



ПЕРЕДМОВА

Випуск дайджесту присвячено проблемам збереження електронних інформаційних ресурсів та обладнанню для мікрофільмування.

У публікації «Роб Шарп: В защиту миграции» розповідається про погляди прихильників і противників міграції електронних матеріалів.

У публікації «Флэшки в 2 раза опаснее, чем вы думаете» розповідається про ризики використання незахищених USB-накопичувачів.

У публікації «Как продлить жизнь «флэшкам»» розповідається про типові для USB-накопичувачів несправності, дано кілька порад, які допоможуть знизити ризик їх поломки.

У публікації «Как защитить и сохранить данные на портативном носителе» розповідається як захистити дані на жорстких дисках встановлених на ПК і ноутбуках, зовнішніх накопичувачах.

У публікації «Надежно ли хранение данных на CD/DVD дисках?» розповідається про критерії "якості" для CD / DVD дисків.

У публікації «Микрографическая камера УКМ-3» наведені опис, технічні характеристики і комплектація мікрографічної камери УКМ-3.

У публікації «Универсальный сканер микрофильмов 16/35 и микрофиш А6 Imagelink 2400/3000 DV Plus» наведені опис і технічні характеристики сканера Imagelink 2400/3000 DV Plus.

У публікації «Поточный сканер СКАМАКС 2000/3000» наведені опис і технічні характеристики потокового сканера СКАМАКС 2000 / 3000.

У публікації «Промышленный сканер Скамакс 5000М» наведені опис і технічні характеристики промислового сканера ЕЛАР СКАМАКС 5000М.

У публікації «Читальный аппарат MicroVue RF 35» наведені опис і технічні характеристики читального апарату для перегляду мікрофільмів 35 мм MicroVue RF 35.

У публікації «Exttek 3150 Silver Duplicator» наведені опис, технічні характеристики і комплектація високошвидкісного дублюатора Exttek 3150.

У публікації «Просмотровый стол Solar для 16/35 мм микроплёнки» наведені опис і технічні характеристики переглядового столу Solar.

У публікації «Микроскоп MESSWELK» наведені опис і технічні характеристики переносного вимірювального мікроскопа MESSWELK - 75х.

У публікації «Сенситометр Wejex 1S» наведені опис і технічні характеристики сенситометра Wejex 1S.

У публікації «Цифровой денситометр X-Rite 301» наведені особливості і технічні характеристики цифрового денситометра X-Rite 301.

У публікації «Пункт водоподготовки ЭЛАР» наведено опис пункту водопідготовки для проявних машин.



РОБ ШАРП: В ЗАЩИТУ МИГРАЦИИ

Источник: http://rusrim.blogspot.com/2014/10/blog-post_8.html

В кругах специалистов по обеспечению долговременной сохранности электронных материалов (электронной сохранности) есть тенденция ставить под сомнение необходимость миграции. Сторонники этой точки зрения формулируют свои аргументы слегка по-разному, однако, в сущности, их позиция сводится к тому, что существует (и будет продолжать существовать) программное обеспечение, способное читать (и выполнять необходимые функции, например, отображать) старые форматы, и поэтому они считают, что в миграции нет необходимости. Я раньше полагал, что эту точку зрения разделяет меньшинство, однако на недавнем семинаре стало очевидно, что она поддерживается многими. *(Со своей стороны я бы отметила следующее: миграция требует знаний и ресурсов, и, соответственно, является затратным процессом. Интересно, что ряды сторонников миграции начали редеть одновременно с появлением проблем в мировой экономике, когда резко сократилось финансирование подобных проектов – Н.Х.).*

Тем не менее, мне такая аргументация никогда не казалась убедительной. Я всегда смотрел на программные продукты, способные работать не только с новыми форматами, но и со старыми, как на программное обеспечение для работы с новыми форматами, к которому «прикручен» инструмент для миграции старых форматов. В сущности, эта аргументация равносильна утверждению о том, что мне не нужен инструмент миграции и отдельный инструмент отображения, потому что у меня есть комбинированный инструмент для миграции и отображения. Очевидно, что такое комбинированное решение вполне приемлемо, но означает ли его использование отсутствие выполнения процесса миграции?

С моей точки зрения, всякий раз, когда программное обеспечение используется для интерпретации «неродного» (non-native) формата, ему приходится выполнять в каком-то виде переход от информационной модели, присущей этому формату, к информационной модели, используемой в программном обеспечении. Затем программное обеспечение может выполнять ряд последующих операций, например, отобразить информацию на экране или даже сохранить её в родном формате этого приложения (в последнем случае, это, конечно, будет миграция в чистом виде).

Безусловно, способы поведения программного обеспечения могут быть бесконечно разнообразными, но, думается, было бы справедливо утверждать, что наибольший риск потери информации, как правило, связан с первой операцией (преобразованием от одной информационной модели к другой), чем с последующими операциями, которые, вероятно, будут использовать информационную модель, присущую данному программному обеспечению (будь то в операциях отображения или сохранения в родном формате).

приложения). Следовательно, если нас волнует вопрос о том, действительно ли мы видим точное представление оригинала, то именно этап преобразования нужно проверить в первую очередь.

Именно здесь отдельный инструмент миграции вступает в свои права. Дело в том, что в этом случае возможно проведение независимой проверки качества выполняемого преобразования (путем сопоставления существенных свойств исходного и полученного файлов). Считается, что при последующем использовании мигрированного файла (например, инструментом отображения) дополнительных потерь информации уже не будет (или, по крайней мере, они будут намного меньше), поскольку у Вас есть возможность выбрать новый формат так, чтобы он был «родным» форматом для того инструмента, который Вы собираетесь использовать в дальнейшем (т.е. при чтении файла этим инструментом преобразование информационной модели уже не потребуется).

Тем не менее, я должен признать, что есть ряд практических соображений, которые следует принять во внимание.

Во-первых, миграция либо стоит денег (если требуется сохранить мигрированный файл) или выполняется медленно (если она, например, выполняется по требованию). Следовательно, будут, вероятно, случаи, в которых использование комбинированного инструмента для миграции и отображения окажется более удобным и достаточно хорошим решением. (С моей точки зрения, затратность миграции связана скорее с трудозатратами квалифицированных специалистов, особенно на этапе контроля качества, чем с затратами на хранение мигрированных файлов. Кроме того, в отсутствие миграции есть риск того, что старые форматы в какой-то момент перестанут поддерживаться, да и точность отображения оригинала не прошедшим соответствующую сертификацию средством может быть оспорена... - Н.Х.)

Во-вторых, стоит ли проверка качества миграции затрачиваемых на неё усилий? Конечно, всегда есть смысл проверить, например, работу инструмента отображения, используя набор тестовых файлов, прежде чем принять решение о его использовании – этого большей частью будет достаточно для установления работоспособности данного инструмента без проведения его детальной проверки. Тем не менее, бывают случаи, когда мы выявляем необычные сбои в работе распространенных средств миграции, поэтому валидация миграции действительно позволяет выявить проблемы, которые остались бы незамеченными, при использовании средств миграции в составе комплексного инструмента миграции и отображения.

