помните, что **этим файлом не нужно делиться с другими пользователями, так как он содержит ваш закрытый ключ**.

Что если закрытый ключ утерян?

Если ваш закрытый ключ утерян и у вас нет его резервной копии, вы больше никогда не сможете расшифровать информацию, зашифрованную вами или другими пользователями при помощи открытых ключей. Такая информация оказывается бесполезной и не подлежит восстановлению.

Распространение открытого ключа

После того, как вы создали ключевую пару, вам нужно распространить копии своего открытого ключа тем пользователям, с которыми вы намереваетесь обмениваться зашифрованными сообщениями. Вы делаете свой открытый ключ доступным для тех, кто будет отправлять вам зашифрованную информацию и проверять вашу цифровую подпись, а также вам нужны открытые ключи тех пользователей, которым вы планируете отправлять зашифрованные сообщения.

Распространить открытый ключ можно несколькими способами:

- Опубликовать свой ключ на сервере (см. параграф *"Размещение открытого ключа на сервере ключей"*). По большому счету, этот способ является основным и его одного может быть вполне достаточно.
- Добавить открытый ключа в e-mail сообщение (см. параграф *"Добавление открытого ключа в e-mail сообщения"*).
- Экспортировать или скопировать открытый ключ в файл (см. параграф

(“Экспорт открытого ключа в файл”).

Публикация на сервере

Лучшим способом сделать ваш открытый ключ доступным для других пользователей является его размещение на общедоступном сервере, представляющем собой большую базу данных ключей. Таким образом, пользователи смогут отправлять вам зашифрованные сообщения без необходимости специально запрашивать копию вашего открытого ключа. Также, это избавляет вас и других от необходимости хранить большое количество открытых ключей, которые вы редко используете.

По всему миру существует множество серверов ключей, в том числе и сервер CyberSafe, на которых вы можете сделать свой открытый ключ доступным для каждого.

Прежде чем вы начнете работу с каким-либо из серверов ключей и разместите на них копии своего открытого ключа примите во внимание следующие моменты:

- Это именно тот ключ, который вы намереваетесь использовать? Другие пользователи попытаются связаться с вами, зашифровав информацию при помощи этого открытого ключа. Поэтому, мы настоятельно рекомендуем вам публиковать на сервере ключей только тот открытый ключ, который действительно предназначается для других пользователей.
- Запомните ли вы пароль для этого ключа? Или, если вы не намереваетесь в дальнейшем использовать этот ключ, быть может, будет лучше не размещать его на сервере?
- Некоторые серверы ключей, в отличие от сервера CyberSafe, придерживаются политики, согласно которой, если открытый ключ опубликован на сервере, он должен оставаться там и в дальнейшем, из-за чего и у вас могут возникнуть трудности с удалением открытого ключа. На некоторых серверах имеются функции по автоматическому распространению ключей на другие серверы, поэтому даже если вы сможете удалить свой ключ на этом сервере, он может появиться на нем позже.

Как правило, пользователи публикуют свои открытые ключи на сервере CyberSafe во время создания сертификата и ключевой пары. Если вы уже сделали это, вам не нужно публиковать свой открытый ключ снова. В большинстве случаев, нет необходимости также публиковать свой открытый ключ и на других серверах ключей.

Примите во внимание также и тот факт, что другие серверы могут не проверять подлинность размещаемых ключей, поэтому, если вы скачаете открытый ключ с такого сервера, с вашей стороны может потребоваться потратить большее количество усилий для того, чтобы связаться с владельцем открытого ключа и сверить с ним уникальный электронный отпечаток этого ключа.

► Для публикации открытого ключа на сервере вручную

- 1** Откройте CyberSafe .
- 2** Убедитесь что выбрано меню Ключи и Сертификаты (Keys and Certificates).
- 3** В Рабочей области выделите тот ключ, который вы хотите опубликовать и в Меню опций нажмите кнопку **Публиковать** (Publish).
- 4** На ваш e-mail, указанный при создании сертификата, будет выслан код подтверждения – введите его в открывшееся диалоговое окно и нажмите **Принять**. После этого пройдет публикация вашего открытого ключа на сервере CyberSafe.

Как только ваш открытый ключ размещен на сервере, он становится доступным для пользователей, которые хотят отправить вам зашифрованные данные или проверить вашу цифровую подпись. Даже если вы напрямую не укажете пользователям ваш открытый ключ, они могут получить его копию

при помощи функции поиска на сервере ключей, используя для этого ваше имя или адрес электронной почты.

Многие пользователи включают web-адрес своего открытого ключа в конце своих e-mail сообщений. В большинстве случаев, получателю такого e-mail достаточно просто кликнуть на адресе для того, чтобы получить копию открытого ключа на сервере. Некоторые даже размещают уникальные электронные отпечатки своих открытых ключей на своих визитных карточках для упрощения их проверки.

Добавление открытого ключа в e-mail сообщение

Другим хорошим способом распространить свой открытый ключ другим пользователями является добавление его в e-mail сообщения.

Отправляя кому-либо открытый ключ, не забудьте подписать электронное сообщение своей цифровой подписью. Таким образом, получатель сможет проверить вашу подпись и убедиться в том, что никто не изменял информацию на этом этапе. Конечно, если ваш ключ еще не был проверен ни одним доверенным поручителем, получатель может быть точно уверенным в том, что это ваша цифровая подпись лишь сверив с вами ее уникальный электронный отпечаток.

Экспорт открытого ключа в файл

Еще одним способом поделиться открытым ключом с другими является его экспорт в файл, имеющий расширение *.pid, после чего этот файл нужно сделать доступным для пользователя, с которым вы хотите обмениваться зашифрованной информацией.

Получение открытого ключа от других пользователей

Наряду с тем, что вам нужно распространять свой открытый ключ, также вам необходимо получить открытые ключи других пользователей для того, чтобы отправлять им зашифрованные сообщения и проверять их цифровые подписи.

Для этого существует несколько способов:

- Найти открытый ключ вручную на сервере;
- Добавить на свою связку ключей открытый ключ, прикрепленный в e-mail сообщении;
- Получить открытый ключ из экспортированного файла.

Открытые ключи представляют собой простые блоки текста, поэтому они легко могут быть добавлены на вашу связку ключей посредством импорта их из файла или копирования из e-mail сообщения с последующим добавлением на связку.

Скачивание открытого ключа с сервера ключей

Если человек, которому вы хотите отправить зашифрованное сообщение, является опытным пользователем CyberSafe, скорее всего, он уже разместил свою копию открытого ключа на сервере CyberSafe или на другом сервере. Это является очень удобным для вас, поскольку вы всегда можете использовать самую последнюю версию этого ключа. Кроме того, это избавляет вас от необходимости хранить множество открытых ключей на своей связке.

Существует множество открытых серверов ключей, подобных серверу CyberSafe, на которых вы можете найти ключи интересующих вас пользователей. В том случае, если пользователь не указал вам web-адрес где храниться его открытый ключ, вы можете зайти на любой сервер ключей и выполнить поиск по имени пользователя или его адресу электронной почты. Это может сработать, а может и не сработать, поскольку не все открытые серверы ключей регулярно обновляют информацию о ключах, хранящихся на остальных серверах.

► Для получения открытого ключа пользователя с сервера

- 1 Откройте CyberSafe и перейдите в меню **Ключи и Сертификаты** (Keys and Certificates).
- 2 Выберите пункт **Поиск ключей** (Search for Keys).
- 3 В диалоговом окне введите e-mail пользователя, открытый ключ которого вы хотите нажать **Принять**.
- 4 Если ключ данного пользователя уже размещен на сервере CyberSafe он автоматически будет добавлен на вашу связку. Проверить добавление ключа можно перейдя на вкладку **Все ключи** (All Keys)

Импорт ключей и сертификатов

Вы можете импортировать свои сертификаты в CyberSafe, которые были созданы ранее. Для этого вам потребуется файл с расширением *.id, содержащий ваш открытый и закрытый ключи. После импорта вы сможете использовать сертификат для шифрования файлов для своего личного пользования, а также для создания цифровых подписей.

Вы также можете импортировать открытые ключи других пользователей на свою связку, если для вас доступен с файл расширением *.pid, содержащий открытый ключ пользователя (к примеру, он скопировал этот файл на ваш компьютер либо разместил в том месте, откуда вы можете его скачать). После импорта открытый ключ будет добавлен на вашу связку и вы с его помощью сможете шифровать файлы для отправки этому пользователю.

► Для импорта открытого ключа пользователя

Примечание. Перед импортом сертификата, содержащего закрытый ключ, убедитесь, что вы знаете пароль к этому сертификату.

- 1 Откройте CyberSafe и перейдите в меню **Ключи и Сертификаты** (Keys and Certificates).
- 2 В панели опций нажмете **Импорт** (Import).
- 3 В открывшемся системном окне укажите путь к файлу с расширением *.id или *.pid и нажмете **Открыть**.
- 4 Произойдет импорт ключа из файла, после чего импортированный ключ будет отображен на вашей связке. Проверить добавление ключа можно перейдя на вкладку **Все ключи** (All Keys)

Работа с серверами ключей

В своей работе вы можете использовать как сервер ключей CyberSafe, а также другие серверы открытых ключей, доступные в Интернет.

- **Сервер ключей CyberSafe.** Для удобства работы пользователей, CyberSafe предоставляет бесплатный открытый сервер ключей, предоставляющий возможность быстрого и удобного доступа к открытым ключам и сертификатам пользователей CyberSafe. В своей работе он использует новую технологию, позволяющую проверить каждый ключ пользователя на соответствие его e-mail адресу. Поэтому на сервере не хранятся не использующиеся ключи и ключи, которые закреплены за одним и тем же адресом электронной почты, а также отсутствуют другие проблемы, которые были характерны для серверов ключей старого поколения. Кроме того, сервер CyberSafe поддерживает функции по управлению вашими ключами, включая их замену, удаление и добавление дополнительных e-mail адресов к вашему ключу.

Используя сервер CyberSafe вы значительно повышаете свои шансы найти открытый ключ того пользователя, с которым намереваетесь обмениваться зашифрованными сообщениями.

- **Другие серверы ключей.** В большинстве случаев, другие серверы

ключей – это также открытые общедоступные серверы, хранящие открытые ключи пользователей. Тем не менее, у вас может быть доступ (к примеру, через компанию, в которой вы работаете или по каким либо другим причинам) и к закрытым серверам.

Для более подробной информации о работе с серверами ключей см. раздел *“Функции ключей”*.

6

Хранение ключей CyberSafe на токенах

Используйте программу CyberSafe для создания ключевой пары непосредственно на токене или для того, чтобы скопировать созданную ранее ключевую пару на токен. Оба варианта обеспечивают дополнительный уровень безопасности, суть которого заключается в том, что вы всегда можете держать свой закрытый ключ при себе, вместо того, чтобы оставлять его на вашем компьютере.

В том случае, если закрытый ключ хранится на токене, а не на компьютере пользователя, он менее уязвим, потому что после завершения работы с конфиденциальной информацией токен вместе с ключами можно забирать с собой.

В этой главе описывается, как использовать токены при работе с CyberSafe.

В этой главе

О токенах...	34
Использование флеш-накопителя в качестве токена.	35

О токенах

Токен – это компактное USB-устройство, которое может быть использовано для авторизации пользователя, защиты электронной переписки, безопасного доступа к удаленным информационным ресурсам, а также надежного хранения любой конфиденциальной информации, в частности – криптографических ключей. Иными словами токен – это подобие USB флеш-накопителя, имеющего защищенную память. Многие токены используют двухфакторную аутентификацию и дополнительно требуют введения PIN-кода со встроенной клавиатуры.

Для того, чтобы использовать CyberSafe совместно с токеном определенного производителя, вы должны иметь соответствующее программное обеспечение (драйверы), которое потребуется установить на ваш компьютер. Драйверы должны включать в себя библиотеку PKCS#11 (криптографический стандарт интерфейса токенов).

Компания КиберСофт настоятельно рекомендует вам устанавливать программное обеспечение, предоставляемое разработчиками вашего токена и не использовать драйверы третьих лиц.

Если вы храните свою ключевую пару на токене, для доступа к ней вам потребуется вводить PIN код для токена, а не пароль закрытого ключа. Существуют также токены, имеющие другие типы аутентификации (например, встроенную клавиатуру либо биометрические устройства).

Примечание. Основной особенностью токенов является то, что после сохранения на него ключа, он больше не может быть извлечен с устройства (не может быть экспортирован). Все действия по дешифрованию и созданию цифровых подписей осуществляются непосредственно на токене. Если же вы создавали свою ключевую пару на компьютере и затем копировали ее на токен, тогда вы по-прежнему можете экспортировать ключи с компьютера.

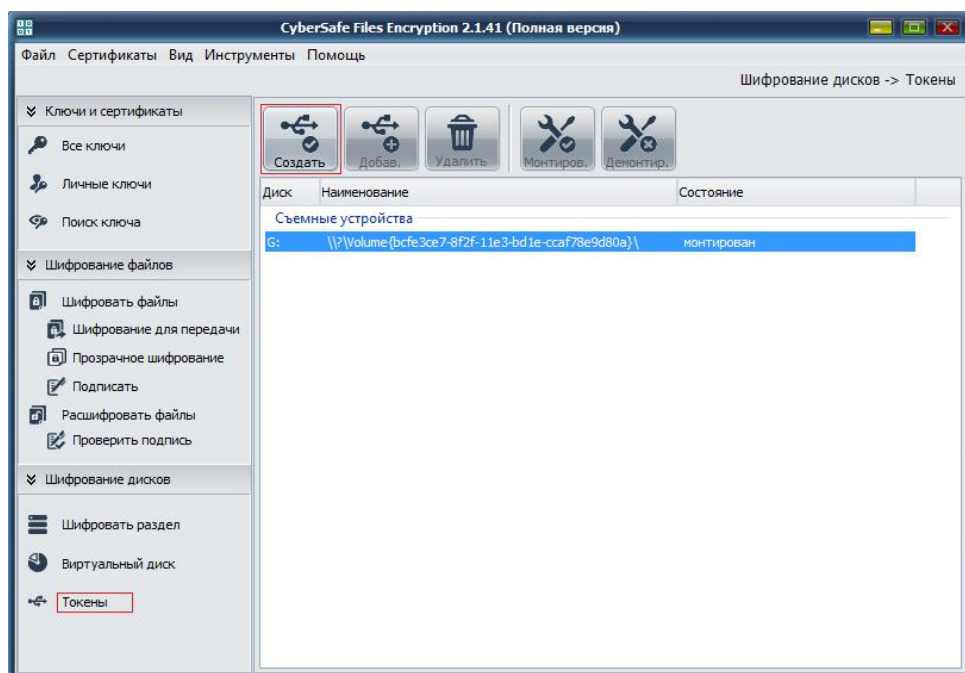
Токены – достаточно дорогостоящие устройства, которые чаще всего можно приобрести только напрямую у производителя. Кроме того, не все токены могут быть совместимы с программами для шифрования, в том числе и с

Использование флеш-накопителя в качестве токена

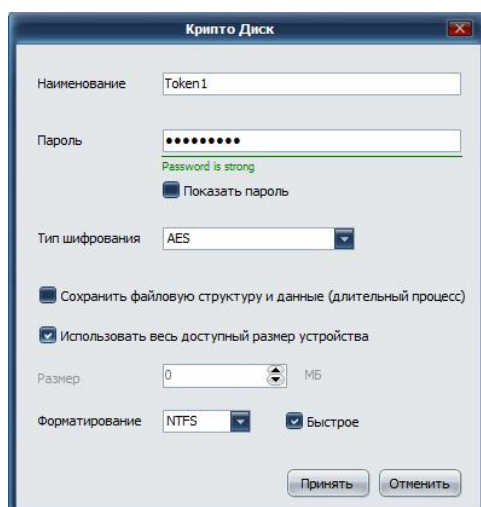
Исходя из вышесказанного, в CyberSafe существует возможность создать токен из обычного USB флеш-накопителя. Это также позволяет организовать двухфакторную аутентификацию, поскольку для работы с зашифрованными файлами требуется не только знание пароля к закрытому ключу, но и физическое присутствие флеш-накопителя вместе с ключом в компьютере.

► **Для использования USB флеш-накопителя в качестве токена:**

- 1 Подключите флеш-накопитель к своему компьютеру. Откройте CyberSafe и перейдите на вкладку **Шифрование дисков – Токены**. В рабочей области в списке Съемные устройства выделите нужный флеш-накопитель и нажмите **Создать**:

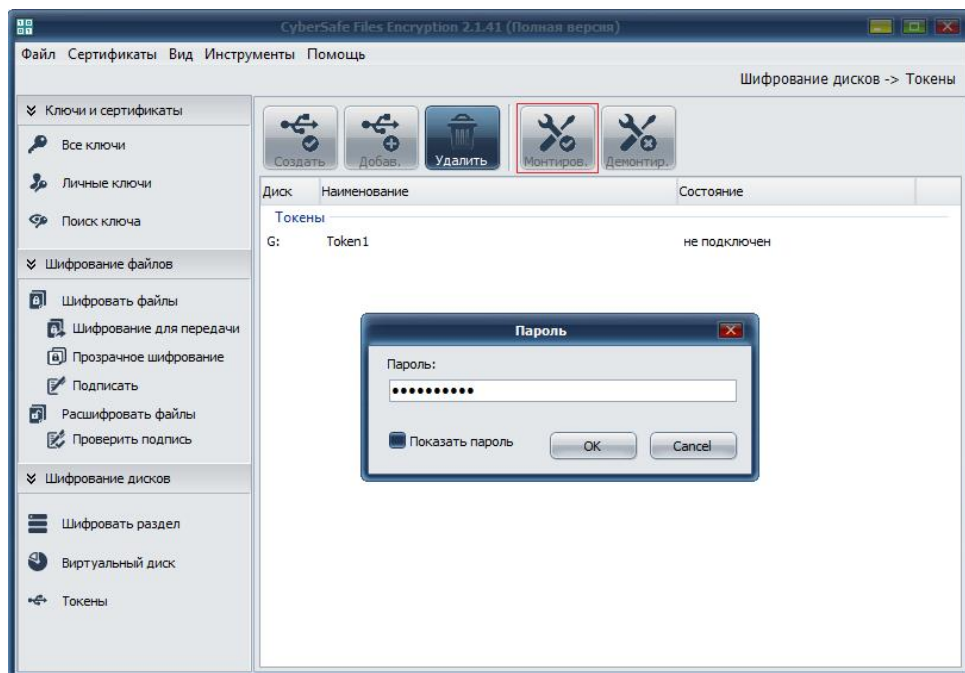


- 2 В открывшемся окне задайте *Наименование* устройства и пароль к нему, выберите алгоритм шифрования и файловую систему. Нажмите **Принять**:



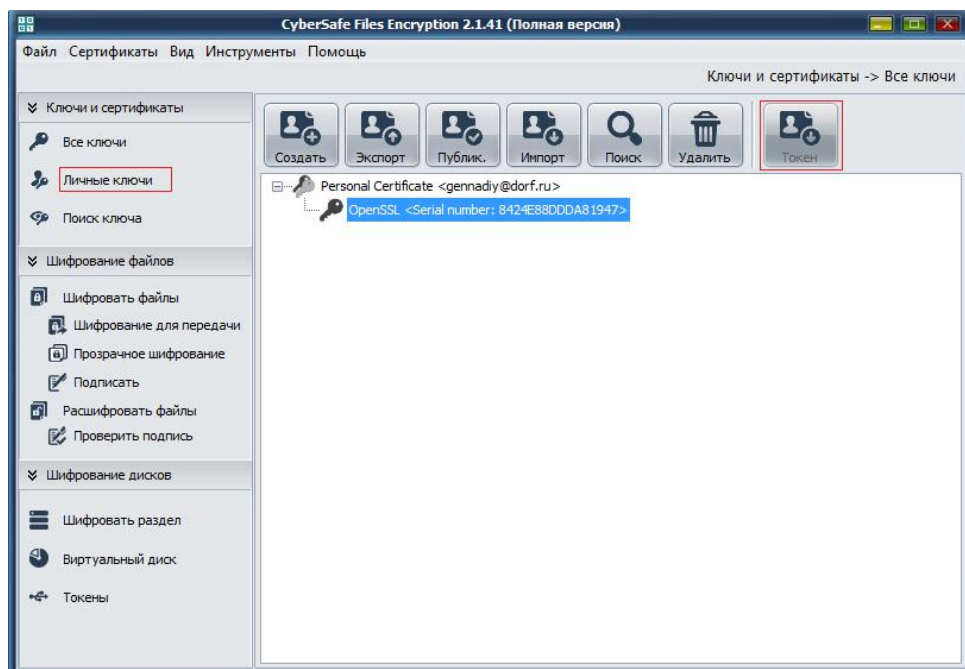
USB флеш-накопитель будет преобразован в токен и отобразится в рабочей области в списке Токены.

- 3 Для того, чтобы токен можно было использовать, его необходимо смонтировать. Для этого выделите токен в *Рабочей области*, нажмите **Монтиров.** в *Панели опций* и в открывшемся окне введите пароль к этому токену:



Токен подключен и готов к работе.

- 4 Для того, чтобы скопировать на токен свой сертификат (ключевую пару), перейдите на вкладку **Ключи и Сертификаты – Личные ключи**, выделите ключ, который хотите хранить на токене и в *Панели опций* нажимаем **Токен**:



Произойдет копирование сертификата на устройство.

После этого все действия по шифрованию и дешифрованию информации с использованием скопированных на токен ключей возможны лишь при подключении токена к компьютеру.

Для операционной системы подключенный в CyberSafe токен виден как

неотформатированное устройство, поэтому в случае подключения к компьютеру пользователя злоумышленника (например, по сети), похитить ключи с токена для него будет невозможно.

После завершения работы с токеном его необходимо демонтировать.

Для того, чтобы стереть ключи с токена, флеш-накопитель нужно отформатировать в Windows. При этом, все хранящиеся на устройстве ключи будут уничтожены, поэтому если у вас имеется зашифрованная с их помощью информация, необходимо убедиться, что у вас есть дополнительная копия этих ключей.

В этом разделе рассказывается о том, как использовать CyberSafe для защиты e-mail сообщений при работе с почтовыми клиентами.

В этой главе

Шифрование почты при помощи CyberSafe	39
Работа с Microsoft Outlook	40
Работа с Mozilla Thunderbird	47
Работа с The Bat!	51

Шифрование почты при помощи CyberSafe

С целью защиты электронной почты используется шифрование. CyberSafe предоставляет возможность защитить вашу электронную корреспонденцию при использовании любого почтового клиента (Thunderbird, Microsoft Outlook, The Bat!, Endora и др.).

Перед тем как вы начнете процесс обмена шифрованными сообщениями с другими пользователями, вам необходимо обменяться с ними сертификатами открытого ключа. Это можно сделать, отправив друг другу заверенные цифровой подписью сообщения, а после этого добавить сертификат пользователя в список своих контактов.

После того, как у вас и у других пользователей имеются сертификаты друг друга, процесс обмена шифрованными сообщениями происходит по аналогии с процессом обмена обычными e-mail сообщениями. При этом также шифруются все прикрепленные в сообщениях файлы.

Экспорт сертификата в формате PFX

Работа с почтовыми клиентами требует наличия сертификатов в формате PKSC#12 и X.509. Для некоторых почтовых клиентов необходимо, чтобы файлы сертификатов были размещены в хранилище Windows, другие импортируют их в свои собственные хранилища.

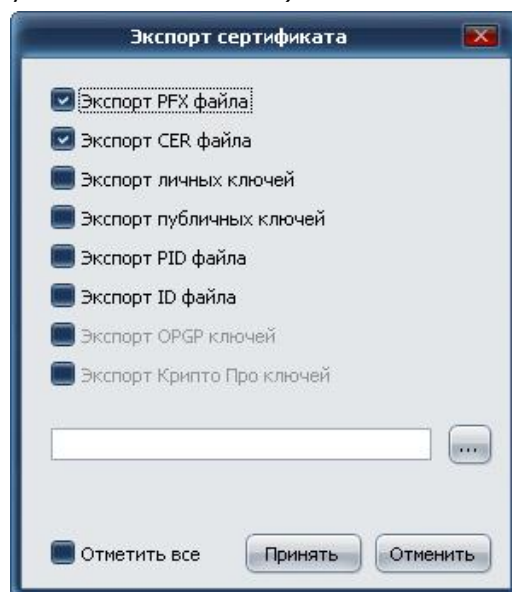
X.509 (файл с расширением *.cer) – формат сертификата, который помимо общей информации (версия, серийный номер, алгоритм подписи, сведения об издателе, срок действия, сведения о владельце, цифровой отпечаток) содержит ваш открытый ключ. Его мы отправляем другим пользователям, с которыми хотим обмениваться зашифрованными сообщениями.

PKCS #12 (файл с расширением *.pfx) – единственный формат сертификата, который помимо общей информации может содержать не только открытый, но и закрытый ключ. С его помощью мы будем расшифровывать сообщения, зашифрованные при помощи нашего открытого ключа, а также ставить свою цифровую подпись.

► Для экспорта сертификатов

- 1 Откройте CyberSafe, и в меню **Ключи и Сертификаты** (Keys and Certificates) выберите пункт **Все ключи** (All Keys). После этого появятся все ключи, имеющиеся на вашей связке.
- 2 Выделите необходимый сертификат ключа из списка, единожды кликнув на нем мышью, и в Панели опций нажмите **Экспорт** (Export).
- 3 В открывшемся окне введите свой пароль для данного сертификата и нажмите **ОК**.
- 4 В открывшемся диалоговом окне CyberSafe установите галочку в чекбоксе

Экспорт PFX файла и Экспорт CER файла (если они не были установлены до этого):



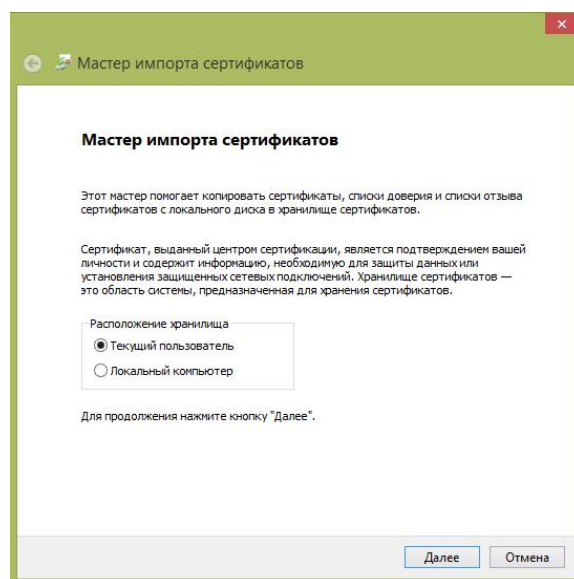
- 5 Укажите место, куда должны быть экспортированы сертификаты. Нажмите **Принять**.
- 6 Сертификаты экспортированы в указанное место.