В-третьих, достаточно ли всеохватывающей является проверка результатов миграции? Ответ на этот вопрос зависит от конкретных форматов, но для некоторых (даже распространенных) форматов ясно, что инструменты, поддерживающие более тщательную проверку, сделают работу более качественно. Конечно же, есть надежда, что качество таких инструментов будет постоянно улучшаться с течением времени.

В заключение хочу отметить, что я действительно рассматриваю миграцию как подходящий метод (и на самом деле данный метод практически все используют, порой не осознавая этого). Одной из задач сообщества специалистов по электронной сохранности я вижу в том, чтобы сформулировать интеллектуально здоровое представление о том, что представляет собой высококачественная миграция (например, посредством всеобъемлющего описания существенных свойств для широкого круга разнообразных объектов). Вполне вероятно, что используемые в реальной жизни инструменты представляют собой некое практическое приближение к этому идеалу (возможно, используя такие упрощения, как объединение средств миграции и отображения в одном инструменте), но мы должны, по крайней мере, понимать эти упрощения и уметь объяснять их.



ФЛЭШКИ В 2 РАЗА ОПАСНЕЕ, ЧЕМ ВЫ ДУМАЕТЕ

Источник: http://sos-ru.info/komp/komp_data_flash2.shtml

ИТ-специалисты компаний как минимум вдвое недооценивают риски использования работниками незащищенных флэшек. Между тем, до 77% сотрудников международных корпораций используют такие USB-накопители для хранения корпоративных данных. По словам российских специалистов, наш бизнес зачастую использует неправильный подход для предотвращения этих утечек.

Сотрудники часто используют личные незащищенные флэш-накопители для хранения ценной корпоративной информации. К такому выводу пришли авторы проведенного в США по заказу компании SanDisk исследования о рисках использования незащищенных USB-накопителей. Опрос рядовых сотрудников и ИТ-специалистов компаний показал, что руководители ИТ-отделов не имеют представления о масштабах распространения незащищенных флэш-накопителей в своих организациях: 77% опрошенных сотрудников корпораций используют личные флэш-накопители для хранения и переноса служебных данных. Однако опрошенные ИТ-специалисты оценивали долю сотрудников, использующих личные флэш-накопители в служебных целях, лишь в 35%.

Результаты опросов также показали, что чаще всего пользователи копируют на личные флэшки данные о заказчиках (25%), информацию финансового характера (17%), бизнес-планы (15%), информацию о сотрудниках компании (13%), маркетинговые планы (13%), объекты интеллектуальной собственности (6%), а также исходные коды программ (6%). Главным достоинством USB-накопителей является мобильность, но она создает значительный риск потери данных.

«Большинство ИТ-директоров понимает, что утечка информации может привести к краже личности, похищению интеллектуальной собственности или раскрытию коммерческих тайн, а также повлечь значительный ущерб как в смысле имиджа, так и с финансовой точки зрения, — говорит Джил Майлдворс (Gil Mildworth), старший директор по маркетингу в подразделении SanDisk по корпоративным решениям. — Результаты нашего опроса говорят о том, что, несмотря на некоторую осведомленность о возможных рисках, связанных с использованием незащищенных USB-накопителей, руководители ИТ-отделов еще не начали разработку эффективных политик, внедрение технологических решений и разъяснительную работу среди сотрудников с целью уменьшения этих рисков. Значительное снижение подобных рисков, как и повышение мобильности и продуктивности сотрудников, возможны только в случае принятия административного решения (на уровне руководства) о развёртывании систем интеллектуального управления устройствами, систем мониторинга и применения соответствующих общекорпоративных политик безопасности».

Примерно 23% опрошенных пользователей были либо вовсе не знакомы с корпоративными политиками в отношении флэш-накопителей, либо знали лишь о существовании подобных политик, но не имели полного представления об их сути. В то же время 44% респондентов отметили, что, насколько им известно, их компания не запрещает копирование корпоративных данных на личные USB-флэш -накопители. Еще 16% опрошенных ответили, что они не знают о таком запрете, в то время как лишь 40% пользователей наверняка знают, что в их компании существует запрет на копирование корпоративных данных на личные флэш-накопители.

Ответы ИТ-специалистов соответствовали результатам опросов пользователей. Примерно 21% ИТ-специалистов считает, что сотрудники компании лишь немного знакомы с принятыми корпоративными политиками, 33% опрошенных считают, что сотрудники посредственно знакомы с политиками, 28% полагают, что сотрудники хорошо знакомы с корпоративными правилами, и лишь 19% считают, что сотрудники полностью осведомлены о принятых в компании правилах и политиках.

Отечественные эксперты отмечают, что полученные в США результаты в полной мере нельзя перенести на Россию. В нашей стране специалисты по ИБ и ИТ в организациях очень хорошо осведомлены об опасности неконтролируемого использования сменных носителей и внешних устройств, считают аналитики компании Perimetrix. Согласно исследованию «Инсайдерские угрозы в России 2008», в ходе которого аналитический центр компании опросил более 450 организаций, специалисты по ИБ и ИТ указали, что именно мобильные накопители являются самым опасным каналом утечки. Он получил 74% голосов, обогнав электронную почту (58%), веб (26%) и принтеры (18%). «Высшие исполнительные лица крупных и средних организаций, не относящиеся к ИТ или ИБ, тоже прекрасно понимают, что их

сотрудникам не нужно хранить конфиденциальную информацию на флэшках, так как это может привести к случайной или злоумышленной утечке, — говорит директор по развитию бизнеса компании Perimetrix Алексей Доля. Таким образом, российский бизнес и государственные организации прекрасно осведомлены об опасности флэш-накопителей и ни в коем случае не недооценивают этот канал утечки».

Другое мнение высказали в компании InfoWatch. «Проблема утечки корпоративной информации при помощи флэшек недооценивается, — считает главный аналитик InfoWatch Николай Федотов. — Но ровно в той же степени, в какой недооценивается опасность утечек на любых других мобильных носителях. Наш мониторинг показывает, что очень большая доля утечек информации (39% от опубликованных случаев за 2007 г.) связана с потерями и кражами ноутбуков. Флэшку потерять даже легче. И украсть ее тоже могут. Тем не менее, такие накопители широко используются для конфиденциальных данных».

Сказанное выше, по словам Федотова, относится к незлонамеренным утечкам (таковых, по его оценкам, 71% в 2007 г.). «Что касается намеренной кражи данных, то здесь роль флэш-накопителей оценивается по достоинству — как службами ИБ, так и злоумышленниками», — подчеркнул эксперт.