Работа с Microsoft Outlook

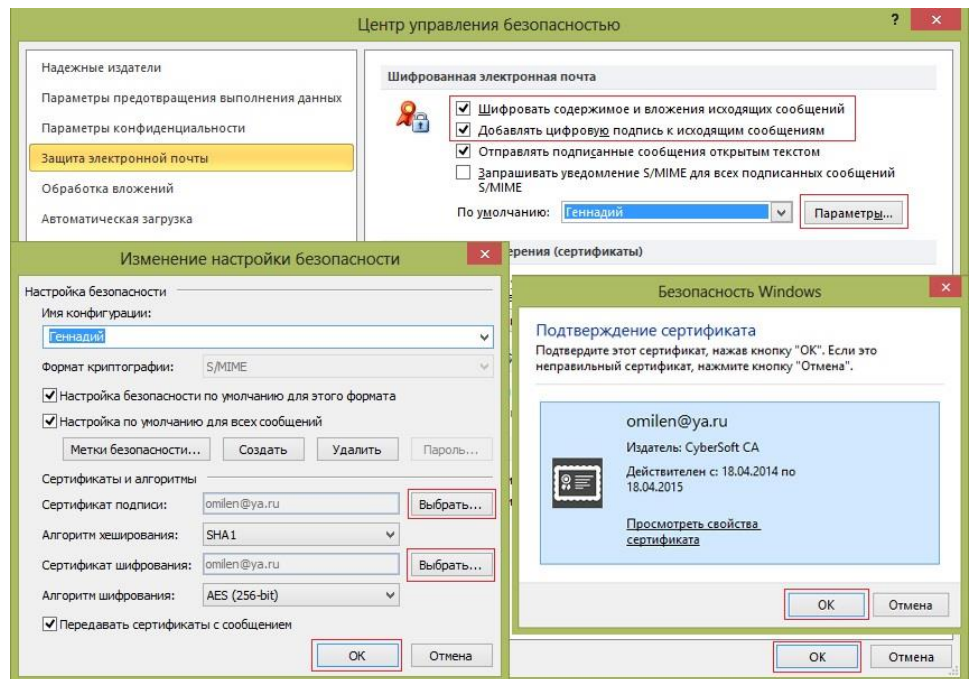
Используя сертификат в формате PFX, вы можете настроить функции шифрования и цифровой подписи в почтовом клиенте Outlook.

► Для настройки функции шифрования

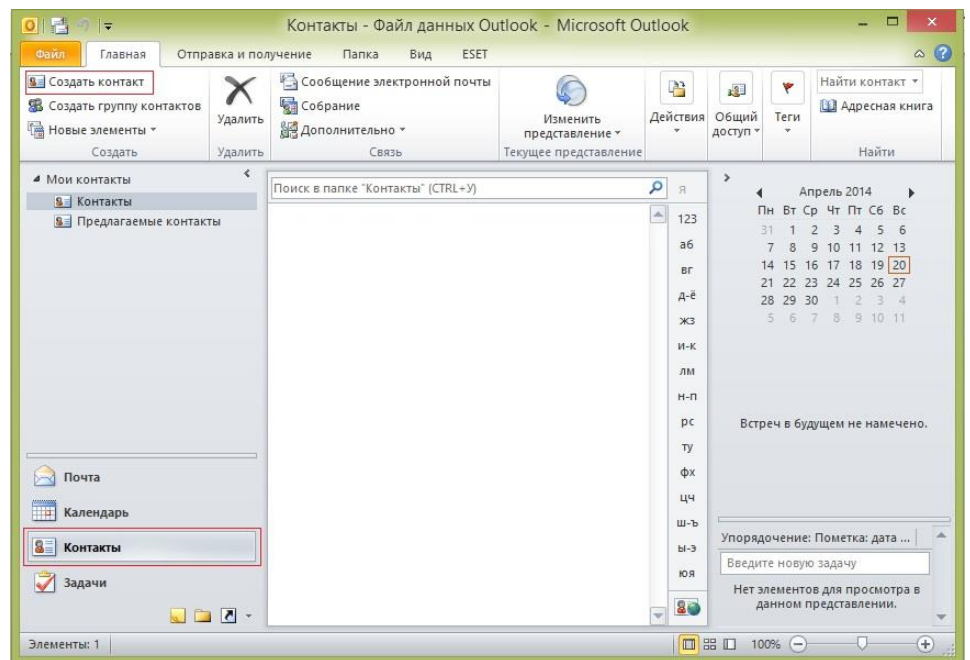
- 1 Установите экспортированный сертификат в формате PKCS#12 в хранилище Windows. Для этого дважды кликните на pfx-файле и следуйте инструкциям Мастера импорта сертификатов. Так как этот сертификат содержит ваш закрытый ключ, в процессе импорта потребуется ввести пароль, который был указан при его создании.



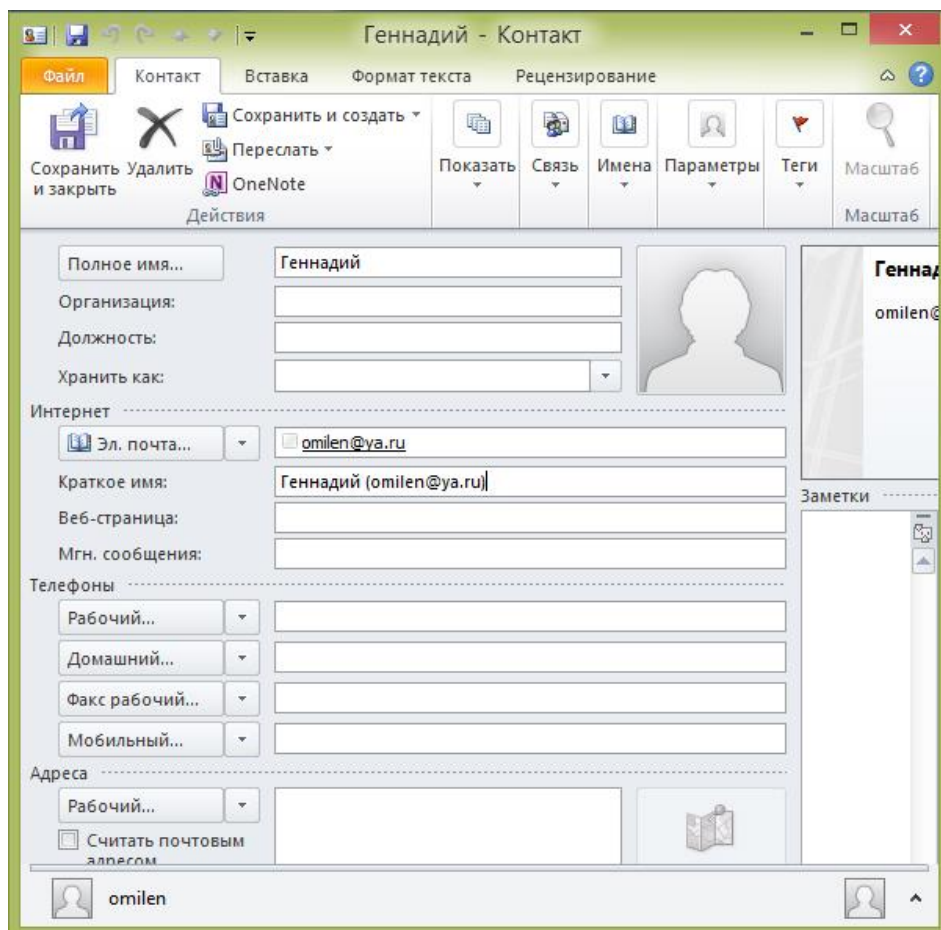
- 2 Откройте Microsoft Outlook и выберите нужный сертификат.
Для этого перейдите: **Файл > Параметры > Центр управления безопасностью > Параметры центра управления безопасностью > Защита электронной почты > Параметры > Выбрать...**



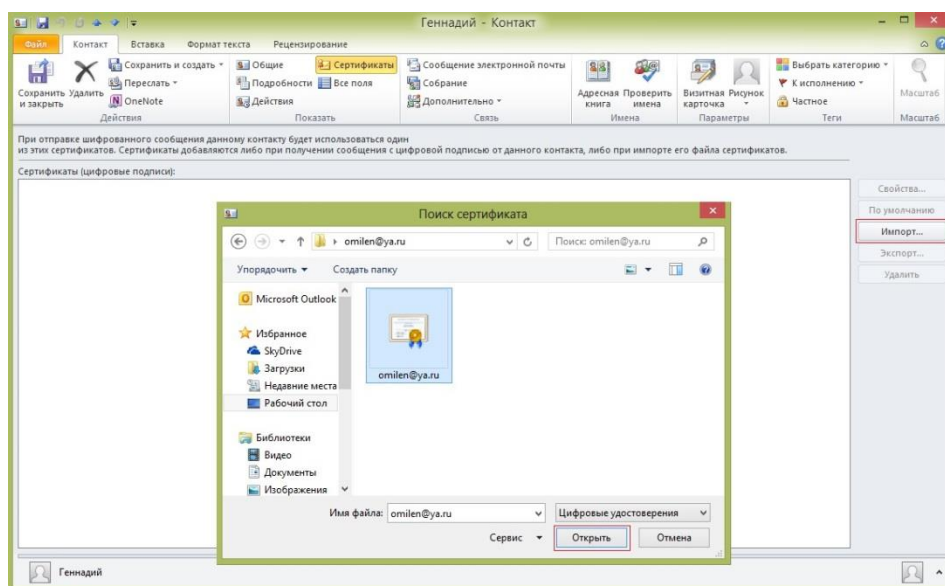
- 3 В разделе *Шифрованная электронная почта* отметьте галочками пункты **Шифровать содержимое и вложения исходящих сообщений** и **Добавлять цифровую подпись к исходящим сообщениям**.
- 4 Далее необходимо проверить функцию шифрования на себе. Для этого:
 - Создайте новый контакт. Перейдите **Главная > Контакты > Создать контакт**.



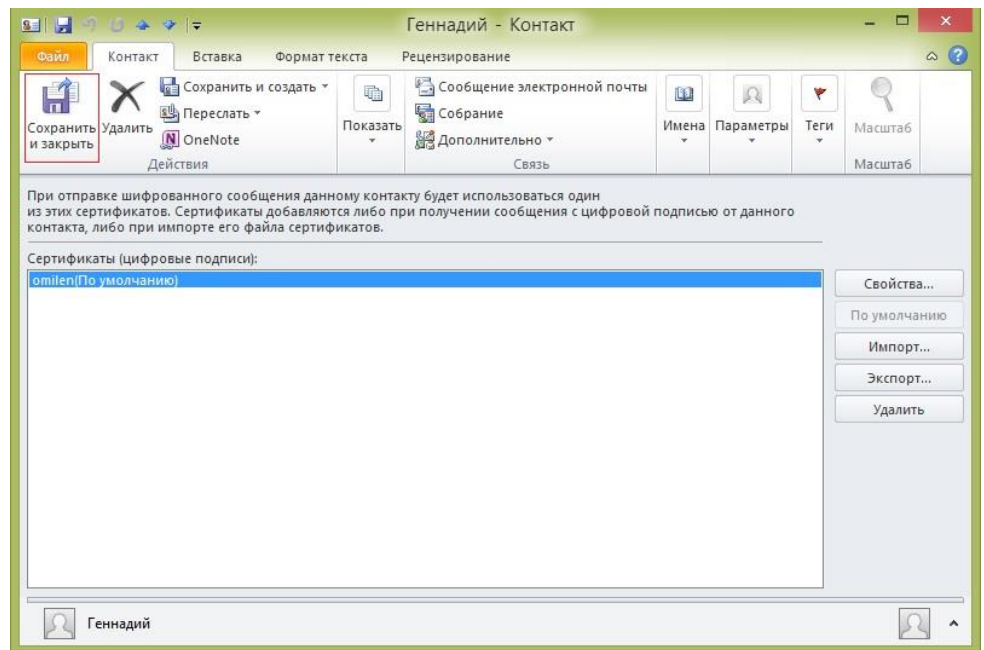
- После этого откроется окно создания нового контакта. Заполните необходимые поля, указав при этом свой e-mail в поле **Эл. почта**.



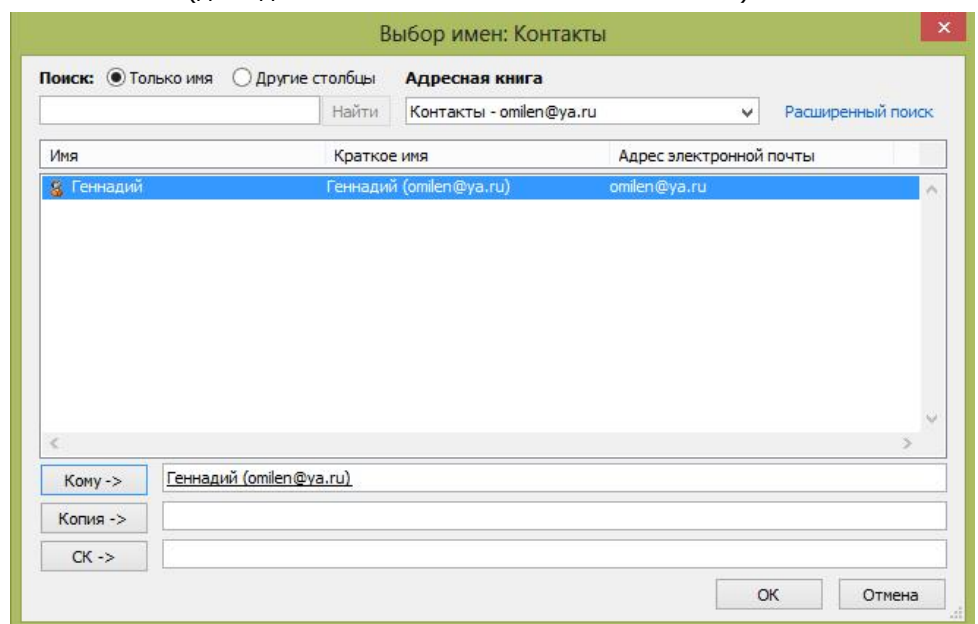
- Далее необходимо импортировать сертификат для данного контакта (в данном случае - ваш). Для этого на вкладке **Контакт** выберите **Сертификаты** и нажмите **Импорт**. В открывшемся окне **Поиск сертификата** выберите файл с расширением *.cer и нажмите **Открыть**. (Файл сертификата с этим расширением может быть экспортирован из CyberSafe по аналогии с экспортом файла сертификата с расширением *. pfx (см. параграф "Экспорт сертификата в формате PFX").



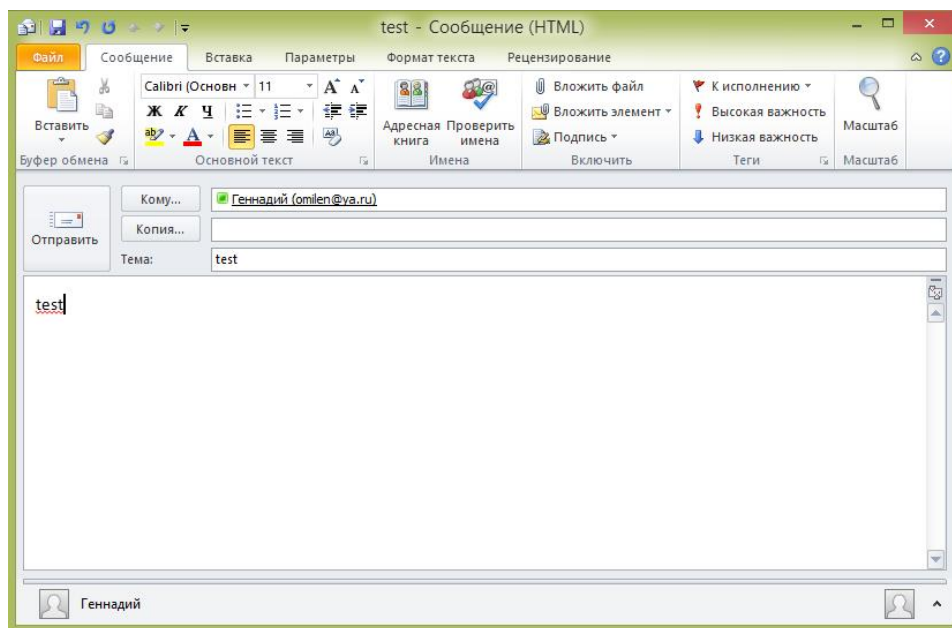
В открывшемся диалоговом окне, запрашивающем подтверждение на добавление выбранного сертификата к контакту нажмите **Да**. После этого в поле *Сертификаты (цифровые подписи)* появится добавленный сертификат. Нажмите **Сохранить и закрыть**.



- Сертификат добавлен к контакту.
- Отправьте самому себе зашифрованное сообщение. Для этого перейдите **Главная > Почта > Создать сообщение**. В поле *Кому* укажите созданный вами контакт, выбрав его из *Адресной книги* (дважды кликните мышью на этом контакте) и нажмите **ОК**:

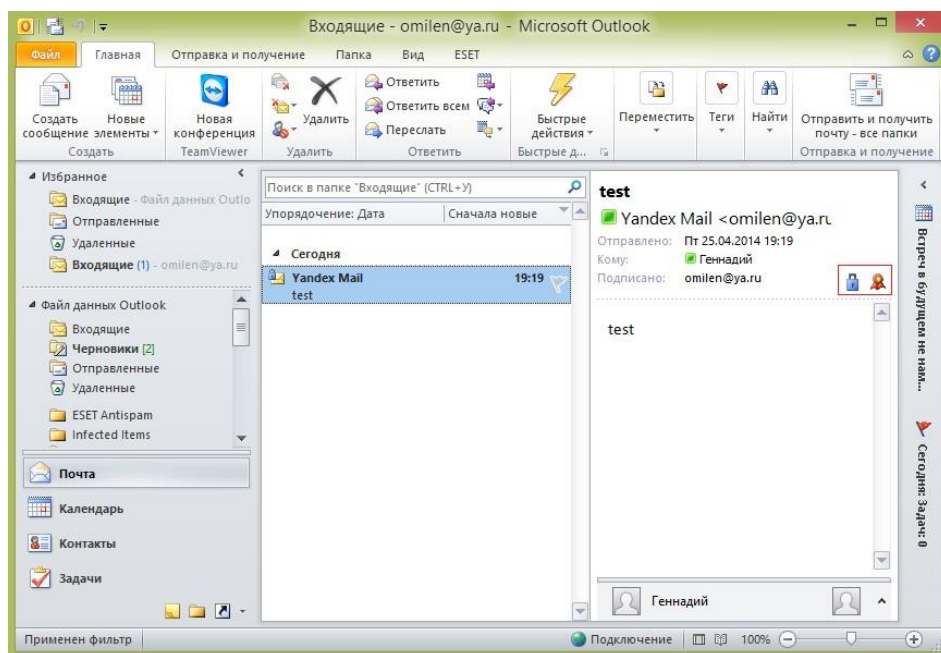


- Заполните поле *Тема*:, введите текст сообщения и нажмите **Отправить**:

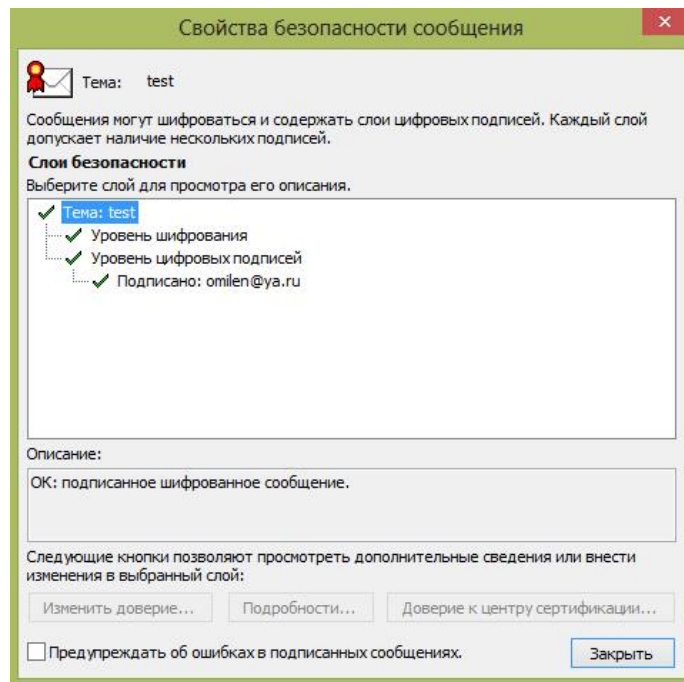


- Перейдите **Главная > Входящие**. В списке входящих сообщений появится отправленное вами сообщение. Оно зашифровано, о чем свидетельствует иконка с синим замочком в верхнем левом углу. Кликните на нем мышью, чтобы автоматически расшифровать и открыть в соседнем окне.

Если вы не видите отправленное письмо во входящих, перейдите на вкладку **Отправка и получение** и нажмите **Обновить папку**.

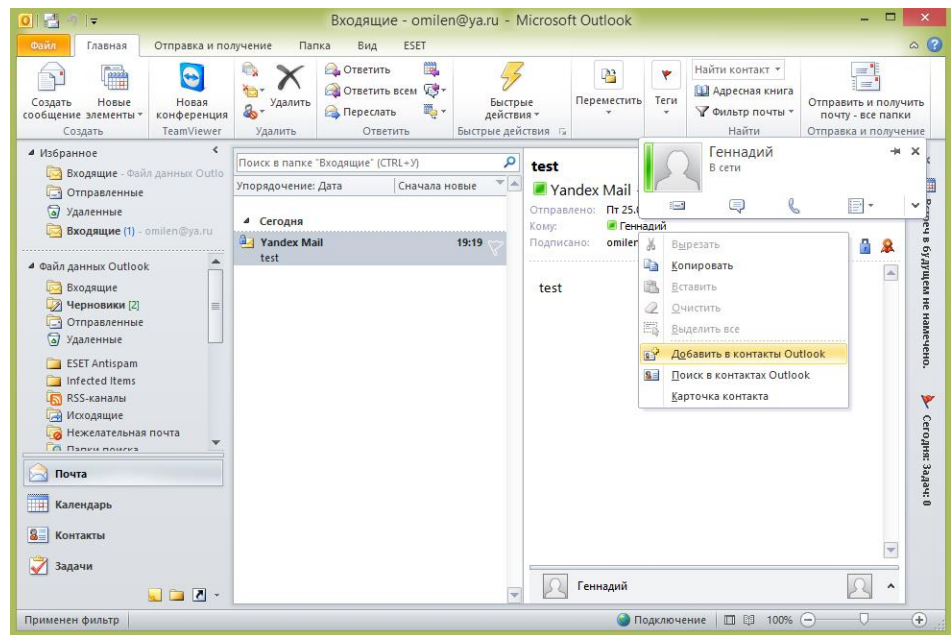


- Для того, чтобы просмотреть свойства безопасности сообщения или информацию о цифровой подписи, нажмите на соответствующих иконках в поле с общей информацией о сообщении. Если сертификат пользователя достоверный, а цифровая подпись подлинна, при просмотре свойств безопасности сообщения вы увидите зеленые галочки:



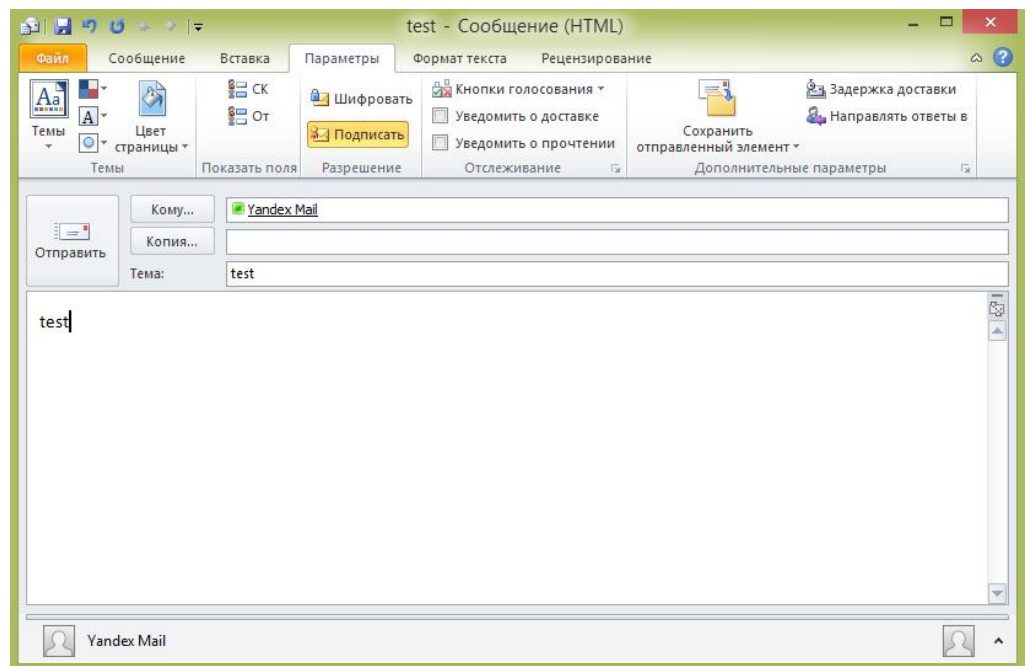
- Проверка функции шифрования на себе выполнена.
- 5 По аналогии отправляем свой сертификат, заверенный цифровой подписью другим пользователям и получаем их подписанные сертификаты.
 - 6 Получив от другого пользователя подписанное письмо, добавляем этого пользователя в *Контакты* (Адресную книгу). Для этого правой кнопкой мыши нажимаем на адресе отправителя и в контекстном меню выбираем **Добавить в контакты Outlook**.

Письмо, подписанное цифровой подписью отправителя, содержит его сертификат в формате X.509 и открытый ключ, который в дальнейшем Outlook будет использовать для шифрования сообщений этому пользователю.



Примечание. До тех пор, пока у вас не будет открытого ключа пользователя, которому вы отправляете зашифрованное сообщение, вы не сможете его зашифровать и Outlook будет выдавать ошибку. Поэтому прежде нужно отправить ему незашифрованное письмо, но подписанное вашей цифровой подписью (такое письмо будет содержать ваш открытый ключ).

Для того, чтобы отключить функцию шифрования, оставив включенной функцию цифровой подписи перейдите на вкладку **Параметры** и отключите опцию **Шифровать**, оставив включенной **Подписать**.



Функция шифрования настроена.

Microsoft Outlook выполняет проверку сертификата по следующему сценарию. В том случае, если издатель сертификата числится в списке доверенных, то сертификат считается доверенным. В данном случае CyberSafe Certificate Authority автоматически добавляется в доверенные во время первого запуска программы.

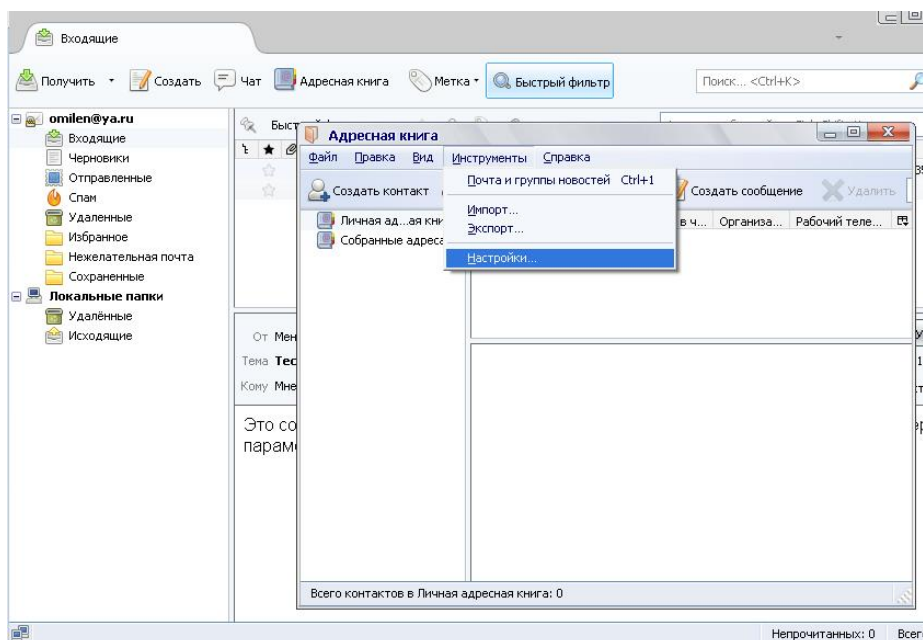
Примечание. Программа CyberSafe позволяет создавать лишь один сертификат на определенный адрес электронной почты. Это означает, что если пользователь самостоятельно не добавил какой-либо недостоверный сертификат, все сообщения, получаемые им с зеленой галочкой напротив пункта *Уровень цифровых подписей*, могут считаться надежными.