Как считают специалисты, одними запретами и разъяснительной работой с сотрудниками проблему утечки информации решить не удастся. «Частые утечки, связанные с утратой ноутбуков, не привели на Западе к запретам их использования, — говорит Николай Федотов. — Руководство предприятий начало вводить обязательное шифрование данных. А производители ноутбуков начали встраивать стойкое шифрование прямо в контроллер жесткого диска. Производители флэш-накопителей неизбежно должны пойти тем же путем. К сожалению, российская тенденция, которую мы наблюдаем, тянет нас совсем в другом направлении. Вместо защиты данных вводятся тупые запреты. В том числе, запрет на использование флэш-накопителей. Хотя элементарное шифрование — эффективнее».



КАК ПРОДЛИТЬ ЖИЗНЬ «ФЛЭШКАМ»

Источник: http://sos-ru.info/komp/komp_data_flash3.shtml

Носители информации на основе микросхем флэш-памяти сейчас очень популярны. У многих есть компьютерные флэш-диски в виде брелка с USB-портом, а без карты памяти одного из многочисленных форматов нельзя представить цифровой фотоаппарат или карманный компьютер.

Активно оснащаются флэш-памятью мобильные телефоны, плееры и другие переносные устройства. В этой статье мы попытались обобщить

типичные для «флэшек» неисправности, а также дать несколько полезных советов, которые помогут снизить риск их поломки.

По практичности «флэшкам» нет равных среди всех сменных носителей. Большой и постоянно растущий объем, высокое быстродействие и надежность хранения данных, компактность, низкое энергопотребление и, наконец, удобство подключения — вот секрет их популярности. Кроме того, эти высокотехнологичные изделия продаются по вполне доступным ценам, которые постоянно снижаются.

Однако ничего идеального в мире не бывает, за все надо платить. В данном случае платить приходится надежностью в эксплуатации. Перечень типовых неисправностей флэш-носителей в порядке убывания их распространенности выглядит так:

- логические неисправности,
- механические поломки,
- электрические и тепловые повреждения,
- сбой контроллера,
- износ памяти.

Подробнее остановимся на основных симптомах поломок, методике ремонта и профилактике.

Логические неисправности

Носитель физически исправен, но опознается как пустой или неформатированный, а ранее записанные данные не видны. В этом случае повреждена файловая система, точнее, ее служебные таблицы. Данные обычно остаются на месте, и их можно попытаться восстановить с помощью различных эвристических программ. Любая эвристика основана на некоторых допущениях, и применительно к флэш-носителям эти допущения не всегда верны. Программы могут в упор не видеть данные, и тогда требуется кропотливая ручная работа. Восстановление цифровых фотографий также зависит от формата данных (JPG, TIFF или RAW) и от прошивки конкретной камеры.

Основная причина неисправности — преждевременное извлечение устройства из разъема или внезапное отключение питания, когда операционная система не успевает обновить файловую систему носителя.

Профилактика: аккуратно завершайте работу с флэш-носителями. В компьютерах и ноутбуках используйте «безопасное извлечение устройства». В ЦФК и другой подобной технике следите за зарядом аккумулятора и выключайте питание не раньше, чем закончится запись на карту.

Механические поломки

«Флэшки» нередко страдают от грубого обращения. Многие флэш-диски имеют непрочный корпус, плату из тонкого текстолита, слабое крепление разъема USB. Карты памяти бывают слабы на изгиб. Механические напряжения создают микротрещины и приводят к нарушению контактов. От ударов и падений страдает кварцевый резонатор. У большинства устройств негерметичный корпус, пропускающий воду.

Ремонт: восстановление контактов, замена деталей. Если треснул чип памяти, то данные потеряны, ремонт не оправдан. К счастью, так бывает редко.

Профилактика: бережно обращайтесь с устройствами, карты памяти храните в футлярах. Выбирайте флэш-диски с прочным, не слишком тонким корпусом; чем больше металла, тем лучше.

Старайтесь не задевать флэш-диск, вставленный в порт USB: вместе с поломкой можно получить замыкание. Если ваш носитель побывал в воде, особенно морской, его лучше сразу отдать специалисту, недостаточная просушка может стать фатальной для данных.

Электрические и тепловые повреждения

Нестабильное электропитание, а также разряды статики — частая причина неисправности флэш-носителей. Многие модели имеют слабую защиту от перепадов напряжения, и случайные броски выводят их из строя. Нередко к поломке флэш-дисков приводит устаревшая электропроводка: многие компьютеры до сих пор не заземлены. На их корпусе может блуждать потенциал в десятки вольт, а статический заряд стекает куда придется. Все это при совпадении неблагоприятных условий приводит к выгоранию контроллера и элементов обвязки.

Еще одна причина неисправностей — «человеческий фактор». Неопытные сборщики компьютеров умудряются неправильно подключить шлейф USB-порта, идущий от передней панели, к разъему материнской платы. В результате при подключении устройство моментально сгорает.

Проблема нагрева для флэш-дисков не так актуальна, как для жестких дисков. Но и здесь кроется причина поломок. Многие пластиковые корпуса не обеспечивают хорошего теплоотвода, и при активной работе нагруженные детали могут перегреться, выйти из строя и даже проплавить корпус.

Ремонт: замена неисправных деталей, если стоимость запчастей невысока.

Профилактика: обеспечьте компьютерам заземление и качественное питание. Прежде чем вставить флэш-диск в порт USB, коснитесь рукой системного блока. От статики и перегрева хорошо защищены флэш-диски в металлических корпусах. В свете проблем со сборкой, а также из-за меньших наводок надежнее использовать порты USB на материнской плате (для удобства доступа к задней панели поставьте удлинитель).

Сбой контроллера

Контроллер стоит на всех флэш-дисках и многих картах памяти, в некоторых ситуациях (предположительно, сбои по питанию) его прошивка блокируется и не отвечает на запросы операционной системы. В этом случае устройство опознается как Generic Drive с нулевой емкостью, данные обычным путем не доступны. Их можно считать непосредственно с чипа памяти на специальном стенде.

Ремонт: восстановление прошивки контроллера с помощью технологических утилит.

Профилактика: защита от статики, контроль питания.

Износ памяти

Носитель опознается, но читается с ошибками вследствие дефектов на физическом уровне. Флэш-память по своей природе выдерживает ограниченное число перезаписей, причем по мере роста емкости чипов заявленный ресурс снижается: от 1 млн циклов 3-5 лет назад до 100 тысяч в новых моделях.

Казалось бы, в любом случае порог высок и опасаться нечего, но вспомните про файловую систему. Ряд ее служебных полей переписывается при каждом обновлении любого из файлов, именно эти ячейки первыми выходят из строя. Для борьбы с этим явлением применяется технология «выравнивания износа» (wear leveling): часто изменяемые данные перемещаются по адресному пространству флэш-памяти.

Ремонт: низкоуровневое форматирование с сокрытием дефектов.

Профилактика: износ ограничивает срок службы флэш-носителей. При постоянном обновлении данных сбои могут начаться уже через 1-2 года. Экземпляры «со стажем» выводите из эксплуатации или используйте для хранения менее важных данных.