Работа с Mozilla Thunderbird

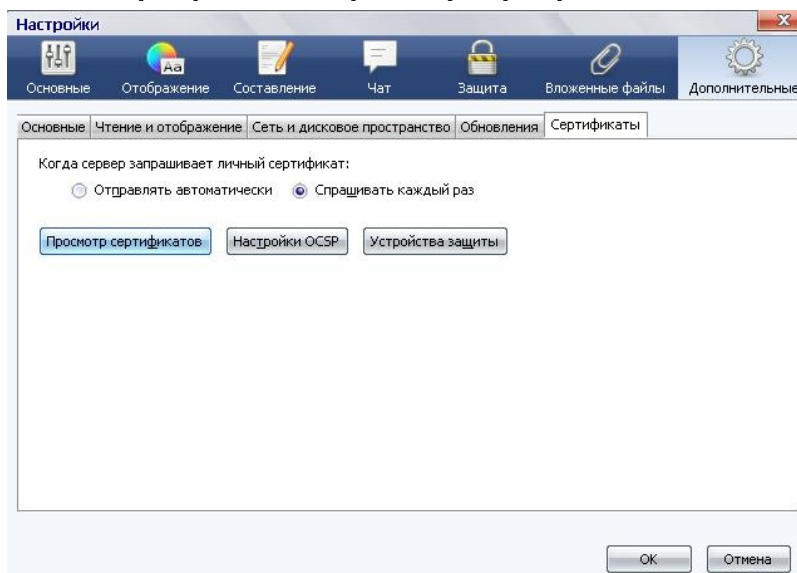
Thunderbird – популярный почтовый клиент от компании Mozilla, отличающийся простотой и удобством при обмене электронными сообщениями.

► Для настройки функции шифрования

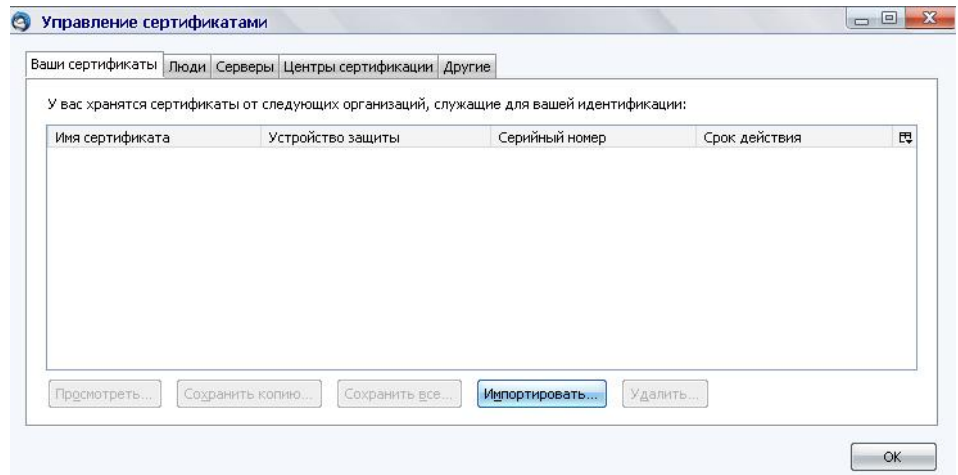
- 1 Прежде всего, необходимо установить свой сертификат в программу. Для этого:
 - Откройте Thunderbird, перейдите на вкладку **Адресная книга**. В открывшемся окне выберите **Инструменты > Настройки**:



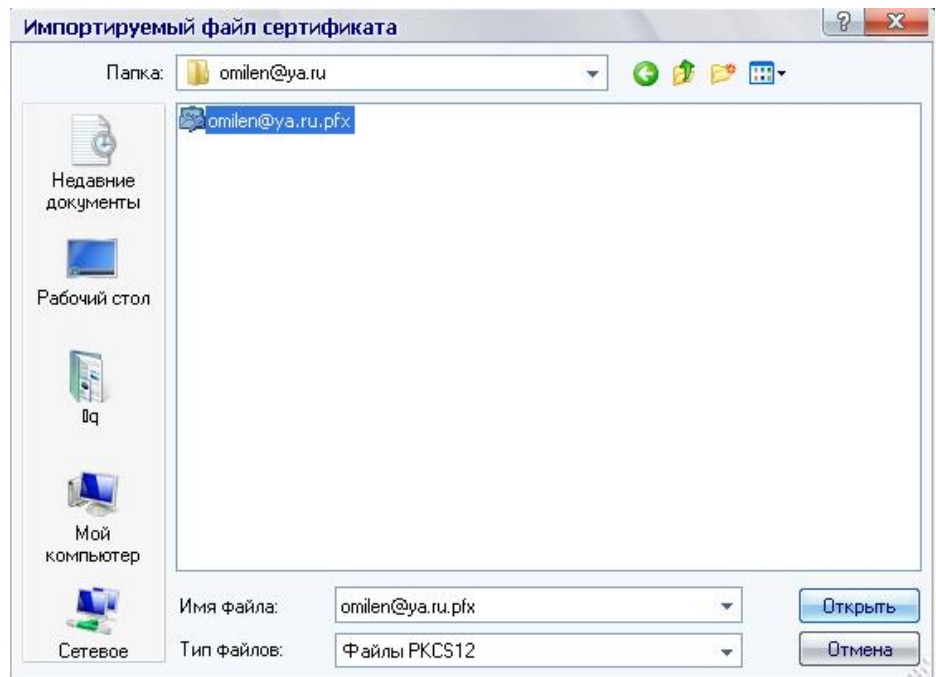
- В открывшемся окне *Настройки* выберите **Дополнительные > Сертификаты > Просмотр сертификатов**:



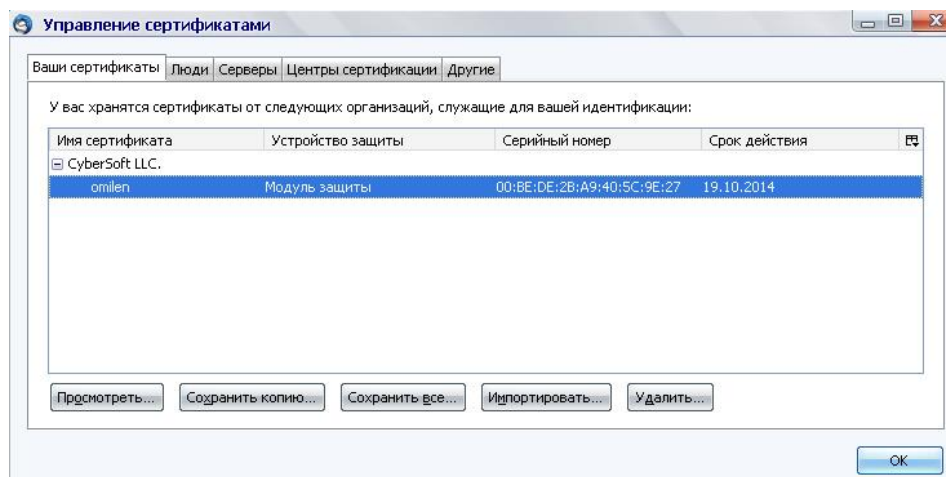
- Откроется окно *Управление сертификатами*. Выберите **Ваши сертификаты > Импортировать**.



- В открывшемся окне укажите путь к файлу сертификата с расширением *. pfx, выделите его и нажмите **Открыть** (об экспорте этого файла см. в параграфе "Экспорт сертификата в формате PFX").



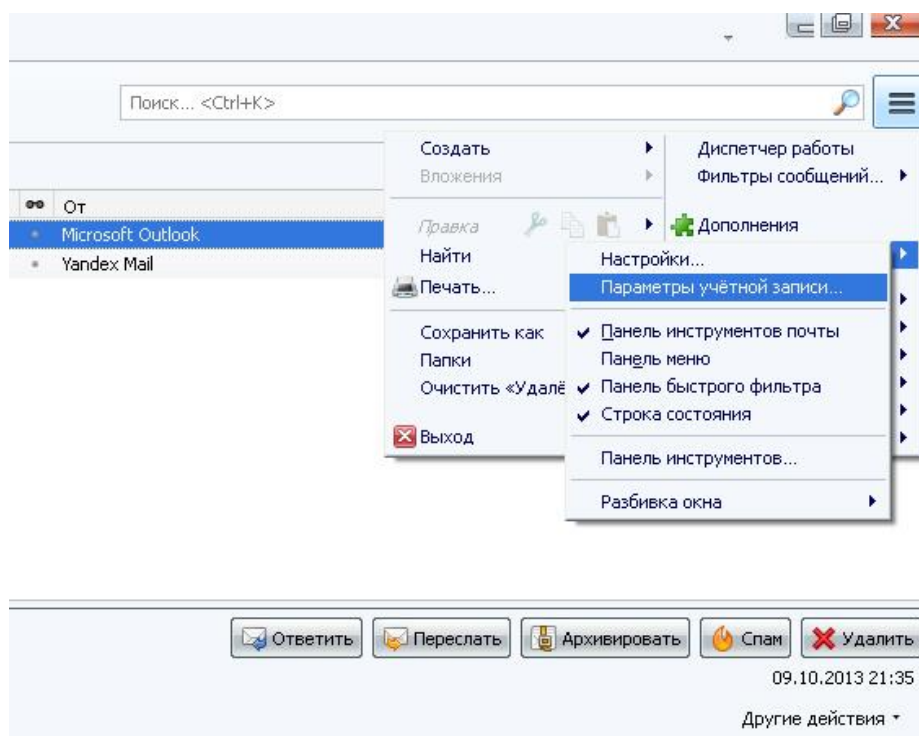
- Откроется диалоговое окно ввода пароля. Введите пароль для данного сертификата и нажмите **ОК**. После этого программа выдаст уведомление об успешном восстановлении сертификата и закрытого ключа, после чего ваш сертификат будет отображен в списке сертификатов.



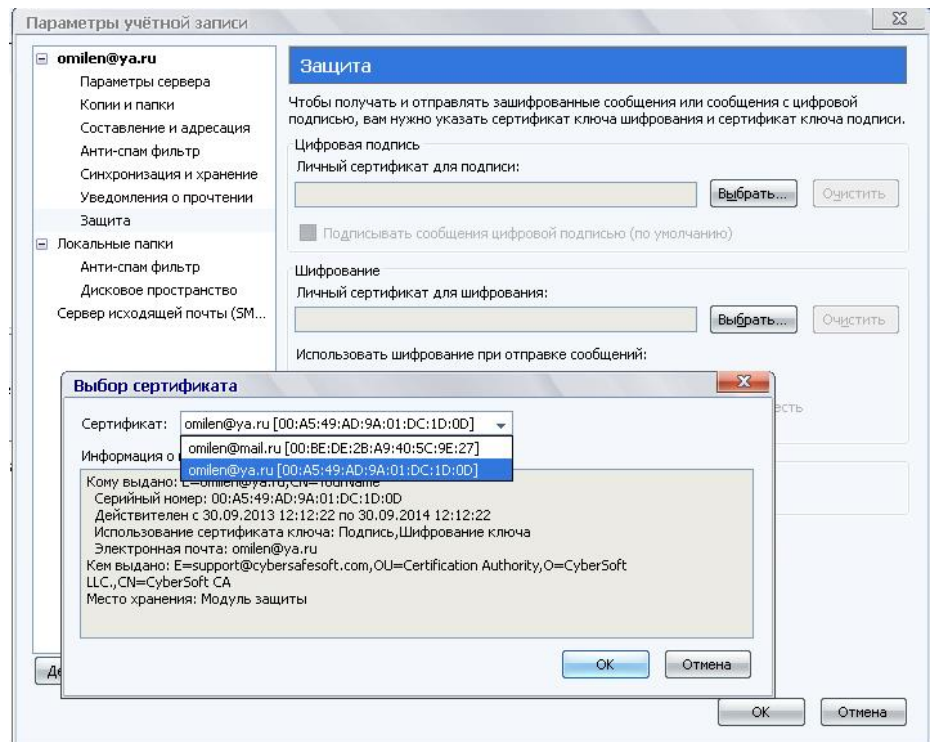
Установка сертификата выполнена.

2 Для настройки программы выполните следующие действия:

- Откройте основное меню программы, выберите **Настройки > Параметры учетной записи**.

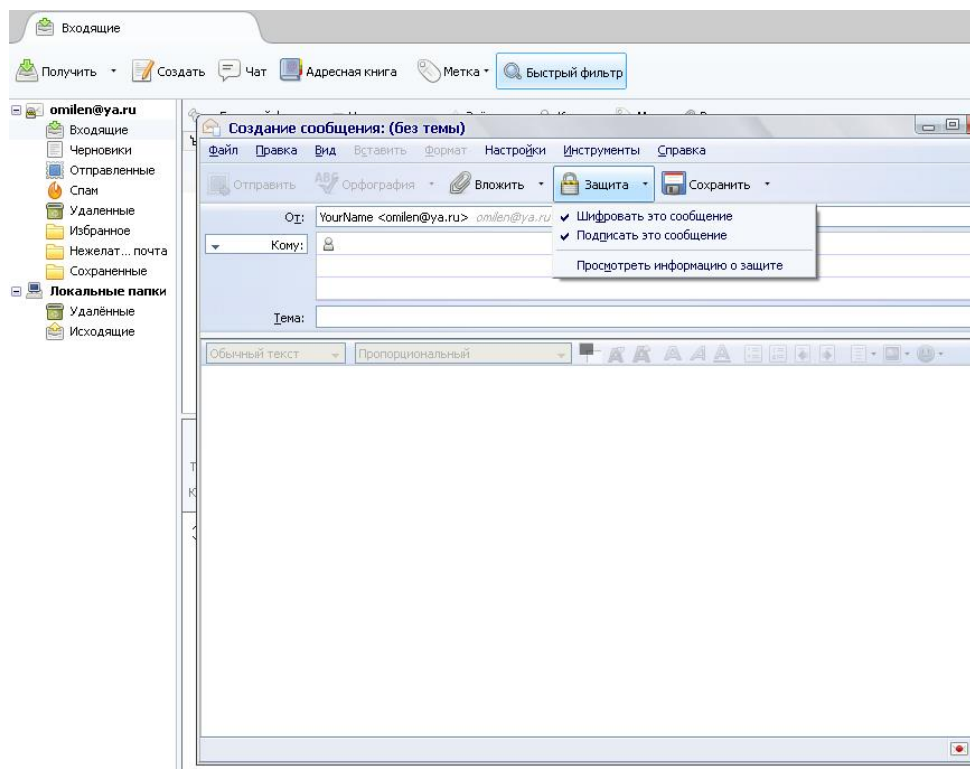


- В открывшемся окне *Параметры учетной записи* выберите пункт **Защита** и укажите личные сертификаты для цифровой подписи и шифрования, нажав кнопки **Выбрать...**. Программа предложит выбрать один из установленных ранее сертификатов. Выберите нужный из выпадающего списка и нажмите **ОК**.



- В открывшемся диалоговом окне, запрашивающем подтверждение на использование одного и того же сертификата для шифрования и расшифровки сообщений, нажмите **Да**.
Для сохранения настроек в окне *Параметры учетной записи* нажмите **ОК**.
Настройка завершена.

- Для отправки зашифрованного сообщения другому пользователю выберите **Создать**. Откроется окно создания сообщения. На вкладке **Защита** отметьте галочками **Шифровать это сообщение** и **Подписать это сообщение**.



Обратите внимание, что если у вас еще нет открытого ключа

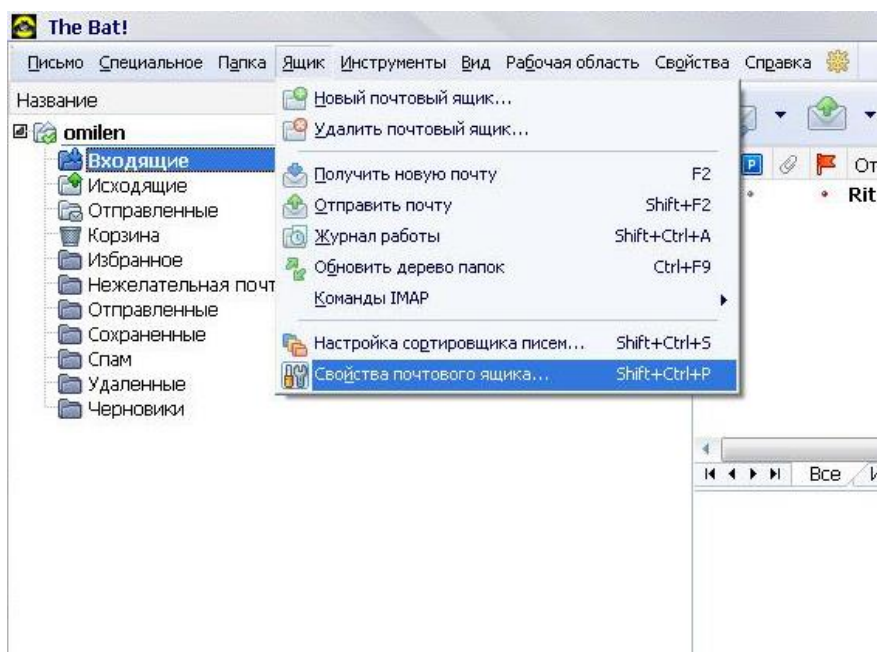
пользователя, которому вы отправляете зашифрованное сообщение, вы не сможете его зашифровать. Поэтому прежде нужно отправить ему незашифрованное письмо, подписанное вашей цифровой подписью (такое письмо будет также содержать ваш открытый ключ) и получить открытый ключ вашего корреспондента.

Пользователь добавит вас в свой список контактов и аналогично отправит вам свой открытый ключ. После добавления его в свою Адресную книгу вы сможете обмениваться с ним зашифрованными сообщениями.

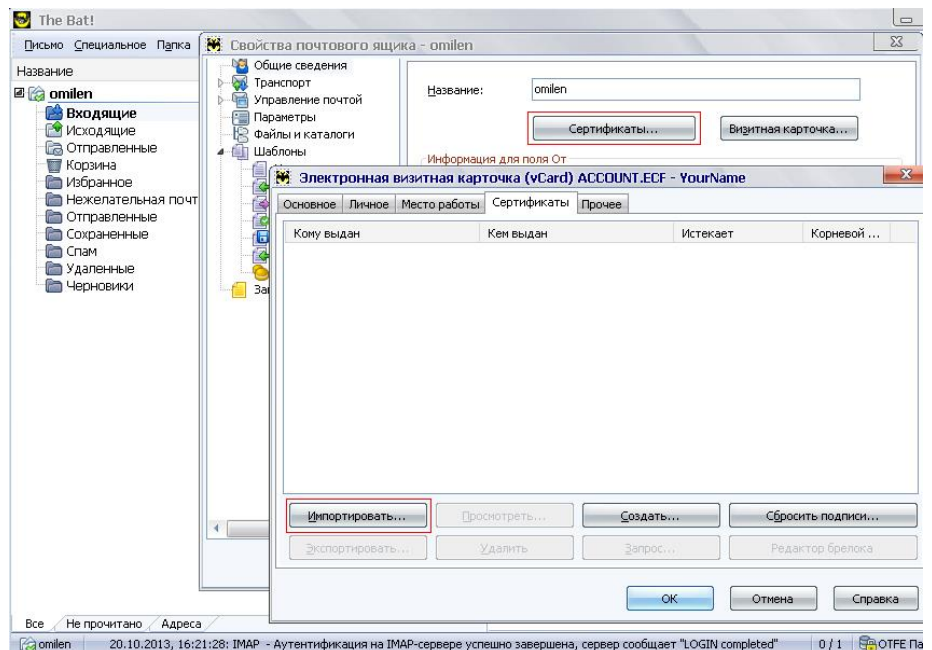
Работа с The Bat!

► Для настройки функции шифрования

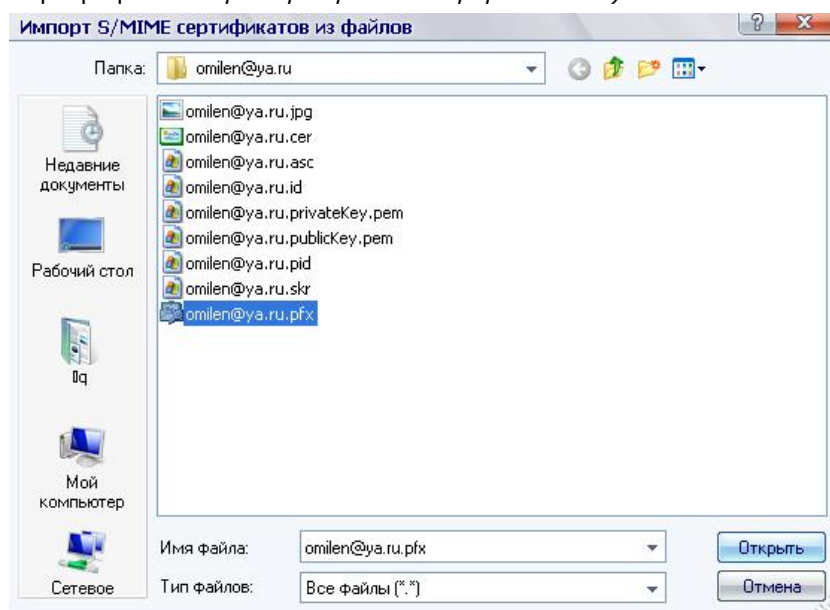
- 1 Откройте The Bat! и перейдите **Ящик > Свойства почтового ящика**.



- 2 В открывшемся окне Свойства почтового ящика выберите **Сертификаты > Импортировать**.

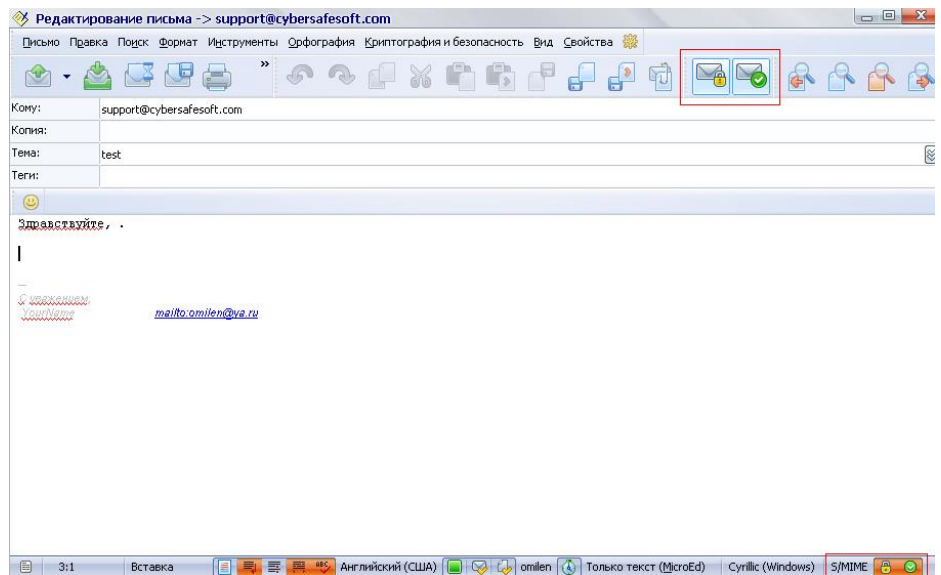


- 3 В открывшемся окне укажите путь к файлу сертификата с расширением *. pfx, выделите его и нажмите **Открыть** (об экспорте этого файла см. в параграфе *Экспорт сертификата в формате PFX*).



Откроется диалоговое окно ввода пароля. Введите свой пароль для импортируемого сертификата и нажмите **ОК**.

- 4 Сертификат импортирован, однако он считается не доверенным. Дважды кликните на сертификате, перейдите на вкладку **Путь сертификации**, выделите нужный сертификат и нажмите **Добавить к доверенным**.
- 5 Создайте новое сообщение, для этого перейдите **Письмо > Создать**. Заполните поля *Кому*, *Тема*, вводим текст сообщения. Для того, чтобы зашифровать и подписать это сообщение, включите соответствующие кнопки с иконками замочка и зеленой галочки на конвертах. После этого в правом нижнем углу становятся активными выбранные функции S/MIME. Отправьте письмо.



Обратите внимание, что если у вас еще нет открытого ключа пользователя, которому вы отправляете зашифрованное сообщение, вы не сможете его зашифровать. Поэтому прежде нужно отправить ему незашифрованное письмо, подписанное вашей цифровой подписью (такое письмо будет также содержать ваш открытый ключ) и получить открытый ключ вашего корреспондента.

Пользователь добавит вас в свой список контактов и аналогично отправит вам свой открытый ключ. Добавив его в список контактов, вы сможете обмениваться с ним зашифрованными сообщениями.

8

Шифрование файлов при помощи CyberSafe

CyberSafe предоставляет возможность шифровать ваши файлы и папки, а также создавать самораспаковывающиеся зашифрованный zip-архивы, что является очень удобным как в процессе собственного использования, так и при обмене информацией с другими пользователями.

В этой главе

О шифровании файлов программой CyberSafe	52
Шифрование файлов и папок	52
Создание зашифрованных zip-архивов	65
Дополнительные настройки шифрования	66

О шифровании файлов программой CyberSafe

Шифрование файлов и папок применяется для их защиты от постороннего доступа. Используйте CyberSafe для того, чтобы создавать, открывать и редактировать зашифрованные файлы, папки и zip-архивы.

Вам может потребоваться зашифровать файл или папку для двух целей: для безопасного хранения на собственном компьютере, либо для отправки другому пользователю.

Если вы выбираете шифрование файла для личного пользования, файл будет зашифрован при помощи симметричного ключа, такого же, который используется в случае шифрования диска или его раздела.

Шифрование отдельных файлов имеет свое преимущество перед шифрованием всего диска или созданием виртуальных дисков. Например, если у вас есть зашифрованный виртуальный диск, на котором храниться 100 файлов, когда вам требуется получить доступ к одному из этих файлов, диск расшифровывается и становится незащищенным, а вместе с ним и становятся незащищенными и остальные 99 файлов. Но если вы зашифруете конкретные файлы по отдельности, работа с одним из них не скажется на безопасности и всех остальных – эти файлы по-прежнему будут незатронутыми, зашифрованными и полностью защищенными.