Заключение

Несмотря на описанные проблемы, «флэшки» — удобные и надежные средства хранения и переноса информации. Несложные меры профилактики помогут вам продлить жизнь своим устройствам и избежать большей части неприятностей. А если сбой все же случился — обращайтесь в специализированные сервис-центры. Ремонтные технологии, лишь частично раскрытые здесь, позволяют добиваться успеха в 90% случаев.



КАК ЗАЩИТИТЬ И СОХРАНИТЬ ДАННЫЕ НА ПОРТАТИВНОМ НОСИТЕЛЕ

Источник: http://sos-ru.info/komp/komp_data_flash.shtml

Объемы и функциональность накопителей растут стремительно: скажем, 4-гигабайтной флешкой уже никого не удивишь. Последнее время стало модно использовать флешку для хранения и запуска приложений: офисных программ, ICQ-клиентов и пр. На USB-флешку можно сохранить архив фотографий или фильм в DVD-качестве. Но что для нас самое главное в процессе использования всех этих новомодных технологий? Главное – это данные, которые мы собираем, обрабатываем, передаем. Согласитесь, сложно представить себе более неприятную ситуацию, чем вернуться из отпуска и обнаружить, что сохраненные на USB-флешке фото частично или полностью удалены, а важные данные на ноутбуке странным образом оказались

испорчены. А дело «всего лишь» в том, что вы по рассеянности оставили ноутбук на пару минут в открытом гостиничном номере (то ли просто «приземлили» его с небольшой высоты), а флешку перепутали с CD и решили немного подредактировать содержащиеся на ней данные. Приятного действительно мало, но, к счастью, в наших силах максимально уменьшить вероятность возникновения такого инцидента и свести к минимуму ущерб в том случае, если это все-таки произойдет. Меры, которые нужно для этого предпринять, мы и рассмотрим в данном материале.

Пара вступительных слов

Перед тем как перейти непосредственно к изложению материала, хотелось бы сказать несколько «предупреждающих слов».

Данная статья НЕ предназначена для специалистов по ИБ (информационной безопасности) или для читателей, стремящихся стать таковыми. В материале не делается акцент на том, что защита данных и защита информации – «это две большие разницы». Многое, что должны знать специалисты об ИБ, не вошло в рамки статьи, которая предназначена исключительно обычным людям и обычным пользователям информационных технологий, которым хотелось бы как-то оградить себя от возникновения неприятных ситуаций, описанных выше – только и всего.

Что и как можно защитить

Наиболее распространенные носители, на которых может понадобиться защитить данные, – это жесткие диски, установленные как на обычных ПК, так и на ноутбуках, и внешние накопители (чаще всего с подключением по USB, но у вас может быть и, например, IDE или eSATA).

Отметим, что понятия «носитель» и «защита данных» очень расплывчаты, поэтому, говоря об этих двух вещах, нельзя упускать из виду и защиты, например, самого ноутбука, в котором инсталлирован жесткий диск с важными для вас данными. Все это взаимосвязанные вещи, и разделять их не стоит. Самые общие принципы обеспечения целостности, доступности и конфиденциальности информации одинаковы для любых носителей.



Простой, но эффективный способ защитить данные - воспользоваться переключателем защиты от перезаписи

Методы защиты могут быть программными или аппаратными. Исходя из этого, классификация методов будет выглядеть следующим образом:

- *Программные средства защиты:*

1. Программное шифрование данных;
2. Программное обеспечение, позволяющее реализовать дополнительные возможности по защите накопителей, чьи функции защиты не работают без соответствующего ПО и установленных драйверов (проще говоря, "сопутствующее" ПО);

3. ПО, позволяющее настроить такие нюансы, как блокировка тех или иных возможностей системы в определенные часы. Например, если вы в отпуске каждый день уходите из своего гостиничного номера на обед с 13-00 до 14-00, вы можете приказать системе блокировать работу USB-носителей именно в это время. То есть даже в том случае, если вы забудете выключить ноутбук/запереть дверь, злоумышленник не сможет скопировать данные на USB-носитель, запустить с него какие-либо утилиты для дальнейших деструктивных действий и т.п. Так же с помощью специального ПО можно создать скрытые области жесткого диска, куда вы могли бы безопасно спрятать данные;

4. Возможность установки пароля на доступ к жесткому диску/USB-носителю обычно реализуется программными средствами;

5. Некоторые производители оснащают USB-носители встроенной защитой от вредоносных программ. Это также можно отнести к нашей теме;

6. Очень специфические методы защиты, с которыми вы вряд ли столкнетесь: например, двухфакторная аутентификация.

- *Аппаратные средства защиты:*

1. Аппаратное шифрование данных;
2. Аппаратный переключатель защиты от записи;
3. Биометрические системы защиты от несанкционированного доступа к данным (сканеры отпечатков пальцев);

4. Технологии, повышающие стойкость к физическим воздействиям: повышение ударопрочности накопителей данных (шоковая защита), защита от влаги, экстремальных температур и т.п.

Это самое общее деление. Теперь еще раз пройдемся по списку и рассмотрим некоторые самые интересные пункты подробнее.

Подробнее о программных методах защиты

Начнем с шифрования. Для чего это нужно? Во-первых, это достаточно просто и удобно. Во-вторых, если вы потеряете портативный носитель или ноутбук (с жестким диском внутри), данные на котором будут зашифрованы, вы хотя бы будете знать, что вероятность того, что злоумышленник сможет просмотреть или скопировать ваши данные, невелика. Без сомнения, это может быть важно с различных точек зрения: как с моральной (вряд ли кому-то будет приятно, если какой-то незнакомец получит доступ к вашей личной переписке, фотографиям и т.п.), так и с «финансово-экономической» (на

ваших носителях могут находиться важные деловые данные, пароли, и их потеря может повлечь за собой уже довольно серьезные неприятности).

Данный метод защиты (называемый криптографическим), как вы наверняка уже заметили, может быть программным и аппаратным (а также программно-аппаратным). Впрочем, это довольно условно-обобщенное деление. Если же подняться на уровень более подробного рассмотрения, то здесь у нас запросто могут разбежаться глаза. Шифрование данных на внешнем накопителе можно реализовывать встроенными средствами, автономно подключаемыми аппаратными модулями, с помощью утилит сторонних производителей (например, ESMART CryptoDisk или знаменитый PGP) или встроенных функций ОС (привет технологии BitLocker в новейшей Windows Vista). Устройств и технологий шифрования сегодня на рынке более чем достаточно, поэтому разговор может идти только о том, что для вас удобнее и дешевле. В области встроенных систем шифрования жестких дисков на ноутбуках, конечно, стоит обратить внимание на решения от Seagate. Многие продукты обладают TPM-модулем (Trusted Platform Module – довольно сложная и несколько неоднозначная технология; главное, что стоит про нее знать, – она помогает реализовать шифрование и работу с паролями на аппаратном уровне). Такая защита реализована в компьютерах MPC Computers. Для шифрования можно установить в компьютер и отдельную плату, реализующую этот механизм.