Если вы захотите зашифровать файлы для отправки их другим пользователям, они будут зашифрованы при помощи открытых ключей этих пользователей. Для этого сертификаты данных пользователей должны находиться в локальной базе данных сертификатов вашего компьютера. В том случае, если у вас нет сертификата какого-то пользователя, вы можете попробовать найти его на глобальном сервере CyberSafe по его адресу электронной почты, воспользовавшись функцией поиска.

Шифрование файлов и папок

Используя CyberSafe, вы можете зашифровать необходимые файлы и папки тремя способами: на основе сертификатов (ключей), использовать шифрование паролем, либо создать самораспаковывающийся зашифрованный zip-архив.

Шифрование файлов на основе сертификатов (ключей)

Используйте шифрование файлов на основе сертификатов (ключей) для:

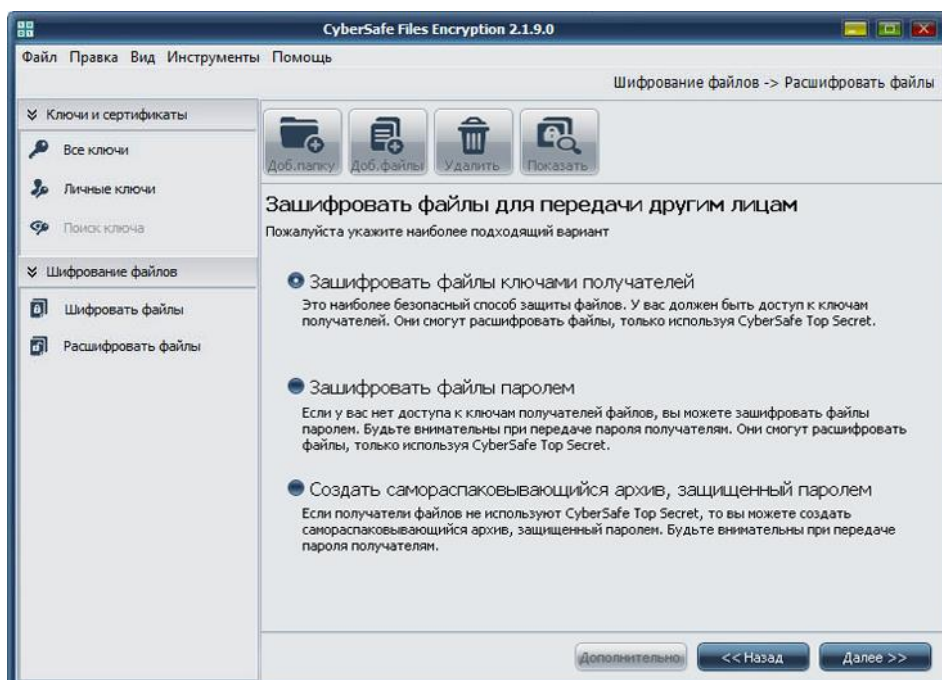
- Обеспечения наивысшей степени защиты файлов.
- Шифрования файлов для личного пользования, а также для обмена файлами с пользователями, у которых на компьютере установлен CyberSafe и открытые ключи которых имеются на вашей связке.
- Когда вы не хотите сообщать получателю пароль к отправляемому файлу.

Если вы отправляете файл другим пользователям, шифрование на основе открытых ключей – лучшее решение, которое должно выбираться в первую очередь, если вам необходима наивысшая степень безопасности и у вас есть все необходимое для этого.

Как только необходимые файлы зашифрованы, вы можете отправить их другим пользователям. После получения файлов пользователь дешифрует их при помощи CyberSafe и своего закрытого ключа. Файлы смогут расшифровать все пользователи, чьи открытые ключи вы использовали при шифровании. В итоге, каждый из пользователей получит одинаковые файлы.

► Для шифрования файлов на основе сертификатов (ключей)

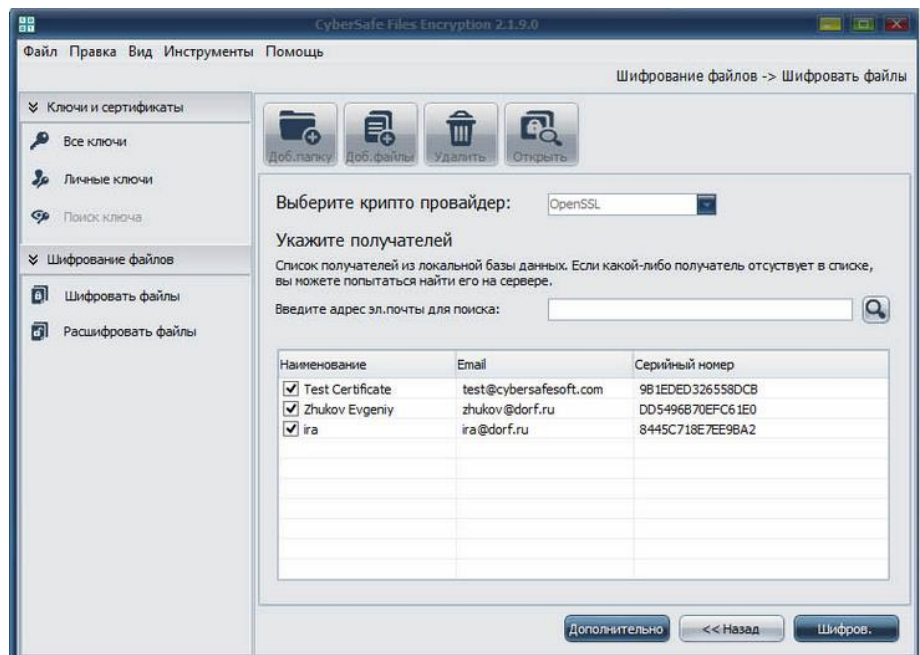
- 1 Откройте CyberSafe, перейдите и на вкладке **Шифрование файлов** выберите опцию **Шифровать файлы**.
- 2 В **Панели опций** выберите **Добавить папку** (Add Folder) или **Добавить файлы** (Add Files) для того, чтобы добавить папку или файлы, подлежащие шифрованию (либо просто перетащите их мышью в Рабочую область программы). После того, как необходимые данные добавлены, нажмите **Далее** (Next).
- 3 В открывшемся окне выберите **Зашифровать файлы ключами получателей** и нажмите **Далее**:



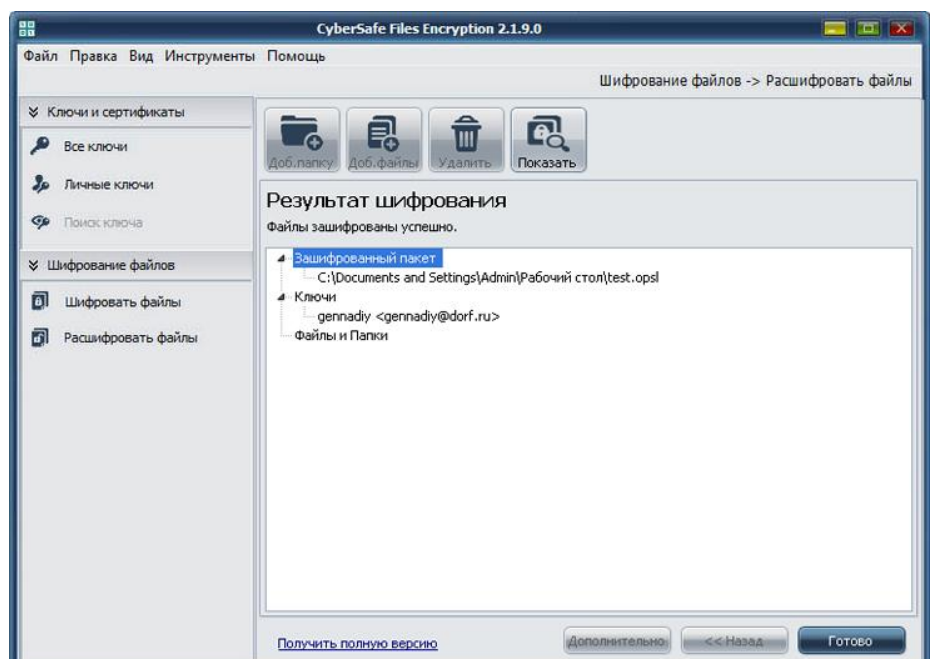
- 4 В открывшемся окне в поле **Выберите крипто провайдер** (Select Crypt Provider) из выпадающего списка выберите криптопровайдер, при помощи которого будет выполняться шифрование.

Выберите пользователей из списка, чьи открытые ключи будут использоваться при шифровании. Если нужный вам пользователь отсутствует в списке, воспользуйтесь функцией поиска его открытого ключа на сервере CyberSafe по электронному адресу этого пользователя.

Нажмите **Шифровать** (Encrypt).



- 5 Начнется процесс шифрования файлов. После завершения шифрования вы увидите следующее окно:



- 6 В разделе *Encrypted Package* будет отображен путь к зашифрованным файлам, в разделе *User Keys* будут отображены пользователи, открытые ключи которых использовались для шифрования, в разделе *Singing* будет отображаться информация о цифровой подписи файлов, а в разделе *Files and Folders* будет отображен список зашифрованных файлов.

Для того, чтобы открыть папку, содержащую зашифрованные файлы, в Панели опций нажмите **Показать в папке** (Show in Folder).

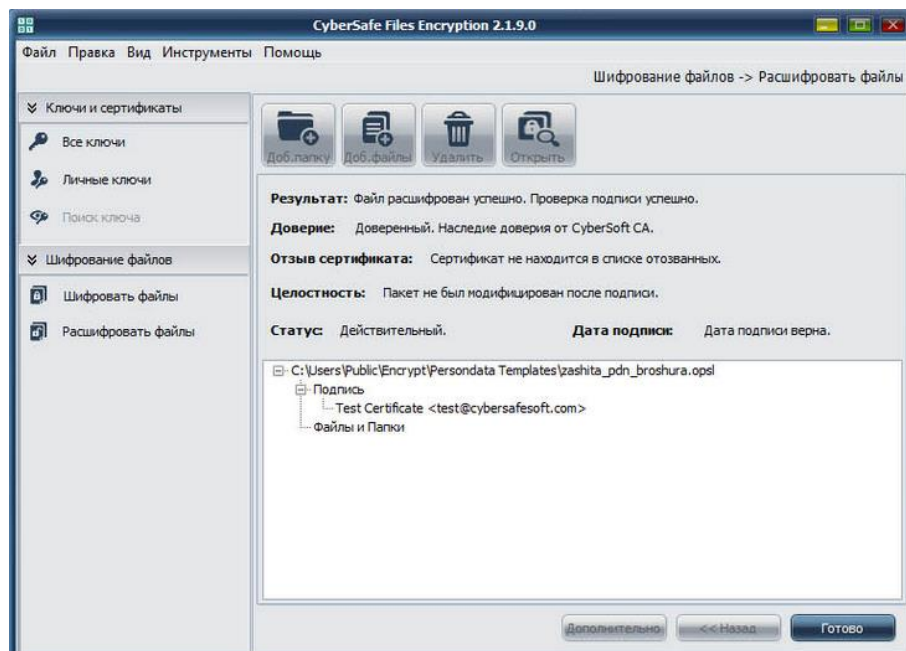
Нажмите **Готово** (Finish). Шифрование файлов на основе сертификатов (ключей) выполнено.

► Для дешифрования файлов

- 1 Откройте CyberSafe, перейдите и на вкладке **Шифрование файлов** выберите опцию **Расшифровать файлы**. В поле *Папка для размещения расшифрованных файлов* укажите, куда должны быть помещены дешифрованные файлы (по умолчанию это будет та же папка, в которой

размещены зашифрованные файлы).

- 2 В **Панели опций** выберите **Добавить файлы** (Add Files) для того, чтобы добавить файлы, подлежащие дешифрованию (или просто перетащите зашифрованные файлы в Рабочую область программы). После того, как необходимые данные добавлены, нажмите **Далее** (Next).
- 3 Откроется диалоговое окно ввода пароля. Введите свой пароль для закрытого ключа, при помощи которого выполняется дешифрование файлов и нажмите **ОК**. Будет выполнено дешифрование файлов, после чего вы увидите следующее окно:



- 4 Дешифрование файла выполнено. Для того, чтобы посмотреть дешифрованные файлы в папке нажмите **Показать в папке** (Show in folder). Для завершения нажмите **Готово** (Finish).

Шифрование файлов паролем

Используйте шифрование файлов паролем когда:

- Вы хотите зашифровать файлы, не используя свой персональный ключ либо открытые ключи других пользователей (это может оказаться менее надежным методом защиты, но, тем не менее, он достаточно надежен).
- У каждого из получателей файлов на их компьютерах установлен CyberSafe .
- Вы хотите, чтобы получатели узнали пароль к зашифрованным файлам.
- Когда у вас нет открытых ключей всех пользователей и вы не можете их найти на сервере CyberSafe .

Примечание. Шифрование паролем относится к традиционным методам шифрования.

Шифрование файлов паролем способно обеспечить очень высокую степень защиты, особенно в случае правильно выбранного пароля. Тем не менее, шифрование при помощи ключа обеспечивает еще более высокий уровень защиты, так как пользователю для дешифрования файлов в данном случае потребуется иметь не только пароль, но и закрытый ключ.

Если файл был зашифрован при помощи пароля, его может расшифровать любой пользователь, который знает этот пароль и у которого установлен CyberSafe , а закрытый ключ в данном случае не требуется.

Предупреждение. Примите все возможные меры для того, чтобы пароль, при помощи которого было выполнено шифрование файлов, не стал известен никому другому, кроме пользователей, для которых предназначены эти файлы. Если пароль стал известен посторонним лицам, зашифруйте файлы заново, используя другой пароль. Однако имейте в виду, что вы не можете ничего сделать для того, чтобы обеспечить новую защиту для изначально зашифрованных файлов.

► **Для шифрования файлов паролем**

- 1** Откройте CyberSafe и на вкладке **Шифрование файлов** выберите опцию **Шифровать файлы**.
- 2** В поле **Encrypt Mode** выберите необходимый режим шифрования. В *Панели опций* выберите **Добавить папку** (Add Folder) или **Добавить файлы** (Add Files) для того, чтобы добавить папку или файлы, подлежащие шифрованию. После того, как необходимые данные добавлены, нажмите **Далее** (Next).
- 3** В открывшемся окне выберите опцию **Шифрование файлов паролем** (Encrypt files by the password) и нажмите **Далее** (Next).
- 4** Откроется диалоговое окно создания пароля. Для того, чтобы видеть вводимый пароль выберите **Показывать пароль** (Show password). В поле **Пароль** (Password) введите пароль, который вы хотите использовать для шифрования данных файлов. Специальный индикатор под вводимым паролем поможет вам оценить его надежность. Надежность пароля будет оцениваться посредством сравнения значения энтропии вводимых вами символов со случайной 128-битной последовательностью (то же значение энтропии, что и в ключе AES128).
- 5** Введите свой пароль повторно в поле **Подтверждение пароля** (Confirm the Password).
- 6** Нажмите **Далее** (Next). Отобразится диалоговое окно создания цифровой подписи. Если это необходимо, выберите закрытый ключ, при помощи которого будет создана цифровая подпись. Пользователь, которому адресованы зашифрованные файлы, сможет проверить вашу цифровую подпись и удостовериться, что эти файлы получены именно от вас.
 - Если вы не хотите подписывать зашифрованные файлы, выберите **Не подписывать** (None).
 - Если вы хотите подписать файлы, выберите ваш ключ из списка ключей, предназначенных для цифровой подписи, затем введите ваш пароль для этого ключа (помните, что это не тот пароль, при помощи которого вы шифруете файлы).
- 7** Нажмите **Далее** (Next). После этого выбранные файлы будут зашифрованы. Нажмите **Готово** (Finish) для завершения. Шифрование файлов паролем выполнено.
- 8** Зашифрованные файлы готовы для отправки другим пользователям. Не забудьте сообщить им пароль к этим файлам, для того, чтобы они могли их расшифровать.

Создание зашифрованных zip-архивов

Zip-архив CyberSafe – это отдельный файл, который зашифрован и сжат для удобства передачи либо резервного копирования. Такие архивы могут содержать любое количество различных файлов и/или папок, что особенно удобно для безопасной их передачи другим пользователям либо создания резервных копий.

Если вы получили zip-архив CyberSafe, вы можете:

- Извлечь все файлы и/или папки из этого архива.
- Извлечь некоторые файлы и/или папки из этого архива.
- Добавить новые файлы и/или папки в архив.
- Изменить архив посредством:

- Изменения типа шифрования.
- Изменения подписывающего ключа.
- Изменения получателей.

Используйте самораспаковывающиеся архивы если:

- Вы хотите создать самораспаковывающийся zip-архив без использования открытых ключей пользователей (это может оказаться менее надежным методом защиты, но, тем не менее, он достаточно надежен).
- У пользователя, которому вы хотите отправить файлы, на компьютере не установлен CyberSafe, но он использует операционную систему Windows.
- Когда вы хотите, чтобы получатели узнали пароль к зашифрованным файлам.
- Когда у вас нет открытого ключа какого-то из пользователей и вы не можете его найти на сервере CyberSafe.

Самораспаковывающийся зашифрованный zip-архив CyberSafe может быть открыт лишь на операционной системе Windows. Его может открыть даже тот пользователь, на компьютере которого не установлен Cyber Safe.

Зашифрованные zip-архивы – это стандартные исполняемые файлы, извлечение которых происходит после двойного клика на них мышью.

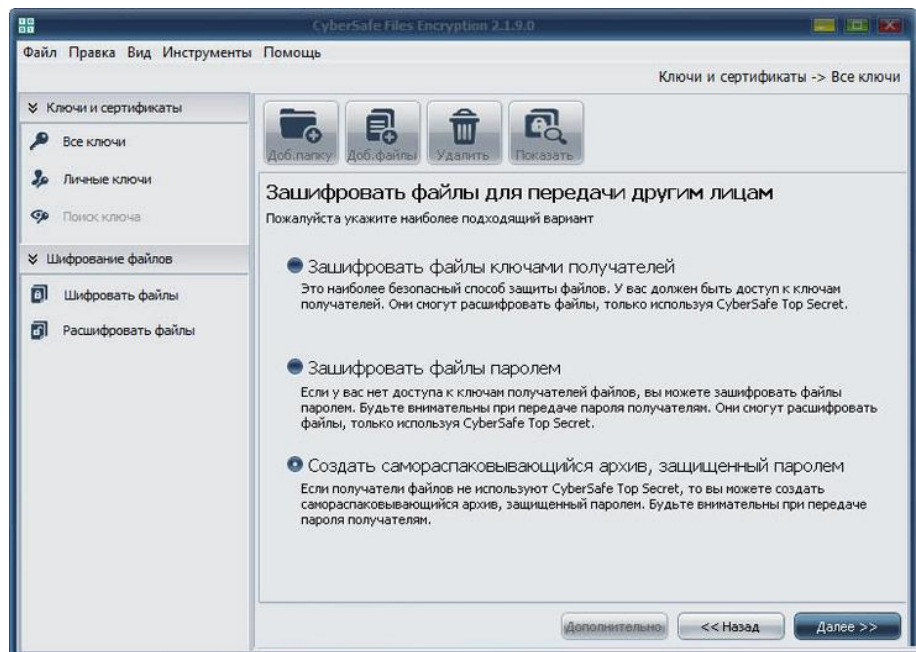
Самораспаковывающиеся zip-архивы имеют больший размер, чем обычные зашифрованные файлы, потому что “механизм”, благодаря которому осуществляется автоматическое извлечение, также занимает определенное место (обычно около 100 Кб).

Как только вы создали зашифрованный zip-архив, отправьте его другому пользователю. Каждый пользователь, который получит такой архив и будет знать пароль к нему, после открытия увидит одни и те же файлы. Если вы хотите отправить различные файлы разным пользователям, вы должны создавать отдельные архивы для каждого из них.

Предупреждение. Примите все возможные меры для того, чтобы пароль, при помощи которого было выполнено создание zip-архива, не стал известен никому другому, кроме пользователей, для которых он предназначен. Если пароль стал известен посторонним лицам, создайте новый зашифрованный архив, используя другой пароль. Однако имейте в виду, что вы не можете ничего сделать для того, чтобы обеспечить новую защиту для изначально созданного архива.

► Для создания самораспаковывающегося zip-архива

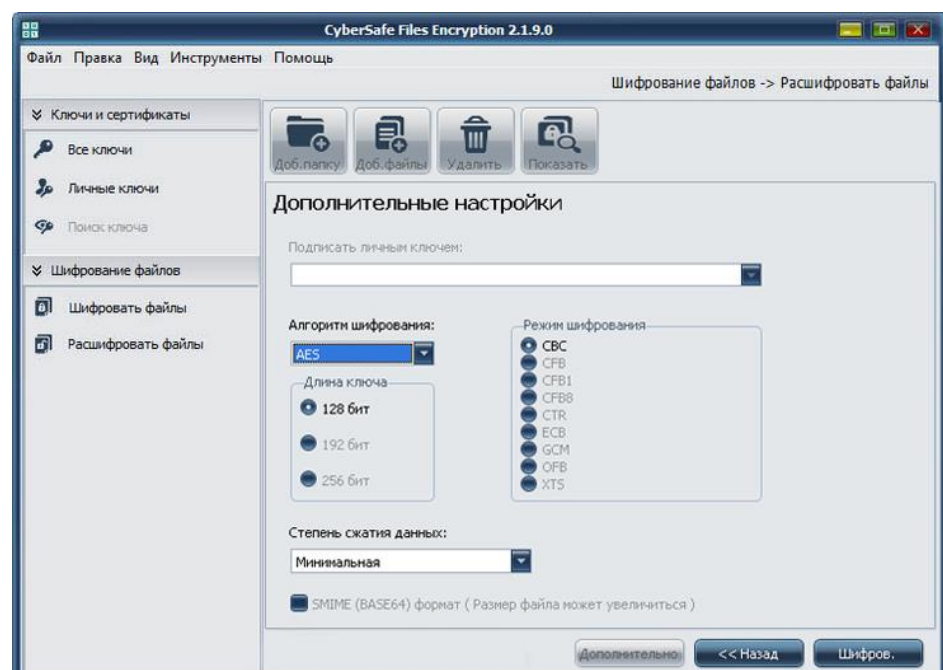
- 1 Откройте CyberSafe и на вкладке **Шифрование файлов** выберите опцию **Encrypt Files**.
- 2 В **Панели опций** выберите **Добавить папку** (Add Folder) или **Добавить файлы** (Add Files) для того, чтобы добавить папки или файлы, которые должны быть добавлены в зашифрованный архив. После того, как необходимые данные добавлены, нажмите **Далее** (Next).
- 3 Выберите опцию **Создать самораспаковывающийся архив, защищенный паролем** (Create the Shelf-Decryption Archive with the password protection) и нажмите **Далее** (Next).



- 4 Откроется диалоговое окно создания пароля. Для того, чтобы видеть вводимый пароль выберите **Показывать пароль** (Show password). В поле **Пароль** (Password) введите пароль, который вы хотите использовать для создания зашифрованного архива и нажмите **ОК**.
- 6 Произойдет создание зашифрованного архива с расширением *.exe, который будет сохранен в папку с исходным файлом.
В том случае, если архив содержит более одного файла, по умолчанию архиву будет присвоено имя одного из файлов.
- 7 В следующем окне будет указан путь к зашифрованному архиву. Нажмите **Готово** для завершения.

Дополнительные настройки шифрования

При выборе любого из способов шифрования (на основе сертификатов, паролем либо зашифрованный архив) прежде чем нажать кнопку **Зашифровать** (Encrypt) вы можете вызвать окно дополнительных настроек при помощи кнопки **Дополнительно** (More options):



В этом окне вы можете:

- Выбрать закрытый ключ для цифровой подписи файлов, подлежащих шифрованию.
- Изменить установленные по умолчанию алгоритм шифрования, уровень защиты и алгоритм хеширования.
- Внести другие дополнительные настройки.

9

Прозрачное шифрование при помощи CyberSafe

CyberSafe предоставляет возможность *прозрачного шифрования файлов* на локальном компьютере пользователя, а также сетевых папок в корпоративном пространстве.

В этой главе

О прозрачном шифровании.	62
Прозрачное шифрование на локальном компьютере.	63
Прозрачное шифрование сетевых папок.	65
Резервное копирование зашифрованных файлов.	67
Система доверенных приложений.	68
Меры безопасности при использовании прозрачного шифрования.	69

О прозрачном шифровании

Функция прозрачного шифрования используется для защиты конфиденциальной информации, хранящейся на локальном компьютере либо на удаленном сервере. Ценная информация, хранящаяся в защищенной папке, постоянно находится в зашифрованном виде. Доступ к зашифрованным файлам, хранящимся в такой папке, пользователь получает после того, как вводит свой пароль закрытого ключа.

При использовании данной функции все файлы защищены при помощи шифрования, однако, не смотря на это, они отображаются в операционной системе как обычные файлы соответствующих приложений – Notepad, Microsoft Word, Microsoft Excel, HTML, графические изображения JPEG, PNG, GIF и так далее. Таким образом, работа со всеми зашифрованными файлами протекает для пользователя в привычном для него режиме.

К примеру, вам необходимо внести изменения в зашифрованный файл с расширением *.doc – все, что вам потребуется – это выполнить те же действия, которые вы выполняете и с незашифрованными файлами. При открытии файл будет автоматически расшифрован, а при сохранении – автоматически зашифрован, однако процесс шифрования/дешифрования полностью прозрачен (незаметен) для пользователя, благодаря чему эта функция получила название *прозрачного шифрования*. Конечно, это очень удобно – для работы с отдельными зашифрованными файлами вам не нужно вручную расшифровывать их и после внесения изменений зашифровывать снова.

Преимущества прозрачного шифрования

Данный вид шифрования функционально похож на работу с зашифрованными виртуальными дисками, однако, с точки зрения безопасности, имеет свои преимущества.

Во-первых, зашифрованные виртуальные диски представляют собой файлы (криптоконтейнеры) больших размеров, которые занимают сотни мегабайт на жестком диске, что явно указывает на то, что на вашем компьютере присутствует зашифрованная информация и, естественно, привлекает ненужное внимание со стороны посторонних лиц и злоумышленников. В то же время папка, созданная при помощи функции прозрачного шифрования, имеет такой же размер, что и незашифрованная папка с аналогичными файлами.

Во-вторых, на криптодисках, как правило, хранится большое количество файлов, а это означает, что на время подключения криптодиска во время

работы хотя бы с одним из этих файлов, уязвимыми для злоумышленников становятся и все остальные. Используя функцию прозрачного шифрования, вы можете создать столько зашифрованных папок, сколько вам нужно и использовать каждую из них для хранения различных файлов. К примеру, можно хранить документы в папках в соответствии с присвоенными им грифами секретности (ДСП, Секретно, СС), используя для их защиты различные алгоритмы шифрования с разной длиной ключа в соответствии с важностью информации. Либо в одной из папок вы можете хранить ценную документацию по рабочим проектам, а в другой – ваши личные фото и видео. В то время, как вы будете работать с одной из этих папок, все остальные папки, содержащиеся в них данные будут надежно защищены.

Это также будет полезным, если к компьютеру кроме вас имеют доступ и другие пользователи. У каждого из пользователей может быть своя папка, защищенная при помощи его собственного ключа и пароля, что позволит разграничить права доступа к конфиденциальной информации.