Флешки Kingston DataTraveler Elite осуществляют шифрование записываемых на накопитель данных в режиме "реального времени" по алгоритму AES (со 128-битным ключом)

Что касается USB флеш-накопителей, здесь стоит вспомнить об устройствах от Kingston (в частности, линейке DataTraveler Elite), которые осуществляют шифрование записываемых на накопитель данных в режиме «реального времени» по алгоритму AES (со 128-битным ключом). Устройства данной линейки также обладают механизмом парольной защиты (в том числе защитой от брутфорса – подбора пароля пользователя злоумышленником), есть возможность создания зон на накопителе для хранения персональных данных и т.п. Средняя цена – \$70-90.

Программное обеспечение, позволяющее реализовать дополнительные возможности накопителей по защите данных, в подавляющем большинстве случаев поставляется вместе с самими устройствами. Либо соответствующие утилиты всегда можно скачать с официальных сайтов производителей.



Программный интерфейс, позволяющий закрыть паролем доступ к выделенной части памяти Kingston DataTraveler Elite

Программ, позволяющих реализовать большое количество задач по защите данных на различных носителях, на рынке есть очень много, и все они отличаются по цене и возможностям: начиная от Z-Lock и заканчивая продуктами Rohos. Думаю, что большинству читателей хватит функционала бесплатных программных пакетов, которые можно свободно найти и скачать из интернета. Например, можно отметить такой продукт, как Code Protection System.

Пароли сегодня установить можно практически на все: на полный доступ к носителям, на доступ к скрытой их области (зашифрованной или нет), на расшифровку данных на носителе и т.п. Хотя пароли как таковые уже, фактически, считаются устаревшим средством защиты, они по-прежнему «живы» как составляющая других защитных технологий и активно используются разработчиками накопителей. Разработчики принимают дополнительные меры по защите самих паролей от их подбора: реализуют механизм удаления/шифрования данных после определенного количества неверных вводов пароля и т.п. Устройства с такими технологиями сегодня не редкость – это и уже вышеупомянутые продукты Kingston, и USB флеш-накопители от Philips и многих других производителей. Как дополнение к другим, более надежным методам защиты (например, тому же шифрованию) пароли весьма полезны.

Несколько слов об интегрированной в накопитель защите от вирусов и прочего вредоносного кода. Например, устройства от Digiworks, которые одними из первых представили подобные продукты – линейку Virus Chaser, в которой используется антивирусный продукт от Bizet. Очень оригинальное решение, но лично я весьма невысокого мнения о качестве этого ПО. Пока что устройства такого типа являются скорее экзотикой, чем действительно удобным и качественным решением.

Что касается методов вроде двухфакторной аутентификации, то он применим к защите информации на жестких дисках ноутбуков и ПК. Примечательно, что для защиты данных на них используется как раз USB-флешка, на которой записывается зашифрованная информация, необходимая для получения доступа. Двухфакторная аутентификация – это наше

ближайшее будущее (хотя, по логике, должно быть уже довольно давно реализованным настоящим). Она позволяет реализовать доступ к ресурсам компьютера с помощью зашифрованного USB-ключа (флеш-накопителя), который может запомнить пароль сколько угодно значительной сложности. Причем доступ к этому ключу может быть защищен PIN-кодом (который запомнить, конечно же, намного проще, чем длинный пароль из букв, цифр и специальных символов). В большинстве двухфакторных систем предусмотрен и режим «аварийного» доступа, позволяющий вам все-таки получить доступ к своей собственной информации, если вы вдруг потеряли/испортили флешку (бывает всякое). Весьма удобной представляется и возможность автоматической блокировки системы после отключения USB-ключа и автоматической же разблокировки после повторного подключения. Бывают USB-ключи, генерирующие одноразовые пароли (например, от Alladin) и т.п. Плюсов, возможностей и вариаций еще предостаточно; так что, если у вас есть насущная необходимость (или просто вам так хочется), такой системой вы можете защитить как свой личный ноутбук/ПК, так и рабочий ПК (если есть такая возможность). Но, вероятнее всего, такая избыточная защита не придется вам по душе, тем более если стоит задача защитить компьютер только на время отпуска. А вот кого сверхнадежная защита точно заинтересует, так это часто путешествующих топ-менеджеров, информация в ноутбуках которых может стоить весьма и весьма дорого.

Как и что реализовать аппаратно

Идем дальше. Об аппаратном шифровании мы уже говорили. Теперь рассмотрим аппаратный переключатель защиты от записи. Это вовсе не так глупо, как вам может показаться: мировой опыт показывает, что наибольшие убытки и проблемы, связанные с потерей (утечкой) данных как в масштабе компании, так и в ПК одного пользователя, возникают уже не столько от действий злоумышленников, сколько от элементарной халатности или невнимательности. Вряд ли будет приятно обнаружить, что вы перепутали флешку с каким-то другим диском или просто решили ее отформатировать вместо дискеты. Аварийное восстановление данных после удаления, конечно, возможно, но применимо далеко не всегда. Так что стоит ли создавать себе лишние проблемы?



Биометрическая защита данных на внешнем накопителе обычно реализуется в виде считывателя отпечатков пальцев

При выборе флеш-носителей обращайте внимание на эту, казалось бы, малозначительную деталь – маленький ползунок, рядом с которым нарисован разомкнутый и закрытый замочек. Что удивительно, есть устройства, не обладающие такой полезной «мелочью».

Следующая большая тема – биометрические системы защиты.

Их разновидностей существует довольно много, но наиболее распространенная из них – контроль доступа по отпечатку пальца. Такие системы встроены как в довольно большое количество моделей ноутбуков, так и во многие модели флеш-карт (например, от Aretmis). Обычно с помощью встроенного в эти устройства ПО и дактилоскопического датчика можно закрыть от доступа посторонних весь носитель или его часть. Обычно такого рода устройства запоминают до 10 отпечатков (интересно, чем им не нравятся остальные 10?), так что, если, скажем, вы обожгли подушечку указательного пальца правой руки, вы все же сможете получить доступ к своим данным. Если, конечно, не приложили к горячей конфорке сразу все пальцы. Но с такой глупостью, согласитесь, бороться не способна ни одна система защиты.

Биометрические системы сегодня приобретают все большее распространение. Можно встретить и биометрическую мышшь (например, от BioLink), которая позволяет реализовывать удобный защищенный доступ как к ПК, так и к Сети. Обычно средняя цена всех качественных устройств с биометрией не ниже \$90.

Физическая защита накопителя

Не стоит забывать о такой важной вещи, как физическая сохранность носителей данных. В любом путешествии вашу технику и носители данных подстерегают множество испытаний на прочность в прямом смысле этого слова: удары, тряска, вода, песок... Желательно постараться максимально оградить свои устройства от этих испытаний. Для этого производители разработали большое количество разнообразных технологий, защищающих как жесткие диски, так и флешки. В частности, можно упомянуть о Shock Protection System (для HDD), которую сегодня реализовывает Maxtor в своих продуктах. Для ноутбуков таких технологий очень много – все они реализуют свою задачу из широкого спектра возможных/доступных. Для портативных накопителей также существуют аналогичные технологии. Из устройств, их использующих, можно, например, вспомнить поистине «бронированную» линейку носителей Flash Survivor от Corsair, сравнительно недавно представленных на мартовском CeBIT. Эти устройства выдерживают давление до 20 атмосфер и могут «спускаться» на глубину до 200 метров (любители дайвинга получили возможность работать с любимой флешкой и под водой). При этом устройства поддерживают и шифрование.

Фотонакопители Sony очень хорошо защищены от случайных падений и тряски. Но самый лучший уровень защиты, пожалуй, обеспечивают профессиональные фотобанки JOB0. В общем-то, систем физической

защиты почти столько же на рынке, сколько и самих производителей, и эта широкая тема заслуживает отдельного материала.



Одни из самых надежных фотонакопителей делает компания JOBO

Заключение

Напоследок отмечу, что красота устройства и его достойный защитный функционал – отнюдь не взаимоисключающие понятия. Устройства таких производителей, как Pqi и Prestigio, позволят вам и самовыразиться, и данные защитить.

Возможно, приведенные здесь рекомендации помогут вам более ответственно подойти к выбору временного хранилища для ваших данных. Надеюсь, что, следуя нашим рекомендациям, вы сможете надежно сохранить данные и не допустить их несанкционированного использования.



НАДЕЖНО ЛИ ХРАНЕНИЕ ДАННЫХ НА CD/DVD ДИСКАХ?

Источник: http://sos-ru.info/komp/komp_data_cd-dvd.shtml

Поговорим о качестве CD/DVD болванок, которые мы покупаем.

Оптические диски – практически идеальный вариант для создания домашнего архива: данных, музыки, видео. CD/DVD диском мы доверяем, часто, ценную и очень ценную для нас информацию. Причина тому – компьютерная мудрость: "хранить как можно меньше важной информации на жестком диске компьютера".

Для справки: Это связано с тем, что компьютер подвержен угрозам заражения вирусами и другим вредоносным ПО из интернета, угрозам сбоя в операционной системе и сбоям в самом жестком диске. Понятно, что какая-то важная и ценная информация, хранящаяся на HDD – постоянно подвергается этим угрозам. А оптический диск – "мирно" лежит в ящике стола и подвергается значительно меньшему количеству угроз: разве что угрозам чрезмерных механических воздействий на диск, царапинам, деформации и перепадам температур/влажности (для полной картины).

Зачастую, мы часто просто не задумываясь записываем информацию на оптический диск, кладем диск в стол и всё, что называется, "душа спокойна" – данные достаточно надежно сохранены на диске.

Как правило, если данные записывались на CD/DVD с жесткого диска, то после успешной записи, они (данные) удаляются с HDD. Таким образом, данные хранятся на оптическом носителе в единственном экземпляре – резервной копии нет. Как кажется, она вроде бы и не нужна – "Данные на "оптике", это все равно не на HDD в компьютере. Ну что им может угрожать? Я же аккуратно обращаюсь с дисками! Значит, все хорошо...".

Однако может случиться так, что в один прекрасный день, записанный пару лет (да что там "лет" – бывает всего пару-тройку месяцев!) назад диск – не прочитается приводом. Или прочитается, но данные извлекутся лишь частично. Некоторые файлы окажутся повреждены. Причем, вероятность успешного восстановления крайне низка (ниже я объясню почему). Либо же с диска нельзя будет вовсе извлечь хоть какую-то информацию.

К сожалению, это распространенная картина.

Если вы купили свой первый компьютер достаточно давно, скорее всего, у вас есть приличный архив личных данных разного типа (документы, музыка, видео) на CD/DVD. Несколько десятков дисков это точно.

А может быть весь ваш архив вмещается в пару DVD дисков – это не важно. Главное, что информация в вашем архиве (будь то 50 или 5 дисков) – ценна для вас и потеря этой информации крайне нежелательна!

Однако, немного тех, кто задумывается всерьез о вышеописанной печальной картине, когда покупает в магазине CD/DVD диски для записи...

В 7 случаев из 10 причиной выхода из строя "болванки" является ее низкое качество.

Здесь вполне логично появляется вопрос: "Какие оптические диски можно считать качественными и как не купить низкосортное изделие?"

К сожалению, внятного и конкретного ответа на этот вопрос нет.

Производителей оптических дисков намного меньше, чем брендов, под которыми выпускаются те или иные диски. Связано это с тем, что производство оптических дисков – дело весьма и весьма сложное. Здесь нужны проверенные технологии и оборудование.

Т.е. всего несколько производителей выпускают диски под десятками брендов. Конечно, некоторые бренды уже зарекомендовали себя, некоторые – не такие раскрученные марки. Но и в том и в другом случае – есть вероятность купить некачественное изделие (хотя и различная).

Не буду вдаваться в технические подробности, чтобы не нагружать вас тяжелым материалом, скажу в общем.

При записи любого оптического диска неизбежно возникают ошибки. Конечно, при чтении данных это не заметно – некоторые ошибки исправляются в процессе чтения приводом, а некоторые пропускаются. Но, существует общепринятый стандарт для дисков, который определяет максимально допустимое число ошибок.

Так вот, критерий "качества" того или иного диска определяется именно количеством ошибок, которые остаются на диске после записи. Это зависит:

А) От самого диска.

Б) От привода, который производит запись.

Итак, пункт А.

Конечно, довольно часто менее известные бренды выпускают диски, которые по качеству ничуть не хуже именитой продукции, при более низкой цене. Однако, не менее часто бывает обратное. И самое грустное то, что проверить и точно установить какие-либо критерии качества таких дисков нельзя даже в тестовых лабораториях. Причина тому – “диск диску рознь”. Т.е. если вы покупаете малоизвестную болванку, сделать вывод о ее качестве можно только тестами конкретно этого диска. Если один диск может показать низкие результаты, то другой – того же бренда, может оказаться более чем хорошим. А причиной этому может стать что один диск из одной партии продукции, а другой диск – из другой партии соответственно.

Конечно, среди известных брендов значительно реже попадает некачественная продукция.

Пункт Б. Приводов множество. Какие-то хорошо записывают, а читают хуже, какие-то наоборот, а некоторые в равной степени хорошо читают и записывают диски.

В конечном итоге, наилучший результат определяется комбинацией: качественный диск + качественный привод. Однако, бывает так, что качественный диск не очень качественно записывает привод. Тогда все преимущества хорошей болванки сводятся на нет.

Поэтому, выбор пользователя должен строиться больше на личном практическом опыте. Или же, нужно проконсультироваться со специалистом в области "железа", чтобы наиболее оптимально выбрать привод и получить аргументированные советы по оптическим дискам.