Прозрачное шифрование на локальном компьютере

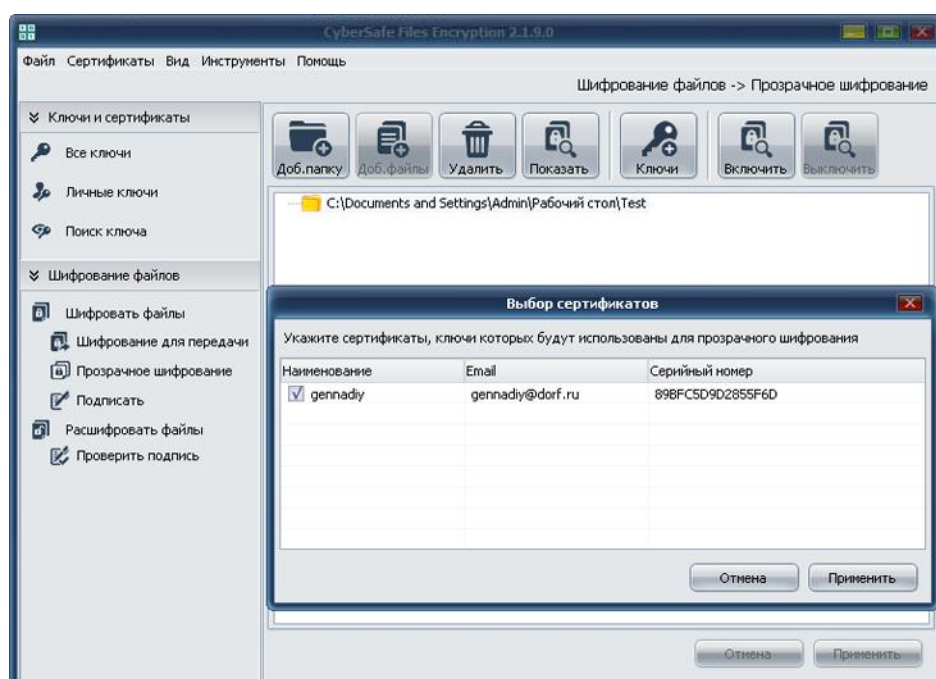
Используйте функцию прозрачного шифрования для защиты файлов на вашем локальном компьютере, а также для быстрой и удобной работы с ними.

► Для создания папки, защищенной при помощи функции прозрачного шифрования на локальном компьютере

- 1 Откройте CyberSafe и на вкладке **Шифрование файлов** выберите опцию **Прозрачное шифрование**.
- 2 На жестком диске вашего компьютера создайте папку, в которой будут храниться зашифрованные файлы и переместите ее в *Рабочую область* CyberSafe при помощи мыши, либо воспользуйтесь опцией **Добавить папку** в Меню опций.

Предупреждение. Добавляемая в CyberSafe папка должна быть *пустой*. Если это не так, содержащиеся в ней данные могут быть утеряны.

- 3 Нажмите **Применить**. В открывшемся диалоговом окне нажмите **Да** – это позволит добавить ключи шифрования для данной папки. Откроется диалоговое окно выбора сертификатов, ключи которых будут использоваться для прозрачного шифрования данной папки. Отметьте галочкой нужные сертификаты (если у вас их больше одного) и нажмите **Применить**:

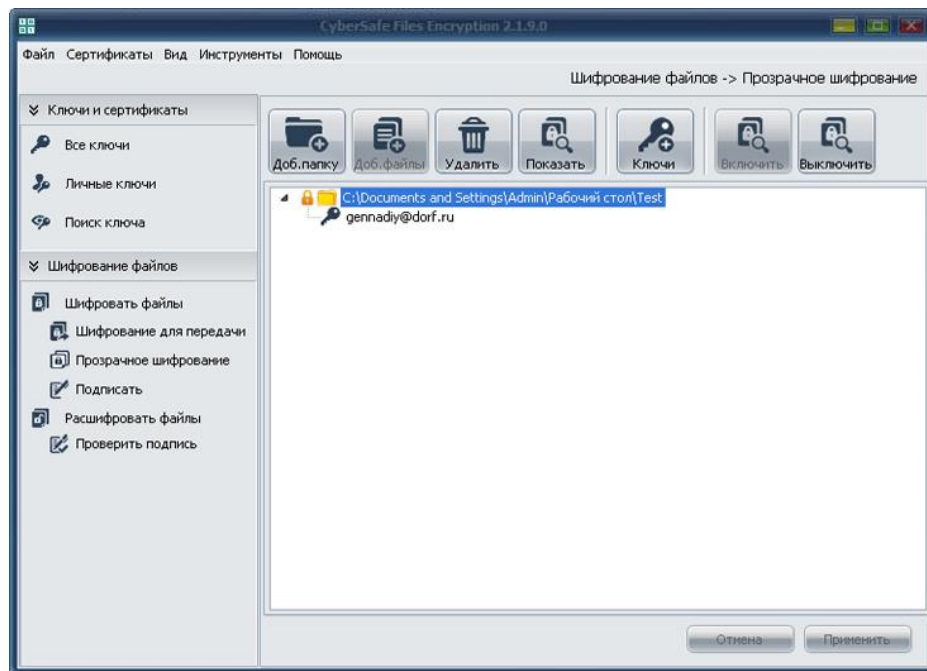


Нажмите **Применить** в Главном окне программы.

Выбранная папка защищена при помощи функции прозрачного шифрования.

- 4 Для того, чтобы добавить в папку файлы, ее предварительно необходимо включить. Для этого выделите папку и в панели опций нажмите кнопку **Включить**. В открывшемся диалоговом окне введите пароль для сертификата, ключ которого используется для шифрования данной папки и нажмите **ОК**.

После того, как папка включена, слева от нее появится иконка замочка. Если дважды кликнуть на папке, под ней отобразится ключ, использующийся для шифрования:



В дальнейшем работа с папкой происходит в обычном режиме – вы можете добавлять, редактировать и удалять хранящиеся в ней файлы.

Получить доступ к файлам, хранящимся в защищенной папке можно двумя способами: либо дважды кликнув мышью на одном из этих файлов непосредственно в этой папке, либо открыть файл через контекстное меню проводника Windows, используя для этого приложение, при помощи которого он был создан.

- 5 После завершения работы с папкой нажмите кнопку **Выключить** в *Панели опций*. Все хранящиеся в папке файлы будут защищены не только от редактирования, но и от копирования и удаления. Удалить папку или хранящиеся в ней файлы, а также внести в них изменения невозможно до тех пор, пока она снова не будет подключена при помощи CyberSafe , либо удалена из программы.

Вы можете создать столько папок, сколько вам требуется, включать и выключать все из них или выборочно, а также хранить эти папки в разных местах на своем локальном компьютере.

Кроме того, вы можете использовать прозрачное шифрование совместно с полнодисковым шифрованием или созданием зашифрованных виртуальных дисков (криптоконтейнеров). Например, вы можете создать зашифрованную папку на жестком диске, защищенном при помощи функции *Шифрование всего диска*.

Каждая из этих трех функций (полнодисковое шифрование, создание виртуальных дисков и прозрачное шифрование) имеют свои отличия и выбираются исходя из существующих требований к безопасности информации. Каждая из них сама по себе обеспечивает надежную защиту

данных, тем не менее, вы можете использовать все эти три функции одновременно, для того, чтобы обеспечить еще более высокую степень защиты.

Прозрачное шифрование сетевых папок

Функция прозрачного шифрования может быть успешно применена для удобной работы с секретными документами в корпоративном пространстве.

Организовать такую работу можно следующим образом. На корпоративном файловом сервере создается папка, содержащая конфиденциальные документы компании и к этой папке по сети устанавливается доступ сотрудникам компании, которым данные документы нужны для работы.

Также как и в случае прозрачного шифрования на локальном компьютере, все зашифрованные файлы, хранящиеся в сетевой папке, продолжают отображаться в привычном режиме и имеют расширения соответствующих приложений (txt, doc, xls, html, jpg и др.). Если сотруднику один из этих файлов необходим для работы, он просто открывает его двойным кликом мыши, вносит необходимые изменения и закрывает. В том случае, если в защищенную папку добавляются новые файлы, они также автоматически зашифровываются.

При обращении к файлу соответствующего приложения он становится доступным для работы, а после завершения перезаписывается на сервер в зашифрованном виде со всеми внесенными изменениями. Процессы шифрования и дешифрования происходят «на лету» - в фоновом (прозрачном) режиме и не требуют от него никаких дополнительных действий и навыков в области шифрования. Иными словами, функция прозрачного шифрования никак не сказывается на удобстве и все работа с файлами происходит для пользователя в привычном для него режиме.

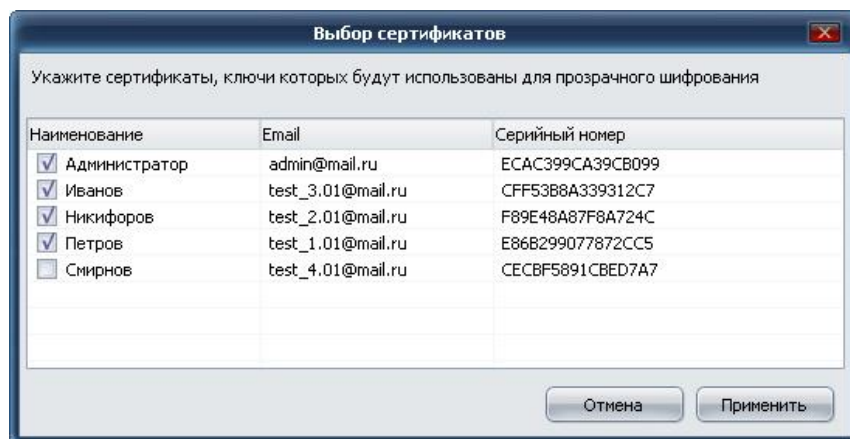
CyberSafe устанавливается только на компьютерах сотрудников компании и не требует никаких дополнительных установок на файл-сервере. Все операции связанные с расшифровыванием и зашифровыванием файлов осуществляются *на стороне пользователя*, а на сервер отправляются лишь зашифрованные файлы, к которым имеют доступ лишь авторизованные пользователи. Другие пользователи могут видеть эти файлы, однако они не имеют к ним доступа.

Пользователи без доступа также могут видеть зашифрованные файлы, но они не могут читать и изменять их. Это означает, что если у системного администратора нет доступа к документам в какой-то из папок, он все равно может осуществлять их резервное копирование. Конечно, все резервные копии файлов также зашифрованы.

Кроме того, функция прозрачного шифрования позволяет разграничить доступ сотрудников компании к конфиденциальной информации. Например, на файл-сервере может быть три папки с грифами ДСП, Секретно и Совершенно Секретно, а доступ к этим папкам имеют лишь некоторые сотрудники, которых назначает администратор.

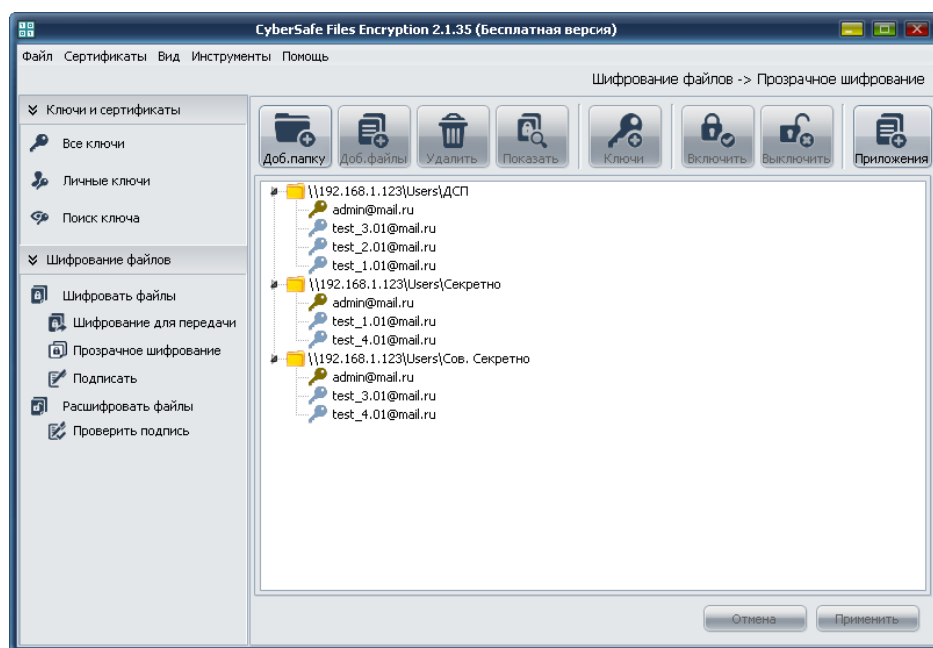
► Для создания папок, защищенных при помощи функции прозрачного шифрования на файловом сервере

- 1** Откройте CyberSafe и на вкладке **Шифрование файлов** выберите опцию **Прозрачное шифрование**.
- 2** На удаленном файл-сервере создайте папки, в которых будут храниться зашифрованные файлы, предназначенные для разных пользователей. Переместите одну из них в *Рабочую область* CyberSafe при помощи мыши, либо воспользуйтесь опцией **Добавить папку** в *Меню опций*.
- 3** Нажмите **Применить**. В открывшемся диалоговом окне нажмите **Да** – это позволит добавить ключи шифрования для данной папки. Откроется диалоговое окно выбора сертификатов пользователей, ключи которых будут использоваться для прозрачного шифрования данной папки. Отметьте галочкой сертификаты тех пользователей, которые будут иметь доступ к данной папке и нажмите **Применить**:



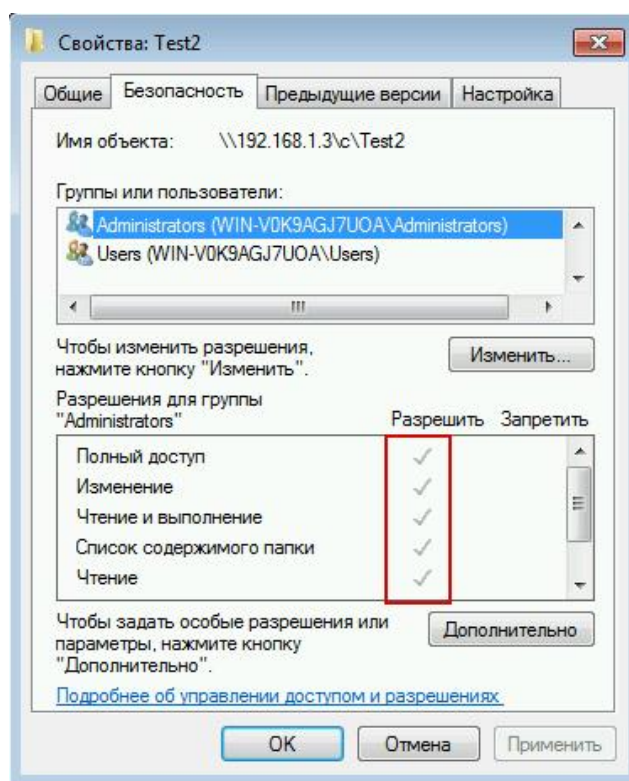
В открывшемся диалоговом окне, запрашивающем подтверждение на установку Ключа Администратора, нажмите **Да**.

- 4 Аналогичным образом добавьте другие папки, размещенные на сервере, в CyberSafe и назначьте для каждой из них ключи требуемых пользователей. В результате в *Рабочей области* программы будут отображаться все добавленные вами папки, а под каждой из них можно увидеть открытые ключи тех пользователей, которые имеют к ним доступ:



Пользователь, ключ которого был назначен Ключом Администратора папки, может в любое время удалить ключи других пользователей, имеющих доступ к этой папке либо назначить новых.

Добавляя в CyberSafe новую папку, администратор должен убедиться, что у него есть доступ и все разрешения к ней. Для этого в свойствах папки необходимо перейти на вкладку *Безопасность* и проверить наличие галочек в соответствующих строках:



Вся служебная о зашифрованной папке хранится в альтернативных потоках данных (ADS) файловой системы NTFS. Для того, чтобы ее обнулить, необходимо удалить данную папку.

Примечание. Так как служебная информация о зашифрованной папке, в частности открытые ключи пользователей, имеющих к ней доступ, хранятся в альтернативных потоках данных файловой системы NTFS, прозрачное шифрование возможно лишь на разделах этой файловой системы.

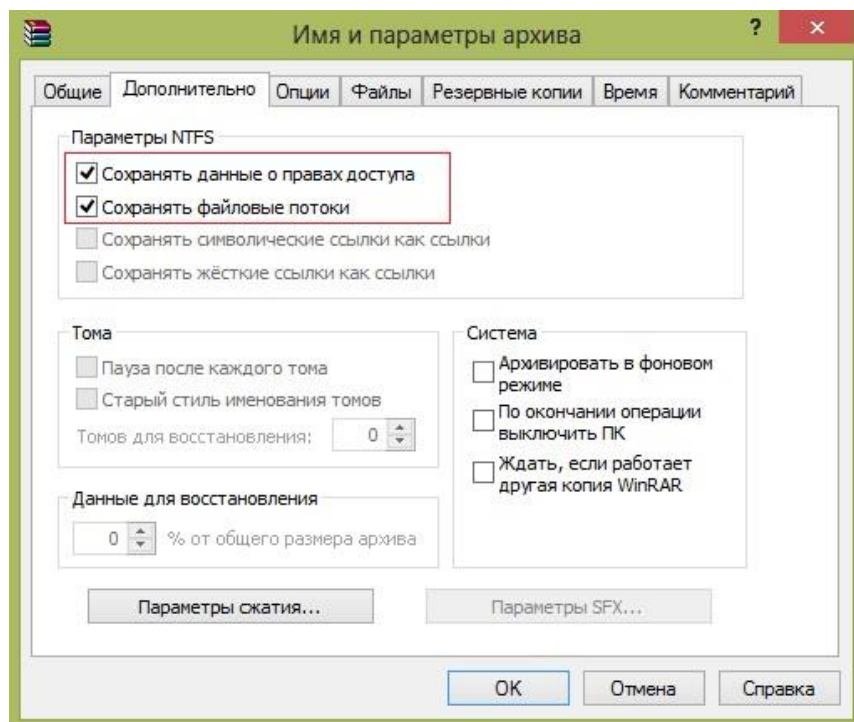
Резервное копирование зашифрованных файлов

В некоторых случаях может возникнуть необходимость выполнить резервное копирование файлов, находящихся в папке, защищенной при помощи функции прозрачного шифрования.

Резервное копирование может быть выполнено при помощи любых автоматических средств, поддерживающих сохранение альтернативных потоков данных файловой системы NTFS, к примеру, архиватором WinRAR:

► Для резервного копирования зашифрованных файлов:

- 1 Правой кнопкой мыши нажмите на папке, защищенной при помощи функции прозрачного шифрования и в контекстном меню выберите **Добавить в архив**.
- 2 На вкладке **Дополнительно** установите галочки в пунктах **Сохранять данные о правах доступа** и **Сохранять файловые потоки**:



- 3 Нажмите **ОК**. Папка будет добавлена в архив.
- 4 Восстановите созданный архив на компьютере, где планируется хранить резервные копии зашифрованных файлов. Для этого переместите архив в необходимое место на новом компьютере, нажмите на нем правой кнопкой мыши и выберите **Извлечь в текущую папку**.
- 5 Разархивированную папку добавьте в CyberSafe в список папок, защищенных при помощи функции прозрачного шифрования. Это можно сделать через меню программы (**Прозрачное шифрование > Добавить папку**) либо просто скопировать данную папку в *Рабочую область* программы (выбрана вкладка *Прозрачное шифрование*). Нажмите **Применить**.
- 6 Файлы доступны для работы и находятся в режиме прозрачного шифрования.

Система доверенных приложений

Не смотря на то, что все файлы в папке, защищенной при помощи функции прозрачного шифрования зашифрованы, в том момент когда пользователь открывает какой-либо из файлов для работы на своем компьютере, существует возможность, что к нему получат доступ нежелательные приложения (в том случае, конечно, если компьютер инфицирован).

Для предотвращения этого в CyberSafe в качестве дополнительной меры безопасности существует *система доверенных приложений*, благодаря которой пользователь на своем локальном компьютере, либо системный администратор в организации может определить список программ, которые смогут получить доступ к файлам из защищенной папки. Все остальные приложения, не вошедшие в список доверенных, не будут иметь доступа.

К примеру, в своей защищенной папке вы храните лишь текстовые документы. Тогда, вполне логичным будет разрешить доступ к этим документам лишь тем приложениям, которые вы используете для работы с ними, например Word, Exel, Notepad или другим текстовым редакторам, а всем остальным запретить, определив их как запрещенные.

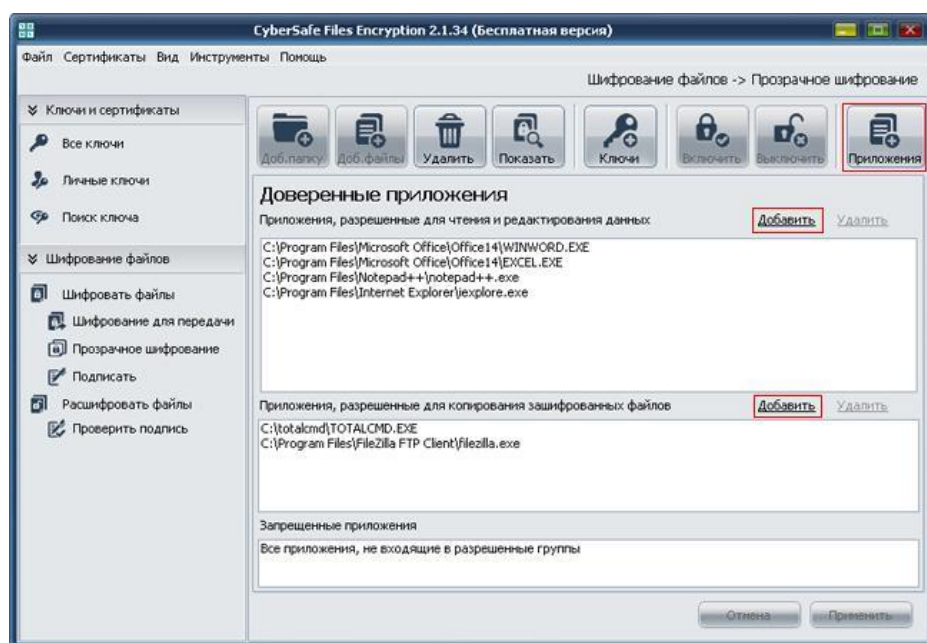
Таким образом, с помощью CyberSafe можно ограничить доступ к конфиденциальной информации для шпионских программ, руткитов и другого вредоносного ПО.

► Для назначения доверенных приложений к папке, защищенной при помощи функции прозрачного шифрования

- 1 Откройте CyberSafe и на вкладке **Шифрование файлов** выберите опцию **Прозрачное шифрование**.
- 2 В *Рабочей области* выберите папку, к которой будут назначены доверенные приложения, и в *Панели опций* нажмите **Приложения**.
- 3 Для того, чтобы добавить приложение в список доверенных нажмите **Добавить** и в проводнике Windows укажите файл с расширением *.exe этого приложения (находится в папке с установленными файлами этого приложения).

Аналогичным образом добавьте все приложения, которые вы планируете использовать для работы с файлами в данной папке.

В том случае, если существует необходимость добавить приложения, которые не смогут открывать файлы в зашифрованной папке, но смогут осуществлять их копирование, используйте кнопку **Добавить** в соответствующем окне:



Изначально для CyberSafe все приложения являются доверенными. Однако после составления такого списка, остальные приложения, не вошедшие в число доверенных, будут считаться запрещенными и не смогут получить доступ к файлам в папке, даже если она подключена и пользователь работает с каким-либо из файлов, хранящихся в ней.

Меры безопасности при использовании прозрачного шифрования

Защищенная при помощи функции прозрачного шифрования папка видна в операционной системе для других пользователей. Однако все хранящиеся в ней файлы не доступны для работы, копирования или удаления до тех пор, пока эта папка не будет включена в CyberSafe при помощи вашего пароля.

Примечание. Для того, чтобы не позволить злоумышленнику подобрать пароль к зашифрованным файлам и папкам, используйте надежные пароли. Подробнее о создании надежных паролей см. в разделе *“Работа с паролями и ключевыми фразами”*.

Для того, чтобы ценные данные, которые вы храните на своем локальном компьютере не попали в руки злоумышленников или посторонних лиц, придерживайтесь следующих мер безопасности:

- Используйте шифрование для защиты всей конфиденциальной информации.
- Не держите папку, защищенную при помощи прозрачного шифрования постоянно включенной, так как из нее можно похитить файлы так же, как и с обычного диска. Подключайте папку только на время работы с хранящимися в ней данными и отключайте сразу же после того, как работа окончена.
- Для ограничения доступа к зашифрованным файлам при включенной папке используйте *систему доверенных приложений*.
- Все данные в папке доступны любому пользователю, знающему к ней пароль. В том случае если на вашем локальном компьютере имеются различные группы информации, предназначенные для разных пользователей, следует завести несколько отдельных папок с разными паролями.
- Зашифрованная информация будет полностью утеряна в том случае, если диск, на котором она хранится, будет поврежден или отформатирован. Поэтому компания CyberSoft рекомендует вам регулярно выполнять резервное копирование вашей конфиденциальной информации, хранящейся в защищенной папке.

10

Защита дисков при помощи CyberSafe

CyberSafe позволяет защитить все данные, содержащиеся на жестких дисках компьютеров, ноутбуков, внешних жестких дисках и USB флеш-накопителях, включая загрузочные сектора, системные файлы и файлы подкачки. Вместе с этим, вы можете использовать программу для шифрования отдельных разделов Windows, в том числе и загрузочного, а также создавать виртуальные зашифрованные диски.

Во время работы с файлами на таких дисках, шифрование протекает как фоновый процесс, который полностью прозрачен для пользователя и автоматически защищает все ценные данные без необходимости выполнения каких-либо дополнительных действий.

В этой главе

О шифровании дисков программой Cyber Safe	81
Подготовка диска к шифрованию	82
Шифрование диска или раздела	83
Создание виртуальных дисков	84

О шифровании дисков программой CyberSafe

При шифровании всего диска CyberSafe шифрует каждый раздел при помощи симметричного ключа. Использование этой функции подразумевает шифрование всех расположенных на диске файлов, включая файлы операционной системы, файлы установленных приложений, файлы данных, файлы подкачки, свободное пространство и временные файлы.

При последующей перезагрузке CyberSafe запросит у вас ввод пароля. После этого зашифрованные данные при вашем обращении к ним будут расшифрованы. В то же время, прежде чем какие-либо данные будут записаны на диск, они будут зашифрованы. Как только вы авторизовались (ввели нужный пароль к зашифрованному диску) файлы становятся доступными для работы. После завершения работы в операционной системе ваш диск снова становится защищенным от использования посторонними лицами.

Прежде чем защитить свой диск при помощи функции шифрования, важно понять, как проходит процесс создания и последующего использования зашифрованного диска. Для этого необходимо:

1. Выполнить пункты, описанные в параграфе *"Подготовка диска к шифрованию"*.
2. Запустить процесс шифрования всего диска или его раздела (см. параграф *"Шифрование всего диска или раздела"*).
3. Узнать о том, как работать с зашифрованным диском (см. параграф *"Использование зашифрованного диска"*).
4. Понять функции, которые помогут избежать проблем с безопасностью (см. параграф *"Особые меры безопасности, предпринимаемые CyberSafe"*).

Предостережение. Как только вы разблокировали зашифрованный диск, введя свой пароль, все файлы на нем становятся доступны как для вас, так и для других пользователей, которые имеют физический доступ к вашему компьютеру. Ваши файлы будут доступны до тех пор, пока вы не заблокируете их снова, выключив или перезагрузив компьютер.

Для того, чтобы защитить файлы даже во время использования компьютера, используйте функцию *Создание виртуальных дисков* или функцию *Прозрачное шифрование*. Для более подробной информации см. раздел *“Создание виртуальных дисков”* и главу 8 *“Прозрачное шифрование при помощи CyberSafe”*.

В чем отличие шифрования логического диска от создания виртуального диска?

Отличие функции *Создание виртуального диска* от функции *Шифрование всего диска* заключается в том, что созданные виртуальные диски работают как дополнительные тома на вашем компьютере, которые могут оставаться зашифрованными даже в то время, когда вы работаете со всей системой. Эти виртуальные тома подобны хранилищам, в которых вы можете хранить файлы, нуждающиеся в защите. Это не физические диски, а только виртуальные, созданные и управляемые CyberSafe.

Функция *Шифрование всего диска* обеспечивает защиту всего физического жесткого диска, но только в том случае, если этот диск не используется.

Обе функции работают независимо друг от друга, поэтому вы можете использовать их одновременно. Для получения более подробной информации см. раздел *“Создание виртуальных дисков”*.

Подготовка диска к шифрованию

Прежде чем вы зашифруете весь жесткий диск, вам необходимо выполнить несколько действий, которые помогут обеспечить успешное шифрование.

- **Определите, поддерживает ли целевой диск шифрование** (подробнее об этом см. в параграфе *“Типы дисков, поддерживающие шифрование”*).
- **Убедитесь в работоспособности диска перед его шифрованием.** Целевой диск может содержать ошибки (CRC). Следует устранить эти ошибки до начала процесса шифрования (подробнее об этом см. в параграфе *“Проверка работоспособности диска перед шифрованием”*).
- **Создайте резервную копию диска перед шифрованием.** Прежде чем вы зашифруете свой диск, убедитесь, что вы создали его резервную копию, что не позволит вам потерять свои данные в том случае, если ваш компьютер будет потерян, украден или вы окажетесь неспособными расшифровать диск. Также не забывайте регулярно делать резервные копии своего диска.
- **Учтите время, которое займет процедура шифрования** и подготовьтесь к этому (подробнее об этом см. в параграфе *“Расчет продолжительности шифрования”*).
- **Убедитесь, что вы будете обеспечены источником бесперебойного питания** во время процесса шифрования (подробнее об этом см. в параграфе *“Обеспечение бесперебойного питания в процессе шифрования”*).
- **Выполните тестирование на совместимость программного обеспечения.** Если вы используете CyberSafe в организации, компания “КиберСофт” рекомендует вам проверить функцию *Шифрование всего диска* на небольшой группе компьютеров (подробнее об этом см. в параграфе *“Тестирование на совместимость программного обеспечения”*).

Типы дисков, поддерживающих шифрование

Функция *Шифрование всего диска* используется для защиты данных на следующих типах дисков:

- Жесткие диски стационарных компьютеров или ноутбуков (полностью весь диск или его раздел).
- Внешние диски, за исключением аудио проигрывателей и цифровых

камер.

- USB-флеш накопители.

Вы можете шифровать диски или их разделы, отформатированные в файловых системах FAT16, FAT32 или NTFS.

Функция *Шифрование всего диска* может быть использована на компьютерах с несколькими операционными системами (такими как Windows XP, Windows 2000, Windows Vista, Windows 7, 8).

При использовании функции *Шифрование всего диска* не существует каких-либо требований к минимальному или максимальному размеру зашифрованного диска. Если диск или его раздел поддерживаются операционной системой, он должен работать с CyberSafe .

Поддерживаются все режимы Windows (Ждущий режим, Спящий режим и Режим гибернации).

Не поддерживается шифрование следующих типов дисков:

- Динамические диски.
- Дискеты и CD-RW/DVD-RW диски.

Предостережение. Windows XP позволяет преобразовывать обычные диски в динамические диски, которые поддерживают функции, не поддерживаемые обычными дисками. Никогда не выполняйте такое преобразование с загрузочным системным диском, который уже был зашифрован при помощи CyberSafe . Такое преобразование (из обычного диска в динамический) приведет к тому, что диск станет непригодным для использования.

Алгоритмы шифрования, используемые для шифрования дисков

Шифрование диска осуществляется при помощи сгенерированного сеансового ключа размером 256 бит для AES и ГОСТ алгоритмов. Сеансовый ключ шифруется при помощи открытого ключа сертификата размером 1024-8192 бит. Такая система является гарантировано надежной, а ее преимуществом по сравнению с системой паролей во всех остальных видах программного обеспечения заключается в том, что длина сеансового ключа максимальна – 256 бит или 32 символа.

Проверка работоспособности диска перед шифрованием

Ошибки CRC (Cyclic Redundancy Check errors) во время шифрования жестких дисков – совсем не редкость. Для того, чтобы избежать проблем во время шифрования, компания “КиберСофт” рекомендует устранить все ошибки на диске еще до начала шифрования и шифровать только исправные диски.

Хорошим решением в данном случае будет использование специальных утилит для сканирования дисков, позволяющие выполнять их проверку и устранение всех несовместимостей, которые могут привести к возникновению CRC-ошибок. Стандартной утилиты Windows в данном случае не достаточно и вместо нее следует использовать такие программы как SpinRite или Norton Disk Doctor. Эти приложения смогут исправить ошибки, которые способны нарушить процесс шифрования.

Предупреждение. Диски с высокой степенью фрагментации перед шифрованием следует дефрагментировать.

Расчет продолжительности шифрования

Шифрование диска – это энергоемкий процесс, оказывающий значительную нагрузку на процессор компьютера. Чем больше размер шифруемого диска (или его раздела), тем дольше длится его шифрование. Если вы планируете начать процедуру шифрования всего диска, вы должны принять это во внимание.

На скорость шифрования диска влияют следующие факторы:

- Размер диска или раздела.
- Скорость работы процессора и количество процессоров.
- Количество активных системных процессов.
- Количество других активных приложений.
- Мощность процессора, потребляемая другими активными приложениями.

На среднестатистическом компьютере шифрование диска объемом 100 Гб занимает около трех часов (при условии, что никакие другие приложения не работают). Тем не менее, на мощных компьютерах шифрование диска такого же объема может занять менее часа.

В процессе шифрования вы по-прежнему можете работать с операционной системой. Не смотря на то, что операционная система будет работать медленнее, чем обычно, тем не менее, она полностью работоспособна.

CyberSafe автоматически замедлит скорость шифрования если вы начнете работать с операционной системой. Это означает, что если вы не будете работать с компьютером во время шифрования диска, процесс шифрования будет проходить быстрее. Операционная система вернется к нормальному режиму работы сразу после окончания процесса шифрования.

Если в процессе шифрования вы решите запустить другие приложения, скорее всего, они будут работать медленнее чем обычно, до тех пор, пока процесс шифрования не будет завершен.

Обеспечение бесперебойного питания в процессе шифрования

Так как шифрование – это энергоемкий процесс, оказывающий значительную нагрузку на процессор компьютера, он не может быть выполнен на ноутбуках, работающих от аккумуляторной батареи. Компьютер должен быть подключен к сети.

Не отключайте компьютер до тех пор, пока процесс шифрования не будет завершен. Если существует вероятность того, что в процессе шифрования могут быть перебои в питании – или если у вас нет источника бесперебойного питания – его следует подключить.

Предупреждение. Это справедливо и для съемных носителей, таких как внешние жесткие диски. Вы рискуете повредить устройство, если отключите его во время процесса шифрования.

Тестирование на совместимость программного обеспечения

Если вы используете CyberSafe в организации, компания “КиберСофт” рекомендует вам проверить функцию *Шифрование всего диска* на небольшой группе компьютеров, для того, чтобы убедиться в том, что эта функция не конфликтует с каким-либо программным обеспечением, установленным на этих компьютерах, а уже после этого использовать функцию шифрования на большом количестве компьютеров.

Это особенно необходимо для компьютеров, работающих в стандартизированной Корпоративной операционной среде (Corporate Operating Environment или COE). Некоторое другое программное обеспечение по защите дисков может быть несовместимым с функцией *Шифрование всего диска* CyberSafe и это может привести к серьезным проблемам с дисками, вплоть до потери данных.

Шифрование диска или раздела

Как только вы подготовили диск, можно переходить к его шифрованию. Прежде чем начать, примите во внимание следующее:

- Во время шифрования ваша система будет работать несколько медленнее, чем обычно, однако она будет полностью пригодна для работы.

- Вы можете свернуть или закрыть окно CyberSafe во время шифрования. Это не приведет к прерыванию процесса, но, в тоже время, не повысит его скорость.
- Вы не можете выполнять операции по шифрованию, дешифрованию или повторное шифрование диска или раздела одновременно. Как только вы начали какую-либо из этих операций, вы не можете запустить еще одну до тех пор, пока не завершится предыдущая.

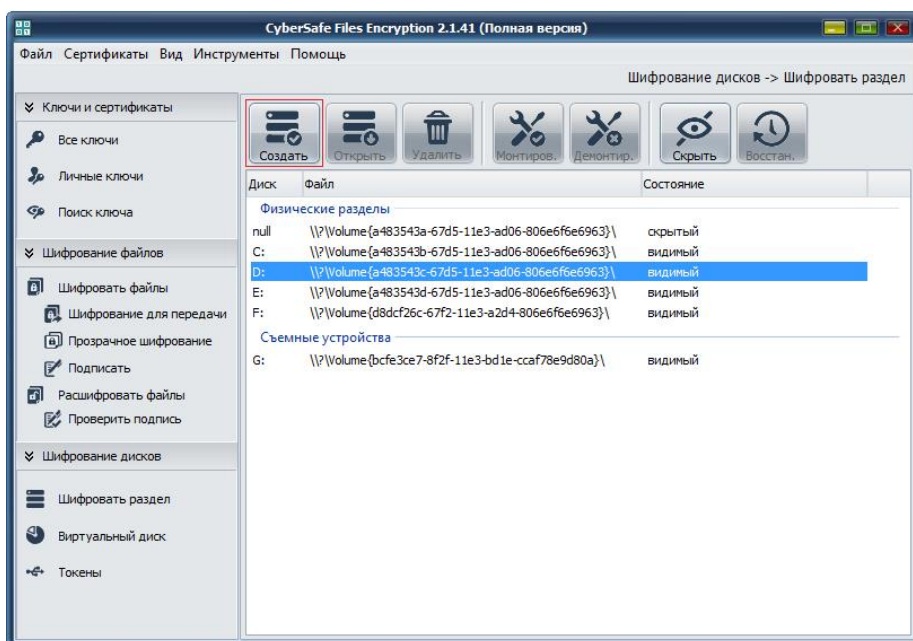
Шифрование логического диска/раздела

Перед началом шифрования логического диска убедитесь, что вы создали его резервную копию – это не позволит вам потерять ваши данные, если ноутбук или компьютер будет украден или вы не окажетесь неспособными расшифровать диск.

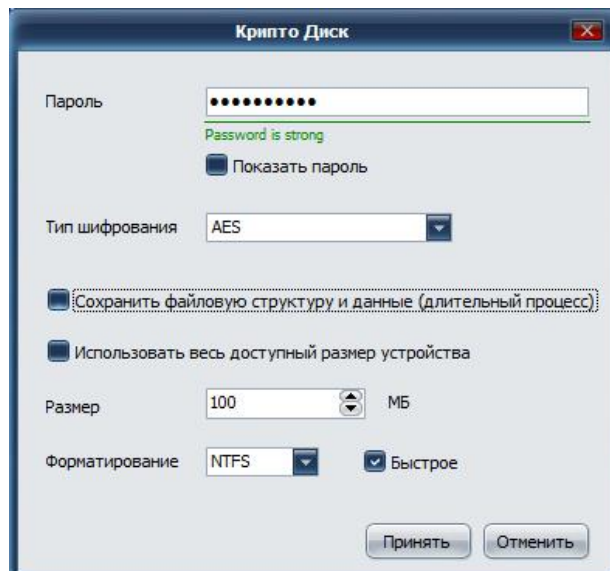
Предупреждение. Во время шифрования диска, не соглашайтесь ни с какими системными уведомлениями об обновлении. В том случае, если обновление было запущено автоматически, не перезагружайте компьютер до тех пор, пока процесс шифрования не будет завершен.

► Для защиты диска или раздела при помощи CyberSafe

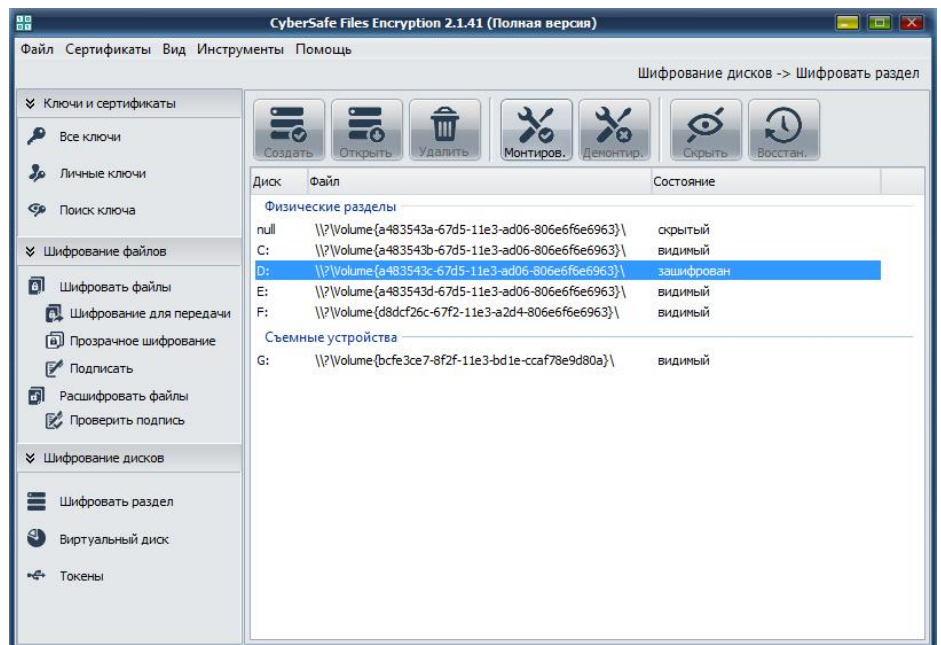
- 1 Откройте CyberSafe, перейдите на вкладку **Шифрование дисков**, выберите опцию **Шифровать раздел** и в *Рабочей области* выделите диск, который будет зашифрован (или диск, на котором будет создан зашифрованный раздел):



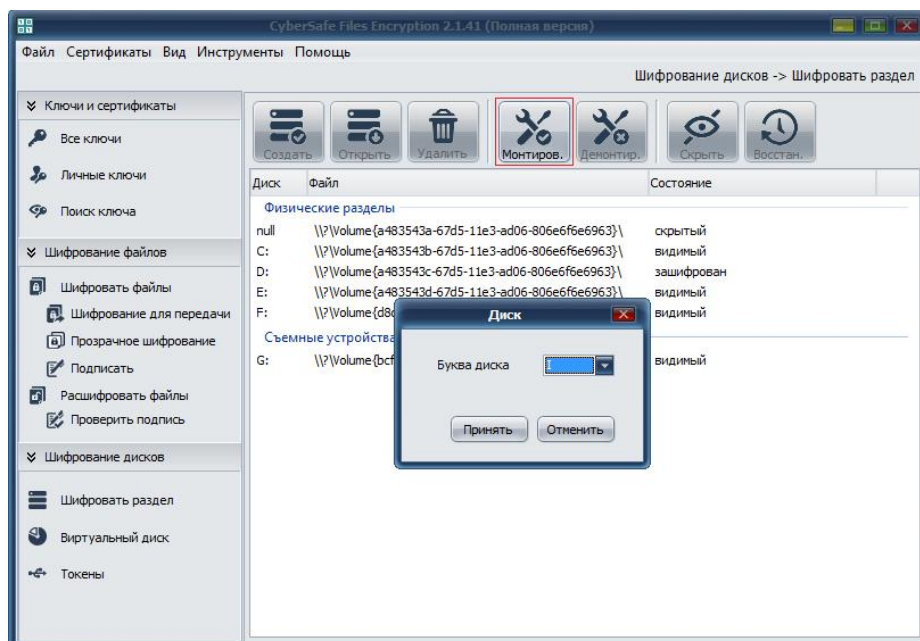
- 2 В открывшемся диалоговом окне введите пароль к шифруемому диску/разделу, выберите алгоритм шифрования, а также файловую систему. В том случае, если вы хотите зашифровать жесткий диск целиком, галочку напротив пункта **Использовать весь доступный размер устройства** следует оставить включенной. Если вы хотите зашифровать раздел выбранного диска, эту галочку следует снять, после чего указать размер зашифрованного раздела:



- 3 Нажмите **Принять**. Произойдет шифрование диска/раздела, после чего в *Рабочей области* выбранный диск будет значиться как зашифрованный:



- 4 Для того, чтобы монтировать диск выделите его в *Рабочей области*, нажмете **Монтиров.** в *Панели опций* и в открывшемся окне выберите свободную букву, на которую будет смонтирован созданный криптодиск в качестве логического диска операционной системы:

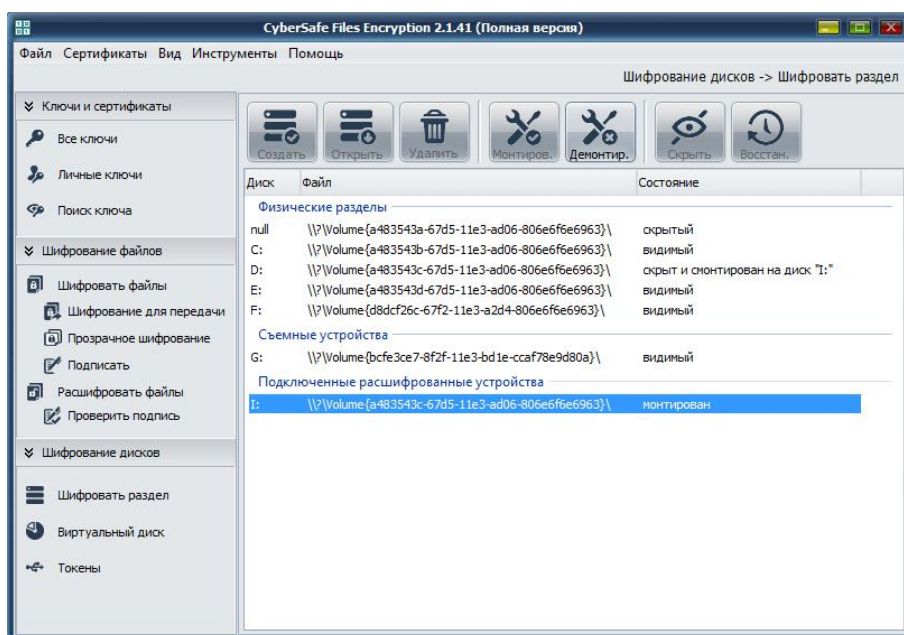


Нажмите **Принять**. В открывшемся диалоговом окне введите пароль к этому криптодиску. После этого криптодиск будет смонтирован и доступен для работы.

В Windows такой диск будет отображаться в качестве обычного логического диска, а в CyberSafe он будет виден в *Рабочей области* в разделе *Подключенные расшифрованные устройства*.

Предупреждение. После монтирования криптодиска все данные на нем становятся расшифрованными, поэтому в подключенном состоянии криптодиск следует держать минимальное время и отключать сразу же после завершения работы с хранящимися на нем файлами.

Для защиты подключенного криптодиска после его монтирования CyberSafe автоматически скроет смонтированный диск от операционной системы (информацию об этом можно увидеть в графе *Состояние*):



После завершения работы с разделом его необходимо отключить. Для

этого нужно выделить смонтированный диск *Рабочей области* и в *Панели опций* нажать **Демонтир**.

Действия по монтированию и демонтированию повторяются каждый раз при работе с криптодиском, поскольку их сокращение или устранение ведет к возникновению серьезной бреши в системе защиты.

До тех пор, пока криптодиск не будет смонтирован, все хранящиеся на нем данные являются недоступными. Даже в том случае, если диск окажется в руках злоумышленников, он не может быть смонтированным без знания пароля к нему, а вся хранящаяся на диске информация будет представлять собой не что иное, как совокупность бесполезных байтов.

Создание виртуальных дисков

Виртуальные диски – это области пространства на любом из дисков, подключенных к вашему компьютеру, которые не учитываются в качестве свободного пространства и воспринимаются операционной системой в качестве обычных логических дисков.

О виртуальных дисках CyberSafe

Зашифрованные виртуальные диски CyberSafe похожи на банковские сейфы, в которых вы храните свои ценные данные. Создание виртуальных дисков – очень удобная функция, поскольку вы можете хранить на таком диске все ценные данные, нуждающиеся в защите, в то время как прочая информация на вашем компьютере разблокирована и доступна для использования.

Виртуальный диск выглядит и ведет себя как дополнительный жесткий диск, хотя в действительности это просто файл, находящийся на одном из жестких дисков вашего компьютера. Виртуальный диск обеспечивает место для хранения ваших файлов. Кроме того, вы можете устанавливать в него различные приложения. Не смотря на это, такой диск может быть заблокирован в любой нужный момент, не влияя на работу компьютера в целом. Когда вам нужно воспользоваться файлами или приложениями, хранящимися на виртуальном диске, вы можете разблокировать его, снова сделав этот диск доступным.

Виртуальные диски CyberSafe блокируются и разблокируются путем их монтирования и демонтирования на компьютере. CyberSafe помогает вам осуществлять эти операции.

Существует два принципиально отличных способа создания зашифрованных виртуальных дисков. Первый подразумевает создание файла необходимого раздела, его подключение и форматирование. Этот процесс занимает считанные секунды. Вторым способом предполагается создание файла и его шифрование, и лишь после форматирование и подключение. Эта процедура длится в десять раз дольше, тем не менее, она справедливо считается более надежной. CyberSafe основывает свою работу на втором способе.

Если виртуальный диск CyberSafe смонтирован, вы можете:

- Перемещать/копировать файлы на или со смонтированного виртуального диска.
- Сохранять файлы на смонтированный виртуальный диск.
- Устанавливать на виртуальный диск различные приложения.

Файлы и приложения, хранящиеся на виртуальном диске CyberSafe, зашифрованы. Если виртуальный диск демонтирован, он не виден в Проводнике Windows и не доступен для пользователей без прохождения процедуры авторизации. Важно понимать, что все файлы, хранящиеся на виртуальном диске, остаются зашифрованными и защищенными, а расшифруются лишь тогда, когда вы используете какой-либо из этих файлов.

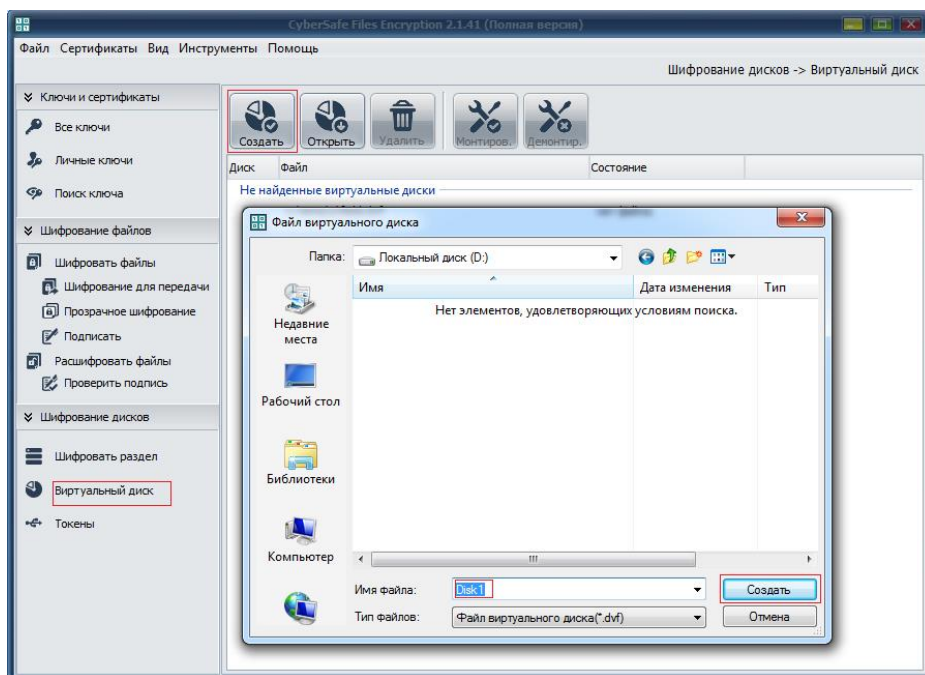
Хранение данных в виде таких томов позволяет легко управлять ими, а также обмениваться с другими пользователями, но, в то же время, приводит к тому, что они могут быть легко утрачены в случае удаления каким-то образом. Поэтому хорошим решением будет хранение резервных копий таких

зашифрованных файлов, благодаря чему ценные данные можно будет восстановить в том случае, если что-то случится с оригинальным файлом.

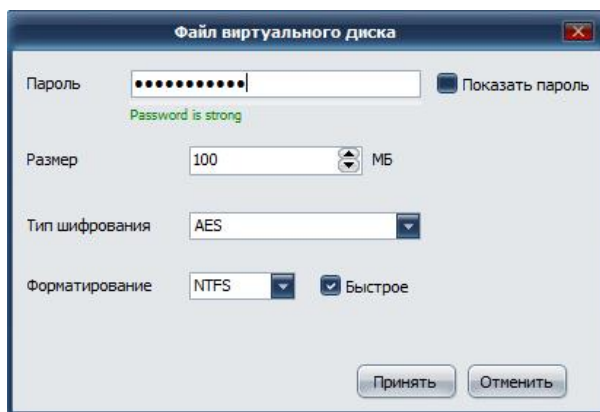
Создание нового виртуального диска

► Для создания нового виртуального диска CyberSafe

- 1 Откройте CyberSafe, перейдите на вкладку **Шифрование дисков**, выберите опцию **Виртуальный диск** и в *Панели опций* нажмите **Создать**. В проводнике Windows укажите путь к папке, в которой будет храниться файл созданного виртуального диска, задайте имя этого файла и нажмите **Создать**:

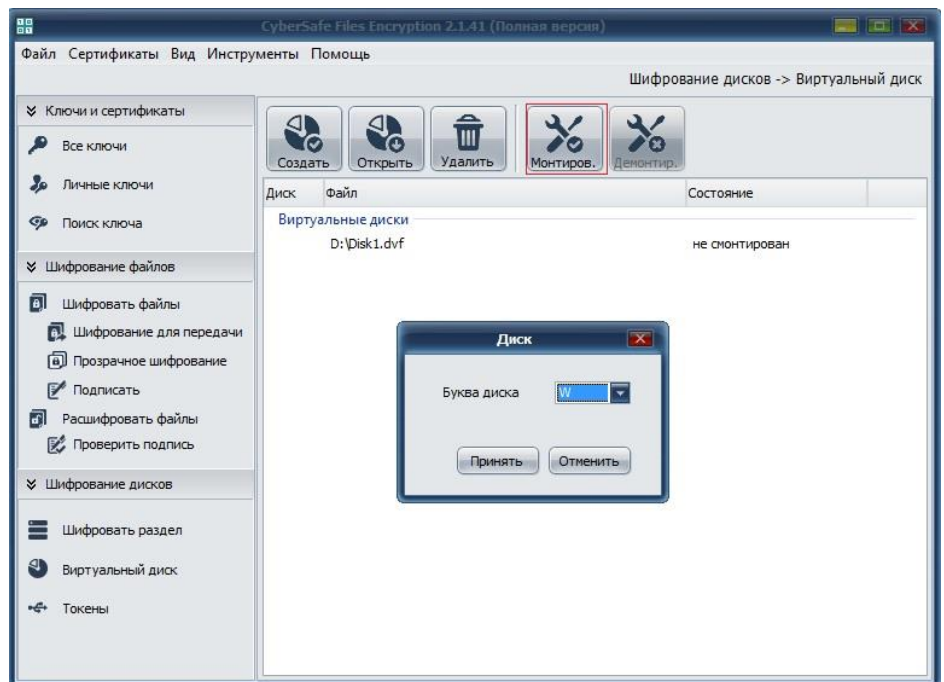


- 2 В открывшемся окне задайте пароль к виртуальному диску, укажите его размер в Мб, выберите алгоритм шифрования и тип файловой системы. Нажмите **Принять**:



Будет создан виртуальный диск, который отобразится в *Рабочей области* в разделе *Виртуальные диски*. Файл криптоконтейнера находится в выбранной ранее папке и имеет расширение *.dvt.