Например, я, по своему личному опыту, могу дать следующие, можно сказать, обобщенные рекомендации:

Привод. Присмотритесь к продукции Plextor, Lite-On и Pioneer. Это тот самый вариант, когда привод одинаково хорошо и читает и пишет диски. Так же хорошим выбором будут приводы LG и Samsung.

Диски. Присмотритесь к следующим брендам: Verbatim, Sony, Imation, TDK, Samsung, Philips (конечно, на этом список хороших брендов не кончается, но мне хочется сейчас выделить именно эти). Да, такие диски стоят несколько дороже, чем их менее известные "собратья", но они того стоят. Почти всегда – это качественные изделия.

P.S. Помните, что от качества комбинации привод + оптический диск зависит очень многое: надежность хранения данных на диске, срок хранения данных и т.д.

МИКРОГРАФИЧЕСКАЯ КАМЕРА УКМ-3

Источник: <http://www.micrography.ru/modelnyj-ryad/mikrograficheskie-camera/mikrograficheskaya-luggage-ukm-3/>



УКМ-3 - единственная серийная камера для микрофигирования, позволяющая производить черно-белую и цветную съемку документации размером до А1/А0 на форматную галогенидосеребряную пленку DIN А6. Особенности микрографической камеры УКМ-3 являются:

Универсальность

- Модульная конструкция позволяет оптимально настроить камеру под потребности заказчиков
- Большое количество дополнительных столов позволяют проводить съемку любых оригиналов

Современные технологии

- Камера УКМ-3 может быть оснащена как специальными съемочными головками под съемку на микрофиши формата DIN А6, так и универсальной съемочной головкой для съемки на любые типы микроформ
- Уникальный аппарат для съемки комбифиши с сеткой неравномерного деления.
- Наличие нескольких базовых моделей.
- Съемочная головка для одновременной съемки двух микрофильмов МР-35.
- Съемочная головка для одновременной съемки МР-16/35/105 и МФ-А6.

Управление съемкой

Специальное управляющее программное обеспечение Fichex позволяет формировать произвольные заголовки фиш и управлять размером и расположением кадров при съемке.

Технические характеристики микрографической камеры УМ-3

Формат оригинала, макс, мм	В зависимости от используемого стола: А0, плоский стол А0 Copy table А1, стол-колыбель ВWA12 Столы взаимозаменяемые
Тип микроформы	МФ-А6
Масштаб съемки (плавная установка масштаба)	В зависимости от используемой колонны: 7.5-30х = колонна 2320 мм 7.5-42х = колонна 2800 мм 7.5-50х = колонна 3120 мм 7.5-72х = колонна 3970 мм
Разрешающая способность, мм ⁻¹	До 150
Режимы выставления кратности	Непрерывного изменения и установки в заданное значение
Производительность, кадр/час	до 200
Изменяемый параметр при экспонировании	1) Выдержка 2) Освещение
Экспозиция	1) Автоматическая 2) Ручная
Объектив	Zeiss S–Biogon f = 40 мм
Фокусировка	Автоматическая во всем диапазоне кратностей
Верхнее освещение	4 лампы по 200 Вт
Толщина оригинала, макс, мм	170
Прижим микрофиши	Вакуумный
Электропитание: В, Гц, кВт	220; 50/60; 2.0
Габариты, для 30х, мм	2700 x 1450 x 2350
Масса, для А1/А0, кг	310/465, в зависимости от комплектации

Стандартная комплектация

- Съёмочная голова для микрофиши
- Маски для съёмочной головы
- Колонна Н=2320 мм
- Стол-колыбель ВWA12
- Пульт управления
- Комплект загрузки одиночной микрофиши

Дополнительная комплектация

- Универсальная съёмочная голова для 105+35+16 мм рулонной пленки, и микрофиши 105x148 мм. Данная голова позволяет использовать одновременно две пленки 16 мм или 35 мм
- Модуль печати заголовков
- Управляющая станция с ПО "FICHEX"
- Книжная колыбель ВWT
- Дополнительные съёмочные столы

УНИВЕРСАЛЬНЫЙ СКАНЕР МИКРОФИЛЬМОВ 16/35 И МИКРОФИШ А6 IMAGELINK 2400/3000 DV PLUS

Источник: <http://www.micrography.ru/modelnyj-ryad/scanners-microforms/universal-scanner-microfilm-16-35/>



Imagelink 2400/3000 DV Plus – это универсальный сканер, предназначенный для просмотра и сканирования микрофиш МФ-А6 и рулонных микрофильмов МР-16/35. Данное устройство работает в режиме покадрового сканирования, при этом оператор осуществляет ручной подвод нужного кадра под объектив.

Основные преимущества:

- Сканер позволяет оцифровывать все типы микроформ
- Высокая скорость сканирования (А3, 400 dpi – 7 секунд) позволяет оцифровывать до 500 кадров в смену.

Дополнительные опции:

- Модуль для сканирования с оттенками серого
- Универсальная каретка с моторизованной перемоткой рулонных микрофильмов для всех типов микроформ
- Объектив 7.5x; объектив 9 - 16x; объектив 13 - 27x; объектив 23 - 50x
- Комплект для ручного маскирования рамки кадра (только для 2400/3000 DV Plus)
- Запасная лампа 150 Вт
- Лазерный принтер А3/А4

Технические характеристики сканера микрофильмов 16/35 и микрофиш А6 Kodak DSV-E 2400/3000

Размер экрана, мм 2400 DSV	300 x 300	303 x 440
Тип микроформ	MP-16/35, МФ-А6	MP-16/35, МФ-А6
Набор объективов	7.5x, 9-16x, 13-27x, 23-50x (для 2400)	7.5x, 9-16x, 13-27x, 20-50 (для 3000)
Разрешение, dpi	200, 300, 400, 600, 800	200, 300, 400, 600, 800
Паспортная скорость сканирования, сек.	A4, 200 dpi — 4 сек., A3, 400 dpi — 7 сек.	A4, 200 dpi — 4 сек., A3, 400 dpi — 7 сек.
Сменная производительность, кадров/смена	500	500
Формат электронного образа	TIFF G 3, G 4	TIFF G 3, G 4
Полярность изображения	Негативная и позитивная	Негативная и позитивная
Электропитание, В/Гц/Вт	220/50/400	220/50/400
Размеры, мм	560 x 760 x 853	560 x 760 x 853
Управляющее ПО	PowerFilm V 5.3	PowerFilm V 5.3
ОС для ПО PowerFilm	Windows NT-4 & 2000, Win XP	Windows NT-4 & 2000, Win XP
Интерфейс с ПК	SCSI	SCSI
Интерфейс с принтером	Video Printer	Video Printer

ПОТОЧНЫЙ СКАНЕР СКАМАКС 2000/3000

Источник: <http://www.scamax.ru/modelnyj-ryad/scamax-200030001/>



ЭЛАР СКАМАКС 2000/3000
Сплав уникальностей

- Скорость – от 90 до 340 страниц в минуту
- Сканирует от чертежной кальки до картонных карточек
- Формат оригинала – от трамвайного билета 2x6 см до схем и чертежей A3+
- Реализует технологии сетевой групповой работы
- Минимальная стоимость сервисных контрактов, срок службы – более 10 лет

Скоростные документные сканеры ЭЛАР СКАМАКС серии 2000 и 3000 предназначены для потоковой оцифровки бумажной документации. Сканеры серии 2000 позволяют получать изображения в черно-белом и сером режимах, а сканеры серии 3000 – в черно-белом, сером и цветном режимах.