- 3 Для того монтирования виртуального диска выделите его в *Рабочей области* и в *Панели опций* нажмите **Монтировать**. и укажите свободную букву, на которую будет смонтирован этот виртуальный диск, нажмите **Принять**:



В открывшемся диалоговом окне введите пароль к этому виртуальному диску. Диск будет смонтирован в качестве логического диска Windows и доступен для работы.

После завершения работы с диском его необходимо демонтировать при помощи кнопки **Демонтировать** в Панели опций.

Предупреждение. Прежде чем вы демонтируете виртуальный диск, закройте все размещенные на нем файлы и приложения, иначе это может привести к потере данных.

Действия по монтированию и демонтированию повторяются каждый раз при работе с виртуальным диском, поскольку их сокращение или устранение ведет к возникновению серьезной брешки в системе защиты.

До тех пор, пока зашифрованный виртуальный диск не будет смонтирован, все хранящиеся на нем данные являются недоступными. Даже в том случае, если диск окажется в руках злоумышленников, он не может быть смонтированным без знания пароля к нему, а вся хранящаяся на диске информация будет представлять собой не что иное, как совокупность бесполезных байтов.

- 4 Если у вас уже ранее был файл с расширением *.dvh добавить его в CyberSafe можно при помощи кнопки **Открыть** в панели опций.

Использование виртуальных дисков

Создавайте, копируйте, перемещайте и удаляйте файлы и папки на виртуальных дисках CyberSafe точно также, как вы делаете это на ваших системных дисках.

Работа с виртуальными дисками предоставляет возможность использования всех преимуществ функции "шифрование на лету", подразумевающей, что шифрование файлов осуществляется в текущий момент времени, является прозрачным для вас и не требует от вас никаких дополнительных действий.

Под *прозрачностью* подразумевается то, что CyberSafe органично функционирует в вашей операционной системе, предоставляя вам и другим приложениям возможность работать в обычном режиме. При этом все или определенные файлы становятся недоступными для других пользователей или злоумышленников в том случае, если стационарный компьютер, ноутбук или съемный носитель информации будет потерян, украден и т. п.

Другие пользователи, имеющие доступ к виртуальному диску (либо на вашем компьютере, либо по локальной сети) также могут работать с хранящимися на них данными. Это возможно до тех пор, пока вы не демонтируете защищенный том.

Предупреждение. Не смотря на то, что ни к какому из виртуальных дисков CyberSafe нельзя получить доступ без соответствующей авторизации, тем не менее, виртуальный диск можно удалить с вашего компьютера. Любой пользователь, имеющий доступ к вашей системе может удалить зашифрованный файл виртуального диска. По этой причине необходимо иметь резервную копию зашифрованного файла, а также держать свой компьютер заблокированным тогда, когда вы не работаете за ним.

Работа с виртуальным диском CyberSafe подразумевает обязательное его *монтирование* в качестве логического диска Windows в начале работы и *демонтирование* (отключение) после завершения работы с этим диском.

Удаление виртуального диска

По какой-то причине вы можете решить, что вам больше не нужен один из виртуальных дисков CyberSafe и захотеть удалить его совсем.

Предупреждение. Удаление виртуального диска CyberSafe , ведет к удалению всех хранящихся на нем данных. Как только диск будет удален, восстановить данные с него будет невозможно. Убедитесь, что вы скопировали все данные с этого диска, которые должны быть сохранены в другое место.

► Для удаления виртуального диска

- 1 Откройте CyberSafe на вкладке **CyberSafe** и в *Списке крипто-дисков* выберите диск, который нужно удалить.
- 2 В *Панели опций* выберите **Удалить диск**. В открывшемся диалоговом окне, запрашивающем подтверждение на удаление, нажмите **Да**.
- 3 Виртуальный диск удален.

Особые меры безопасности, предпринимаемые CyberSafe

CyberSafe имеет в своем наборе функции, помогающие избежать проблем, связанных с шифрованием дисков и их использованием. Это относится также и к зашифрованным виртуальным дискам.

Стирание пароля

Когда вы вводите свой пароль, CyberSafe использует его лишь в течении короткого промежутка времени, а затем стирает из памяти. CyberSafe также не допускает создания копий пароля. В результате пароль пребывает в памяти лишь доли секунды.

Без этой чрезвычайно важной функции, при желании кто-то может найти ваш пароль в памяти компьютера в то время, когда вы отсутствуете. Вы даже не будете знать об этом, а злоумышленник в результате получит полный доступ ко всем вашим данным, защищенным при помощи этого пароля.

Защита виртуальной памяти

Может произойти так, что ваш пароль или другие ключи будут записаны на диск как часть виртуальной памяти системы. CyberSafe заботится о том, чтобы этого никогда не случилось. Эта функция не позволит потенциальному злоумышленнику проверить виртуальную память на наличие пароля.

Защита ключа шифрования

Когда вы защищаете диск или его раздел при помощи CyberSafe , ваш пароль превращается в ключ, который используется для шифрования. В то время, как

пароль стирается из памяти компьютера немедленно, ключ (из которого пароль получить невозможно) остается в памяти.

Этот ключ не может быть получен из виртуальной памяти. Однако если определенные участки памяти хранят одни и те же данные на протяжении очень длительного периода времени без выключения или перезагрузки, память имеет свойство сохранять статический заряд, который могут прочесть злоумышленники.

Если зашифрованный диск или его раздел расшифровывается в течении продолжительного периода, в памяти сохраняются следы вашего ключа, которые могут быть обнаружены. Существуют специальные устройства, которые способны восстанавливать ключи по этим следам. Вы не найдете их в ближайшем магазине электроники, однако они имеются в некоторых правительственных организациях.

CyberSafe защищает ваш ключ от подобных устройств тем, что держит в оперативной памяти две копии ключа – одну исходную, а вторую бит-инвертированную и инвертирует обе копии каждые несколько секунд.

Другие меры безопасности

В основном, защита ваших данных зависит от вас и тех мер безопасности, которые вы принимаете. Ни одна программа для шифрования данных не сможет защитить информацию, к которой относятся небрежно. К примеру, если вы оставите свой компьютер включенным и без присмотра, кто угодно сможет получить доступ к вашей информации, если она храниться на зашифрованном диске (не виртуальном).

Вот несколько советов, которые помогут вам в обеспечении безопасности:

- Когда вы отлучаетесь от своего компьютера, используйте экранную заставку с паролем для того, чтобы не позволить другим получить доступ к вашему компьютеру или изучить его экран.
Также демонтируйте в этом случае все виртуальные диски CyberSafe . Тогда вся информация, содержащаяся в зашифрованном файле диска будет защищена до тех пор, пока вы снова не начнете с ней работать.
- Убедитесь, что зашифрованные диски их разделы или виртуальные диски не доступны для других компьютеров по локальной сети. Как только вы разблокировали ваш зашифрованный диск, CyberSafe больше не сможет защитить хранящиеся на нем файлы и их смогут увидеть все пользователи, имеющие доступ к вашему компьютеру по локальной сети.
Подумайте об использовании виртуальных зашифрованных дисков для хранения ценных данных, которые остаются зашифрованными даже тогда, когда вы работаете со всей остальной системой.
- Никогда не записывайте свой пароль. Выберите ту комбинацию символов, которую вы сможете запомнить.

Если вы делите свой компьютер с другими пользователями, они, вероятно, смогут увидеть хранящиеся на зашифрованном диске файлы, которые вы открыли. Но если компьютер будет перезагружен, а съемный жесткий диск будет отключен от компьютера, данные, хранящиеся на таких зашифрованных дисках будут полностью защищены.

11

Скрытие информации при помощи CyberSafe

CyberSafe имеет функцию по скрытию файлов, папок и логических дисков на компьютере пользователя, которая выступает в качестве дополнительной меры защиты информации совместно с шифрованием.

В этой главе

О скрытии информации на ПК.....	81
Скрытие файлов и папок.....	82
Скрытие логических дисков.....	83

О скрытии информации на ПК

Одним из способов защиты данных на компьютере является скрытие файлов, а также папок, в которых они находятся. Необходимость спрятать файлы и папки может возникнуть по множеству причин. Кому-то нужно просто скрыть от посторонних глаз личное видео или фотографии, а кому-то таким образом защитить свою конфиденциальную информацию - важные текстовые файлы, пароли, номера телефонов и т. д. Нередко возникает необходимость в том, чтобы спрятать целые директории, в которых содержатся десятки и сотни файлов. Суть этого метода проста – если скрытые данные не будут обнаружены, значит, никто не сможет получить к ним доступ.

Для того чтобы скрыть файлы и папки существует огромное количество способов и все они имеют разную степень эффективности, начиная от самых примитивных и заканчивая достаточно сложными и более ли менее полезными.

CyberSafe в своей работе использует одну из передовых технологий, основанную на использовании специального драйвера. Скрытые файлы остаются невидимыми даже при загрузке компьютера в безопасном режиме, во время его просмотра при помощи средств дистанционного администрирования, таких как Radmin или TeamViewer, а также в случае деинсталляции CyberSafe с компьютера.

Кроме того, разработчики CyberSafe прекрасно понимают, что для надежной защиты информации просто скрыть файлы и папки недостаточно – ни один из существующих методов скрытия не способен обеспечить их абсолютную защиту. Поэтому, для защиты данных CyberSafe использует не только скрытие, но и шифрование.

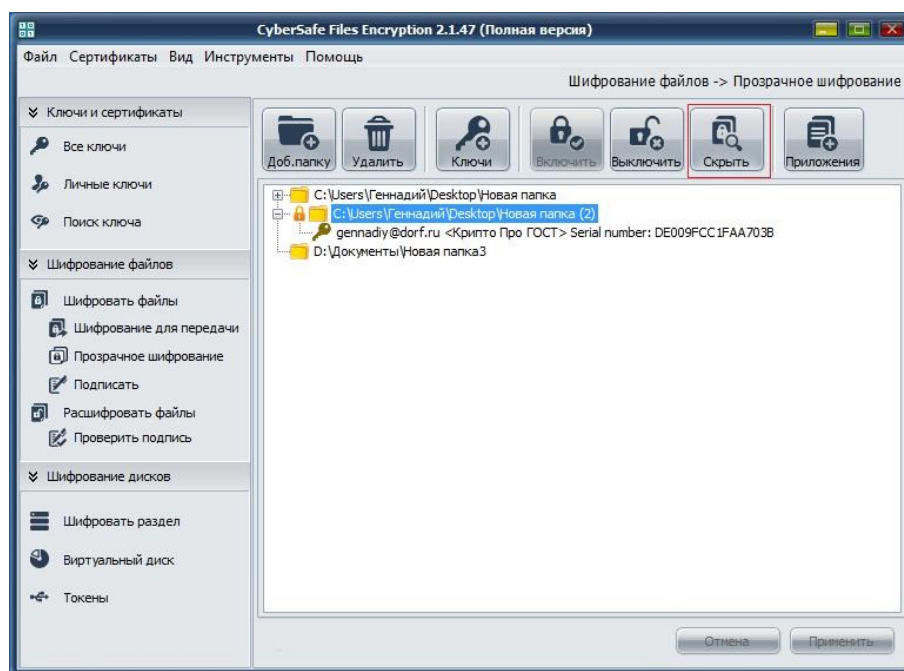
В простом шифровании также есть свой недостаток - зашифрованные файлы привлекают к себе ненужное внимание. И даже если взломать их невозможно, доступ к секретной информации можно получить другим путем, к примеру – тем или иным способом завладеть ключом для дешифрования. И лишь только совместное использование шифрования и скрытия позволяет добиться максимального уровня защиты информации. Именно так и работает CyberSafe.

Скрытие файлов и папок

Данная функция применяется для скрытия папок, защищенных при помощи функции *прозрачного шифрования*. Все файлы, размещенные в такой папке, также скрываются.

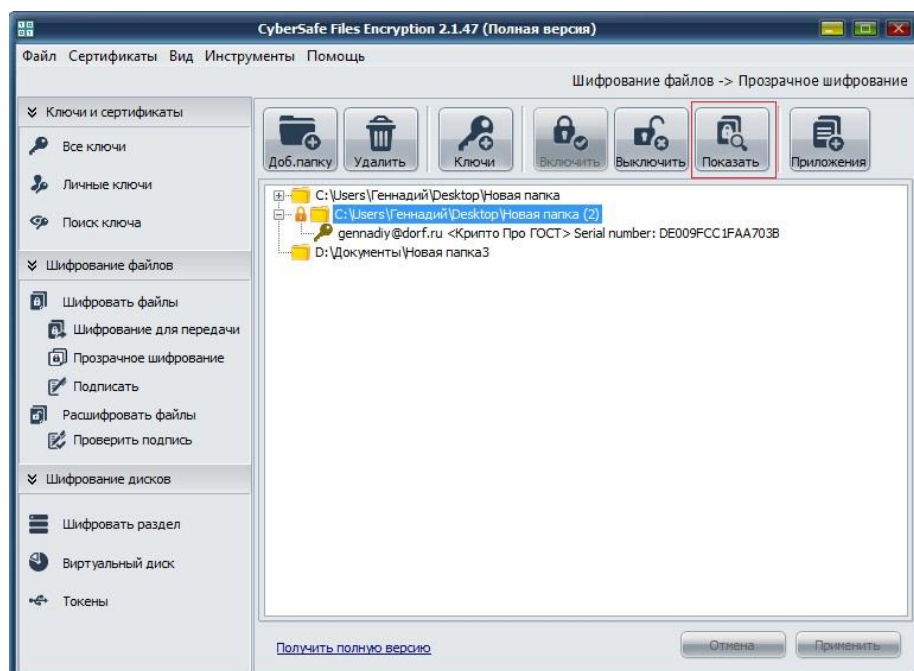
► Для скрытия папки при помощи CyberSafe:

- 1 Откройте программу CyberSafe и выберите **Шифрование файлов > Прозрачное шифрование**.
- 2 В *Рабочей области* выберите папку, которая должна быть скрыта и в панели опций нажмите **Скрыть**.



После этого папка и все содержащиеся в ней файлы скрыты от операционной системы, но она по-прежнему отображается в CyberSafe.

- 3 Для того, чтобы папка снова стала видимой для операционной системы, выделите ее и нажмите **Показать**.



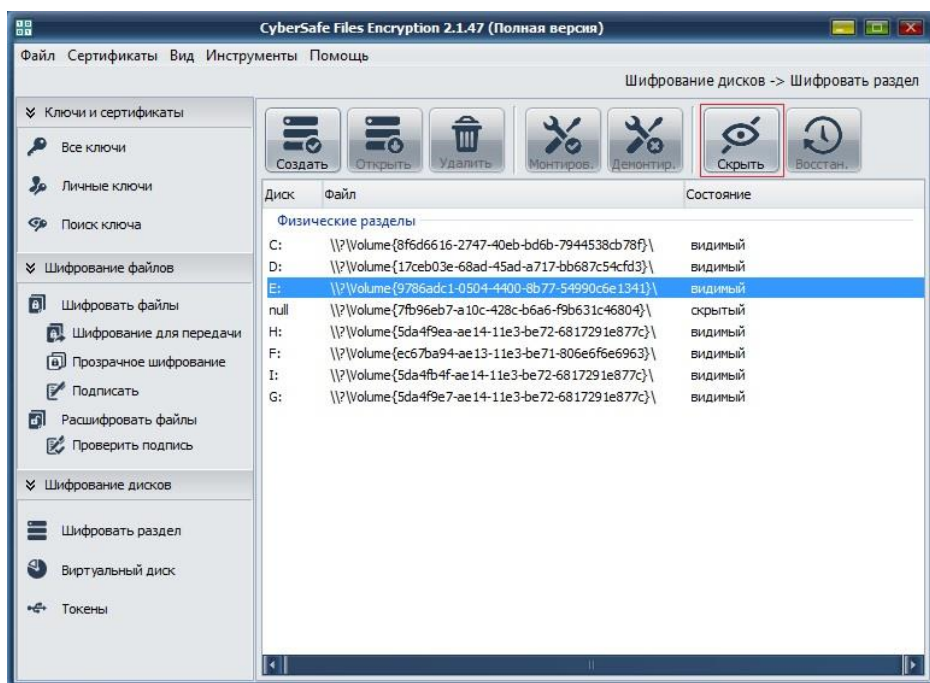
Папка и все содержащиеся в ней файлы снова видны в операционной системе.

Скрытие логических дисков

Данная функция может применяться для всех логических дисков, имеющих на вашем ПК (кроме системного). Могут скрываться как обычные логические диски, так и диски, зашифрованные при помощи CyberSafe.

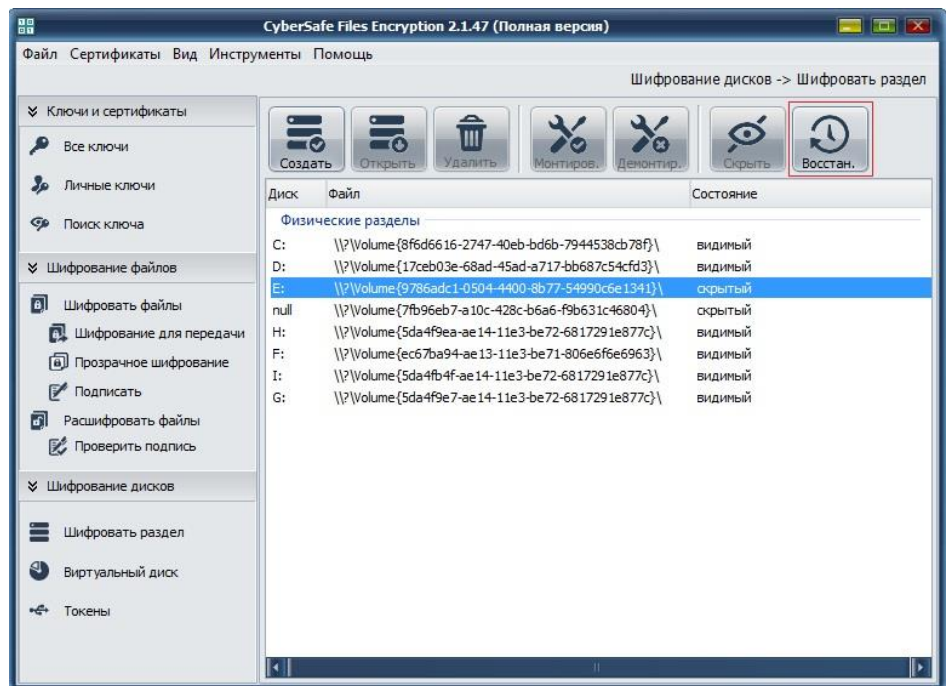
► Для скрyтия логического диска:

- 1 Откройте программу CyberSafe и выберите **Шифрование дисков > шифровать раздел**.
- 2 В списке отображаемых физических разделов выберите незашифрованный раздел, который хотите скрыть и в *Панели опций* нажмите **Скрыть**:



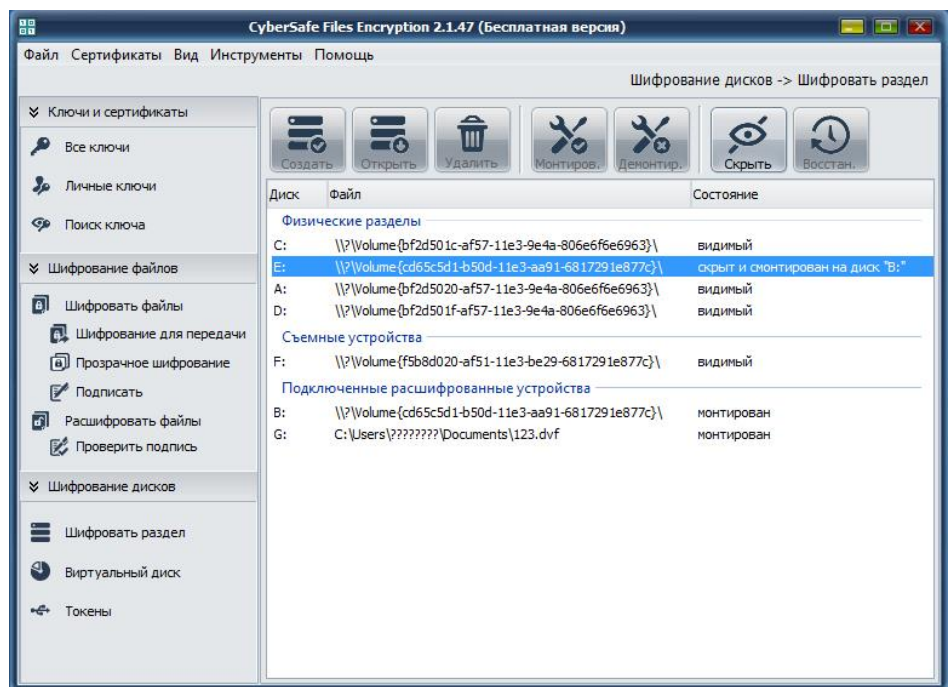
Выбранный диск и вся хранящаяся на нем информация скрыты от операционной системы, но он по-прежнему отображается в CyberSafe.

- 3 Для того, чтобы скрытый логический диск снова был виден для операционной системы выделите его в *Рабочей области программы* и в *Панели опций* нажмите **Восстановить**:



Логический диск снова отображается в операционной системе.

- 4 В том случае, если диск зашифрован в CyberSafe, его скрытие осуществляется программой автоматически после монтирования в качестве логического диска Windows свободную букву:



После демонтирования диска в CyberSafe, он снова отображается в операционной системе под прежней буквой.

Предупреждение. Ни один из существующих методов скрытия информации, в том числе и используемых в CyberSafe, не обеспечивает сто процентную защиту ваших данных. Поэтому, для максимальной защиты конфиденциальных файлов функцию скрытия необходимо использовать совместно с шифрованием.

12 Шифрование ключами КриптоПРО CSP

CyberSafe предоставляет возможность шифрования информации при помощи сертифицированного в России криптопровайдера КриптоПРО CSP, что позволяет использовать программу для защиты информации в государственных учреждениях и других организациях, осуществляющих обработку сведений, составляющих государственную тайну.

В этой главе

О криптопровайдере КриптоПро CSP.....	85
Шифрование файлов при помощи криптопровайдера КриптоПро CSP	86

О криптопровайдере КриптоПРО CSP

КриптоПро — линейка криптографических утилит (криптопровайдеров), которые используются для шифрования файлов, генерации электронно-цифровой подписи (ЭЦП), работы с сертификатами, организации структуры PKI и др.

Средство криптографической защиты КриптоПро CSP разработано по согласованному с ФАПСИ техническому заданию в соответствии с криптографическим интерфейсом фирмы Microsoft — Cryptographic Service Provider (CSP). КриптоПро CSP имеет сертификаты соответствия ФАПСИ и может использоваться для:

- авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной цифровой подписи (ЭЦП) в соответствии с отечественными стандартами ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012;
- обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89;
- обеспечения аутентичности, конфиденциальности и имитозащиты соединений по протоколу TLS;
- контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования;
- управления ключевыми элементами системы в соответствии с регламентом средств защиты.

Реализуемые алгоритмы

- Алгоритм выработки значения хэш-функции реализован в соответствии с требованиями ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012 "Информационная технология. Криптографическая защита информации. Функция хэширования".
- Алгоритмы формирования и проверки ЭЦП реализованы в соответствии с требованиями ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".

- Алгоритмы шифрования/расшифрования данных и вычисление имитовставки реализованы в соответствии с требованиями ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая".

При генерации закрытых и открытых ключей обеспечена возможность генерации с различными параметрами в соответствии ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012.

При выработке значения хэш-функции и шифровании обеспечена возможность использования различных узлов замены в соответствии с ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012 и ГОСТ 28147-89.

Шифрование файлов при помощи криптопровайдера КriptoPRO CSP

Программа CyberSafe полностью совместима с криптопровайдером КriptoPRO CSP и поддерживает шифрование данных по алгоритму ГОСТ 28147-89, что позволяет использовать программу в государственных учреждениях и других структурах, осуществляющих обработку сведений, составляющих государственную тайну.

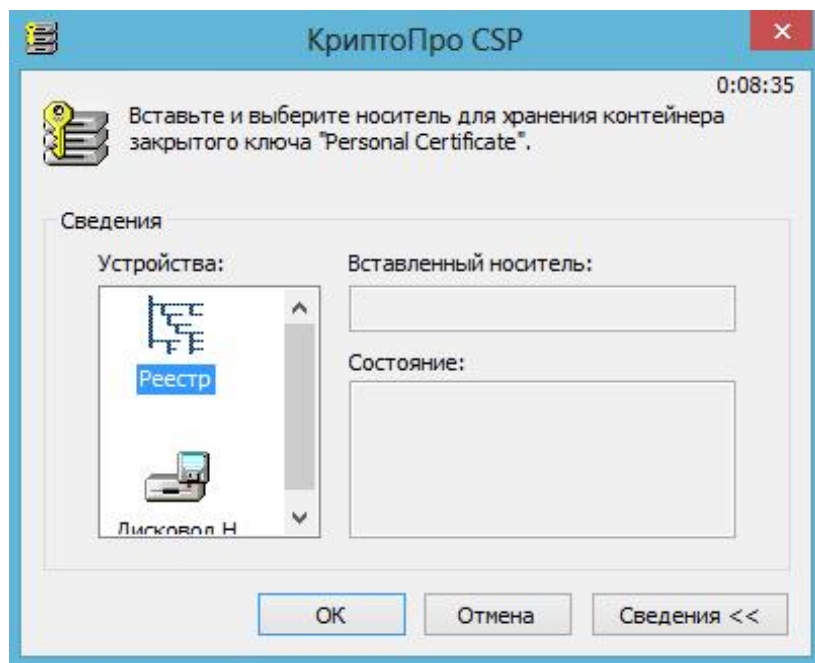
Создание сертификата КriptoPRO

► Для установки сертификата КriptoPRO CSP в CyberSafe:

- 1 Скачайте программу КriptoPRO CSP с официального сайта разработчика (<http://www.cryptopro.ru>) соответствующую типу вашей операционной системы и установите ее на свой компьютер.
- 2 После установки программы при создании сертификата в CyberSafe появится возможность создать сертификат КriptoPRO:

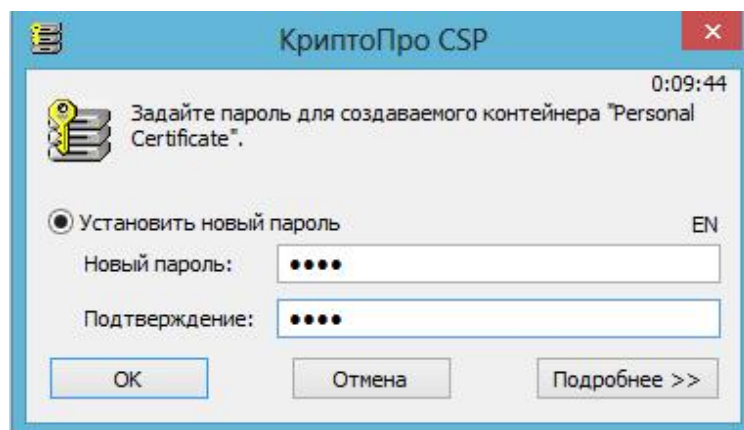
- 3 Нажмите **Далее**. В открывшемся диалоговом окне КriptoPRO CSP укажите место хранения контейнера закрытого ключа КriptoPRO. Как правило, для этого используется реестр операционной системы Windows

(однако также может быть использован съемный носитель, например токен).



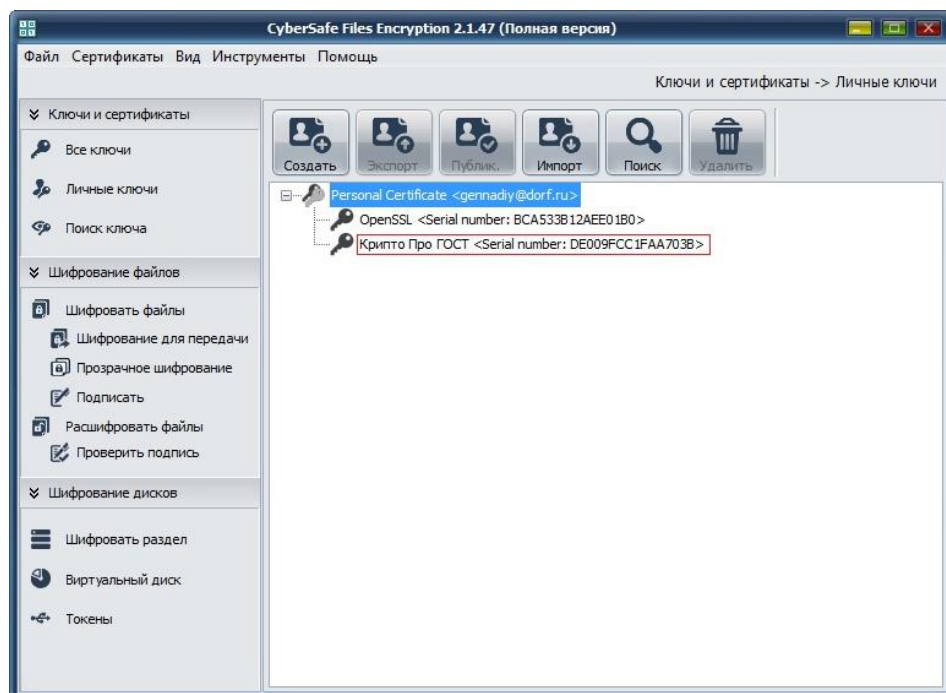
После выбора устройства нажмите **ОК**.

- 4 В следующем диалоговом окне КриптоПРО CSP задайте пароль для создаваемого контейнера с закрытым ключом:



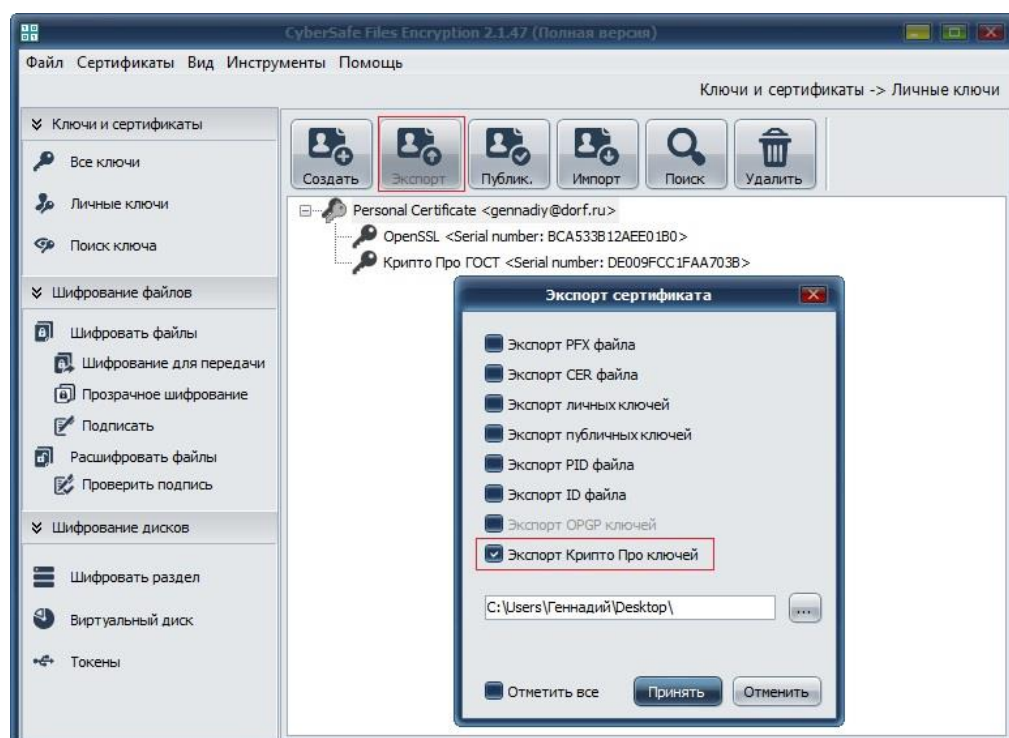
Нажмите **ОК**.

- 5 После завершения создания сертификата CyberSafe ключи КриптоПРО CSP также созданы, отображаются на вашей связке и доступны для использования:



Экспорт Крипто ПРО ключей в файл

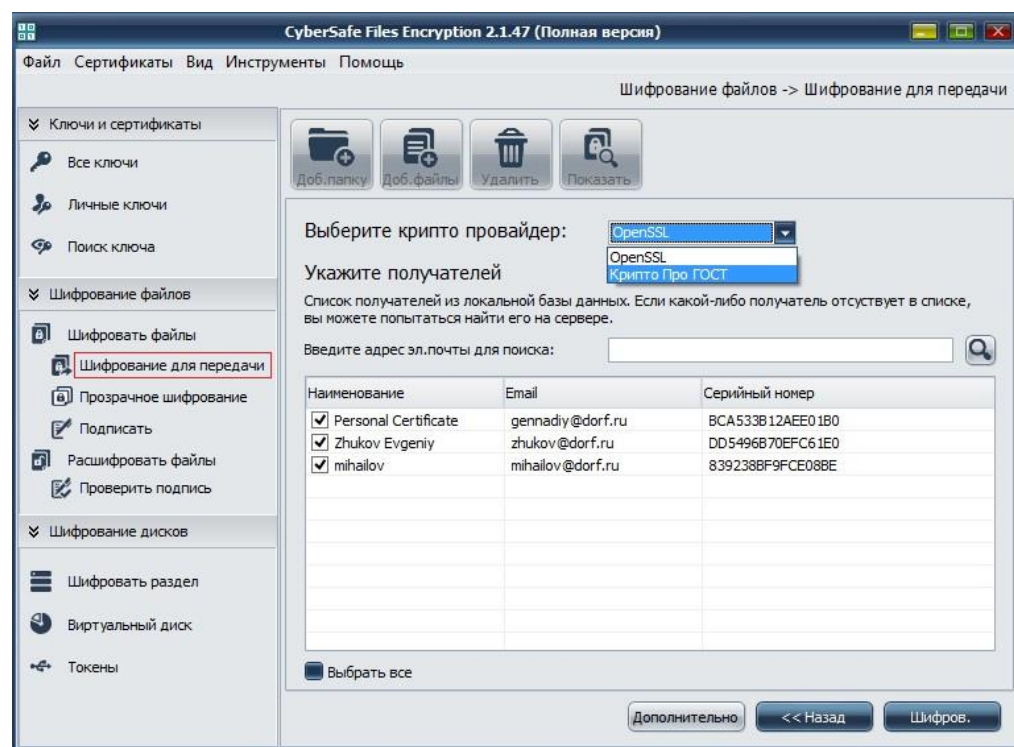
В том случае, если вы хотите экспортировать ключи КриптоПРО в отдельный файл, к примеру, для их резервного копирования, это можно сделать через стандартную функцию экспорта ключей CyberSafe, установив галочку в чекбоксе **Экспорт КриптоПРО ключей**:



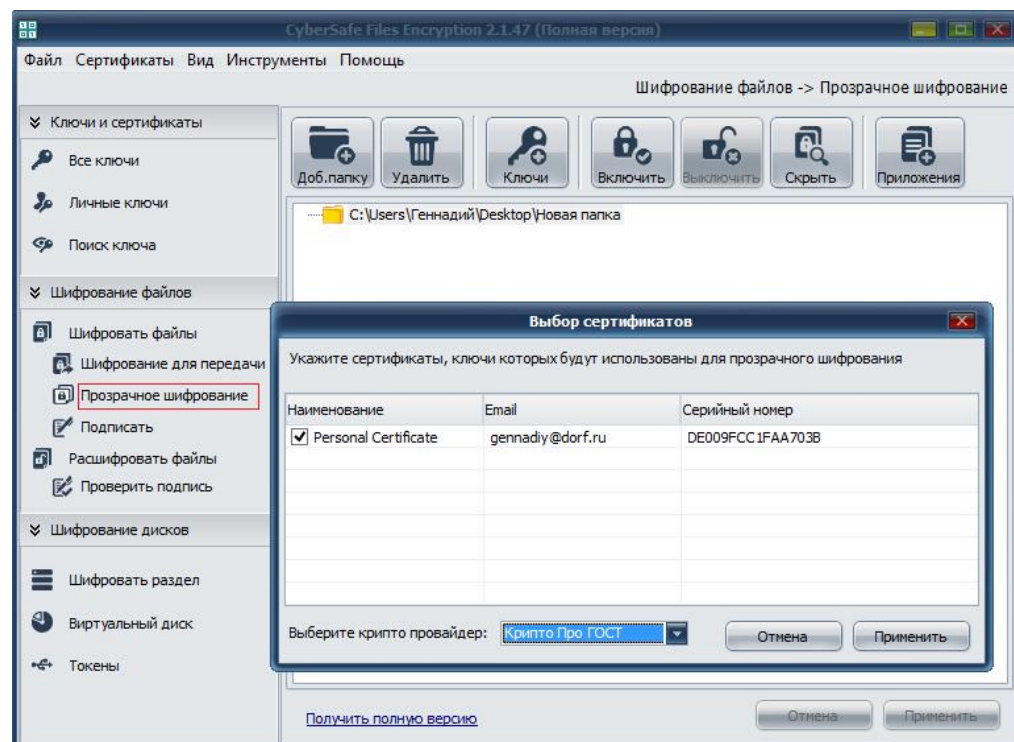
Шифрование файлов и цифровая подпись ключами Крипто ПРО

	Общий алгоритм шифрования файлов описан в разделе <i>Шифрование файлов при помощи CyberSafe</i>. В том случае, если вы хотите зашифровать файлы для передачи другим пользователям (или подписать их своей цифровой подписью) и использовать
--	---

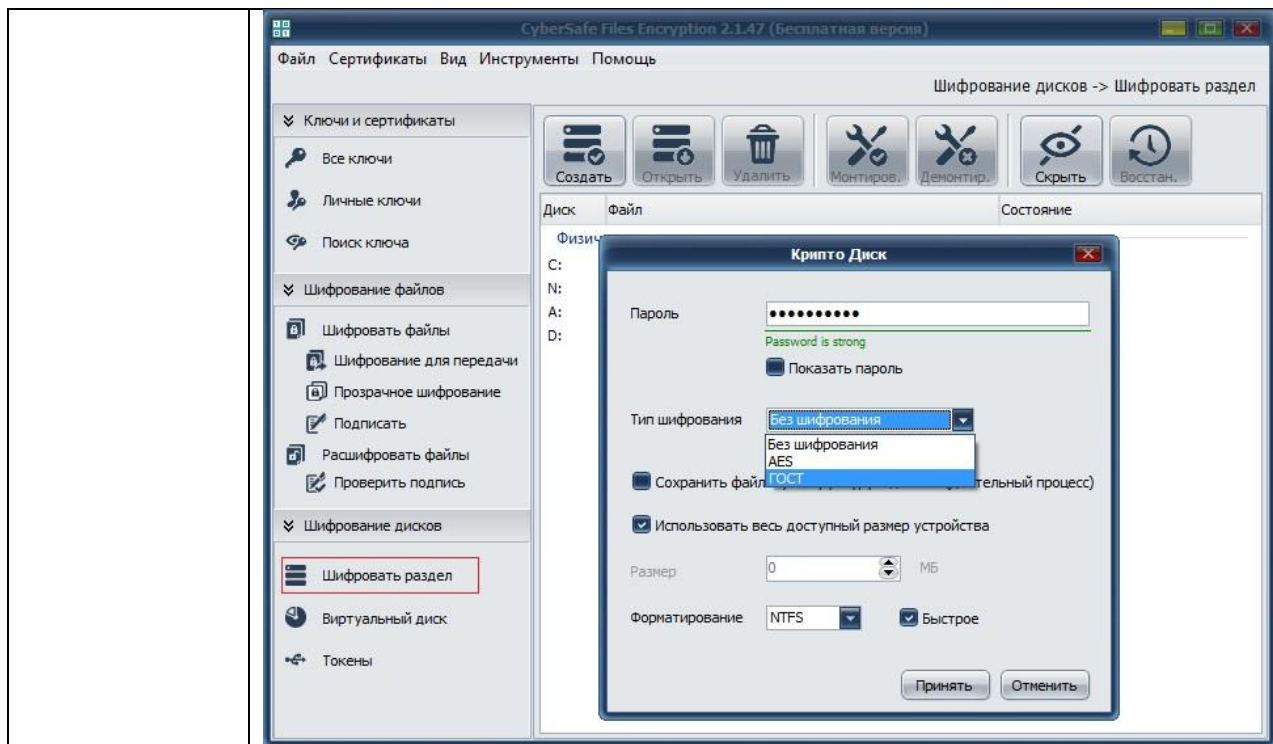
для этого ключи КристоПРО, из списка доступных криптопровайдеров необходимо выбрать КристоПРО ГОСТ:



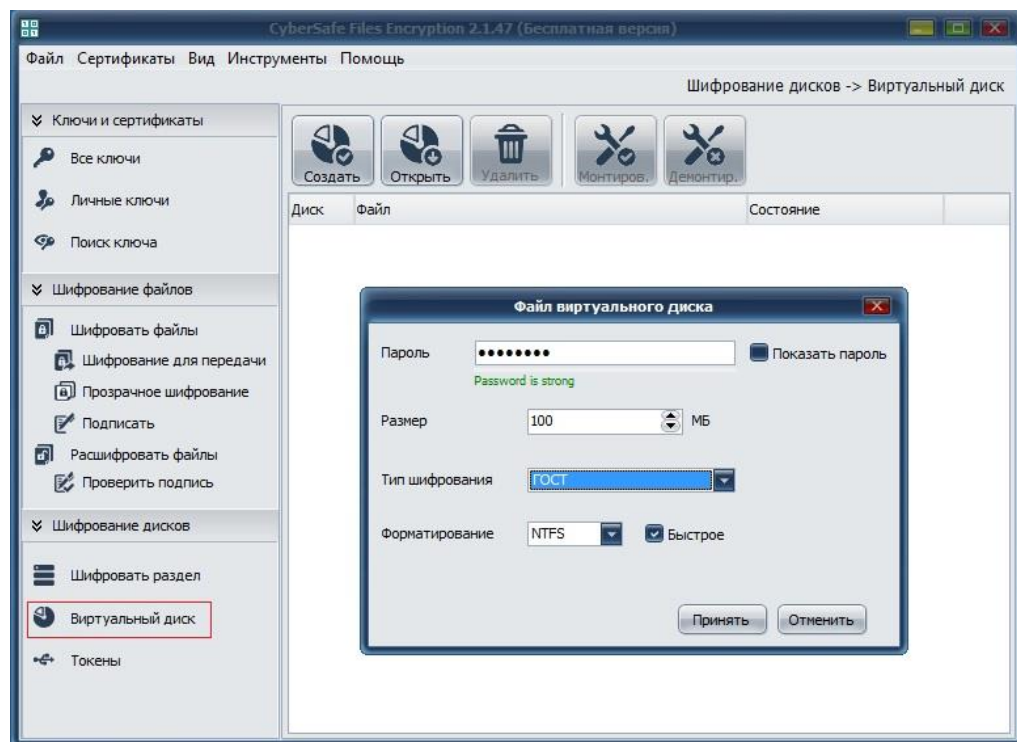
В том случае, если вы хотите использовать ключи КристоПРО для прозрачного шифрования файлов, в окне выбора сертификатов в качестве криптопровайдера также следует выбрать КристоПРО ГОСТ:



В том случае, если вы хотите использовать криптопровайдер КристоПРО для шифрования логического диска (или его раздела), при создании криптодиска следует выбрать алгоритм шифрования ГОСТ:



Ключи КриптоПро и алгоритм ГОСТ также может быть использованы и при создании виртуальных зашифрованных дисков:



При использовании криптопровайдера Крипто ПРО файлы будут зашифрованы при помощи алгоритма шифрования ГОСТ 28147-89, а для создания электронно-цифровой подписи будет использован алгоритм ГОСТ 34.10-2001.

13 Работа с паролями и ключевыми фразами

Пароли и ключевые фразы используются для защиты данных. Как правило, ключевые фразы длиннее и содержат более широкий диапазон символов по сравнению с паролями.

Например, простой пароль может представлять собой объединение двух слов из четырех букв: "whenjobs" без кавычек. Более надежные пароли могут содержать символы верхнего регистра, например: "WhenJobs". Еще более надежный пароль может включать в себя цифры: "When9Jobs4".

Ключевые фразы, по сравнению с паролями, более длинные и включают в себя более широкое разнообразие символов. Например, простая ключевая фраза может выглядеть так: "Mb&1a>tta" без кавычек. Эта ключевая фраза может показаться трудной для запоминания, но в действительности она основывается на простой фразе, запомнить которую намного проще.

Ключевые фразы также могут состоять из простых фраз, например, из любимой книги, включая знаки препинания и заглавные буквы: "Because that's not golf, I replied" включая кавычки. Не смотря на то, что эта ключевая фраза выглядит не очень надежной, на самом деле она как минимум в два раза надежнее, чем любой из примеров, приведенных выше.

В этом разделе описываются различия между паролями и ключевыми фразами, рассказывается об Индикаторе надежности пароля, используемого в CyberSafe , а также дается несколько рекомендаций по созданию надежных паролей.

В этой главе

Что использовать: пароль или ключевую фразу?	90
Индикатор надежности пароля	91
Создание надежных паролей	91

Что использовать: пароль или ключевую фразу?

Итак, знаете ли вы что выбрать для защиты своих данных: пароль или ключевую фразу? Все зависит от того, что вы пытаетесь защитить. Чем более ценна защищаемая информация, тем более сильной должна быть защита.

Большая часть документов по всему миру не защищена вовсе; информация, содержащаяся в них, не настолько ценна и ее защита не оправдывает подобных усилий. Когда вы получаете доступ к онлайн-банкингу, некоторые банки требуют ввод PIN, состоящего всего из четырех символов. В зависимости от суммы денег на счете, это может оказаться очень слабой защитой. Вы можете использовать аккаунт на сервисе почтовых ящиков Hotmail для корреспонденции, не представляющей никакой ценности, и простого пароля в данном случае будет вполне достаточно.

В CyberSafe , например, вы создаете пароль как для ключевой пары, так и для виртуальных дисков. Если вы создадите слабый пароль для вашей ключевой пары и злоумышленникам удастся заполучить ваш закрытый ключ, все что им потребуется - это читать ваши сообщения, а также отправлять сообщения от вашего имени чтобы выяснить ваш пароль.

Индикатор надежности пароля

Когда вы создаете пароль в CyberSafe , Индикатор надежности пароля является основным ориентиром, позволяющим оценить, насколько силен создаваемый вами пароль. Он работает намного лучше, чем простой подсчет количества символов.

В основном, чем больше заполнена шкала оценки надежности пароля, тем он надежнее. Однако, что же в действительности означает длина этой шкалы? Индикатор надежности пароля сравнивает значение случайных величин (энтропии) в пароле с настоящей 128-битной случайной последовательностью (то же значение энтропии, что и в ключе AES128). Это называется 128-битной энтропией. (Энтропия – величина, при помощи которой измеряется сложность взлома пароля или ключа).

Таким образом, если вы создали пароль, при котором Индикатор надежности заполнен приблизительно на половину, это означает, что он имеет приблизительно 64 бита энтропии. А если вы создали пароль, при котором Индикатор надежности заполнился полностью, это означает, что он имеет приблизительно 128 бит энтропии.

Однако, насколько же силен пароль, обладающий 128 битами энтропии? В конце 1990-х были созданы специальные компьютеры “DES-взломщики”, которые могли получить DES-ключ за несколько часов, перебирая все возможные значения ключей.

Если предположить, что кто-либо сможет создать компьютер, способный подбирать DES-ключ не за несколько часов, а за одну секунду (в секунду он должен будет обрабатывать 255 ключей), тогда на то, чтобы взломать 128-битный AES ключ уйдет около 149 триллионов (тысяча миллиардов) лет. Для сравнения: считается, что наша Вселенная возникла менее чем 20 миллиардов лет назад.

Как влияют на энтропию определенные символы? Чем более обширен диапазон символов, входящих в состав пароля, тем большей будет его энтропия. Например, если вам нужно составить PIN-код из одних лишь цифр, то это означает, что вы можете использовать лишь 10 символов. Это очень маленький диапазон и, поэтому, энтропия всех символов вместе будет крайне низкой.

Однако, если вы используете англоязычную версию CyberSafe , все обстоит иначе. У вас в распоряжении имеется три набора символов, из которых можно выбрать: буквы верхнего и нижнего регистров (52 символа), цифры от нуля до девяти (10 символов), а также знаки препинания (32 символа). Когда вы вводите один из этих символов, CyberSafe определяет для него значение энтропии, основываясь на том диапазоне, из которого он выбран и отображает его на шкале, которая показывает надежность пароля.

То же самое относится и к символам на других языках – чем больше диапазон, тем больше энтропии на символ.

Создание надежных паролей

Хороший пароль представляет собой оптимальное соотношение между легкостью в использовании и своей надежностью. Длинные пароли, в состав которых входят символы верхнего и нижнего регистров, цифры и знаки препинания сильнее, но, в то же время, они более сложны для запоминания.

Практика показывает, что пароли, которые трудно запоминаются, очень часто записываются, что полностью противоречит надежности такого пароля.

Намного лучше иметь более короткий пароль, который вы будете держать в голове, чем более длинный, который вы запишете или, еще хуже, забудете. Общий алгоритм по созданию сильных паролей состоит в том, что за основу берется какая-то фраза и эта фраза потом сводится к набору отдельных символов. Например, фраза:

My brother and I are greater together than apart

становится ключевой фразой:

Mb&1a>ttA

В эту ключевую фразу входит 10 символов, встречаются буквы верхнего и нижнего регистров, цифры, а также знаки пунктуации. 10 символов – это относительно короткая ключевая фраза. Если вы считаете, что этого не достаточно, подумайте над другой ключевой фразой, используя тот же метод и объедините ее с уже существующей.

Другой подход к использованию легко запоминающихся паролей подразумевает использование знаков пунктуации и заглавных букв

Например:

Edited by John Doe (not John Doe, Editor)

Эта фраза не очень длинна и сложна для запоминания, но, тем не менее, она сильна. Если вы решите использовать фразу из какой-то имеющейся у вас книги, постарайтесь не потерять саму книгу.

Еще один подход заключается в том, чтобы объединять множество коротких знакомых вам слов. Этот подход называется Diceware. В нем используются кости для случайного подбора слов из специального списка, называемого Diceware Word List, который состоит из 7776 коротких английских слов, аббревиатур и легко запоминающихся символьных строк. Если вы соберете вместе достаточное количество таких коротких слов, вы сможете создать сильный пароль. В FAQ создатели Diceware утверждают, что вы можете достичь 128 бит энтропии используя 10 слов из их списка для составления своей ключевой фразы.

Для получения более подробной информации о Diceware, посетите домашнюю страницу этого сервиса (<http://world.std.com/~reinhold/diceware.html>).

Когда дело доходит до создания пароля, вот несколько вещей, которые вам следует сделать:

- Используйте фразы, которые находятся в вашей долговременной памяти. Вероятность того, что вы их забудете, намного меньше.
- Создайте пароль длиной не менее восьми символов. Длина пароля – далеко не самый главный показатель его надежности, но все-же он не должен быть коротким.
- Используйте в своем пароле сочетание символов верхнего и нижнего регистра, цифры и знаки пунктуации.

Предупреждение. Постарайтесь использовать лишь символы ASCII, если это возможно. Это особенно важно при использовании иностранных клавиатур, в которых некоторые специальные символы в паролях не поддерживаются (например, символ “§”).

- Периодически меняйте свой пароль, лучше всего делать это один раз в три месяца. Чем дольше вы используете один и тот же пароль, тем больше вероятность того, что кто-то его узнает.

Вот некоторые вещи, которые вы не должны делать при создании паролей:

- Не записывайте свой пароль или ключевую фразу.
- Не сообщайте ваш пароль никому.
- Не разрешайте никому смотреть, как вы вводите свой пароль.
- Не используйте шаблоны, такие как “abcdefgh” или “12345678” или “qwertyui” или “88888888” или “AAAAAAA.”
- Не используйте обычные слова. Практически каждый опытный хакер использует программу для взлома паролей, основывающуюся на словарях. Не объединяйте два обычных слова вместе, не используйте множественное число обычных слов, не используйте в обычных словах заглавную букву первой.
- Не используйте цифры, которые имеют к вам какое-то отношение. Если кому либо известны эти цифры, злоумышленник также может их узнать. Не используйте даты своего рождения, номер телефона, номер страховки или адрес и т. д.
- Не используйте имена. Ни имена людей, не имена вымышленных персонажей, ни имена домашних животных. Не используйте даже

название того места, где вы отдыхали прошлой зимой, свой логин или название своей компании. Не используйте название своей любимой спортивной команды, имя из любой из книг, особенно из Библии.

- Не используйте слова, написанные с заду на перед или слова, каждая буква которых чередуется с цифрой.