Скорость оцифровки в зависимости от модели составляет от 90 до 340 страниц в минуту и не зависит от того, в каком режиме работает сканер – в черно-белом, сером или цветном, с односторонним или двухсторонним сканированием листов.

Сканеры серии ЭЛАР СКАМАКС 2000 и 3000 обеспечивают высокое качество получаемых электронных копий даже при работе с ветхими, замятыми или поврежденными оригиналами. Аппаратные функции позволяют улучшать качество образов, например, вычитать цветной фон, выполнять «доворот» перекошенного изображения, удалять «шумы» и черную границу, пропускать пустые страницы и многое другое.

ЭЛАР СКАМАКС имеет удобную сенсорную русскоязычную панель управления, с которой осуществляется большинство настроек сканирования.

Возможна модернизация, благодаря которой сканер может быть легко переориентирован и настроен для выполнения новых задач.

Сканеры ЭЛАР СКАМАКС 2000 и 3000 являются важным звеном системы электронного документооборота организации и обеспечивают возможность гибкого и компактного решения индивидуальной задачи – от организации электронной канцелярии до мощного центра обработки документов.

Благодаря надежности конструкции, отработанной за время многолетнего серийного производства, сканеры СКАМАКС 2000 и 3000 рассчитаны на долговременную работу с предельными нагрузками.

Сканеры продолжают совершенствоваться!

Новый интерфейс подключения сканера Ethernet GigaBit – это высокоскоростной и распространенный интерфейс, совместимый с множеством операционных систем.

Механизм подачи документов с автоматическим определением толщины документа позволяет сканировать оригиналы различной плотности в одной пачке. Для разделения листов используются износостойчивые ролики с резиновыми накладками.

Сканер оснащен светодиодными лампами подсветки, которые обеспечивают правильную цветопередачу на графических образах, не требуют времени на прогрев и соответствуют самым современным стандартам энергосбережения, при этом являются самими долговечными и неприхотливыми в обслуживании.

Два импринтера для надпечатки текста на лицевой и оборотной стороне документа. Характеристики отпечатываемой строки могут свободно выбираться. Она может содержать такую информацию как дата, время или текущий номер, а также любой текст, который пользователь введет через электронную клавиатуру на сенсорной панели управления сканером.

Высокая производительность при низкой стоимости владения

Скоростные документные сканеры ЭЛАР СКАМАКС 2000 и 3000 рассчитаны на интенсивные нагрузки и многосменную работу. Их пиковая сменная производительность ограничена только общей производительностью

процесса оцифровки. Механизмы самого сканера позволяют использовать его без ограничений, 24 часа в день, 7 дней в неделю.

В протяжном тракте сканера ЭЛАР СКАМАКС нет пластиковых или стеклянных деталей. Валы протяжного тракта сделаны из высококачественных металлических сплавов, что обеспечивает их высокую износостойкость. Единственные расходные материалы для сканеров СКАМАКС – недорогие резиновые накладки на ролики захвата оригиналов, рассчитанные на длительный срок службы. Надежный механизм, износоустойчивые расходные материалы и простота в обслуживании обеспечивают для СКАМАКС очень низкую стоимость владения, минимальную среди сканеров данного класса.

Оптимальное соотношение качества изображения и объема выходного файла благодаря возможностям настройки оптического разрешения

Чем выше оптическое разрешение, тем больше элементов отображается на электронной копии, НО, ниже скорость сканирования, больше уровень «шума» на образе документа и больше объем выходного файла. На сканере СКАМАКС доступны и низкие, и высокие оптические разрешения – от 150 до 600 dpi. В зависимости от выполняемой задачи выбирается то разрешение, которое подходит для оптимизации ресурсов конкретной системы пользователя по обработке и хранению изображений.

Универсальность

Благодаря уникальному ременному механизму протяжки документов, сканер СКАМАКС обеспечивают максимально эффективную и бережную работу со всеми типами документов. Он может оцифровывать документы маленького формата (от 2x6 см), мятые и рваные документы, длинные каротажные ленты. Сканеры с роликовым протяжным трактом не справляются с такими задачами, так как площадь контакта роликов с документами гораздо меньше, чем у сканера с ременной протяжкой. СКАМАКС не чувствителен к попаданию в протяжной тракт документов со скрепками, так как в его протяжном тракте нет стеклянных и пластиковых поверхностей.

Сканер автоматически определяет толщину бумаги, что позволяет избежать проскальзывания оригиналов при протяжке, связанного с ветхостью и повышенной шероховатостью материала. Все вышеперечисленные возможности гарантируют неизменно высокую производительность сканера при потоковом вводе документов.

Сканеры ЭЛАР СКАМАКС 2000 и 3000 оснащены тремя ультразвуковыми датчиками, которые распознают захват двойного документа и немедленно реагируют на это. При этом датчик чувствует именно количество страниц, а не толщину, что позволяет беспрепятственно сканировать в одной пачке оригиналы различной плотности.

При обнаружении захвата двойного листа оператор имеет возможность выбрать дальнейшие действия – повторить сканирование или продолжить

работу. Кроме того, оператор имеет возможность активировать или деактивировать, а также настроить любой из датчиков на работу внутри или вне заданной области. Несколько режимов работы датчиков позволяют настроить сканер под любую задачу, даже в случае наклеенных на документ этикеток или фотографий.

Удобство работы

Русскоязычная сенсорная панель управления сканером обеспечивает простоту и удобство работы оператора. Удобный пользовательский интерфейс, наглядные пиктограммы и широкие возможности настройки исключают необходимость пользоваться какими-либо справочными пособиями и переключать внимание на монитор рабочей станции.

Входной и выходной лотки спроектированы максимально удобно – боковые направляющие настраиваются под документы любой ширины, а саморегулирующаяся высота входного лотка подстраивается под толщину пачки документов. Благодаря автоматическому определению толщины оригинала сканер может оцифровывать пакет документов различной плотности из одной пачки. При сканировании последовательность листов в приемном лотке сохраняется, что исключает необходимость дополнительной сортировки.

Благодаря своим компактным размерам и низким шумовым характеристикам, сканеры линейки ЭЛАР СКАМАКС могут быть установлены в любом помещении и не причинят неудобств сотрудникам.

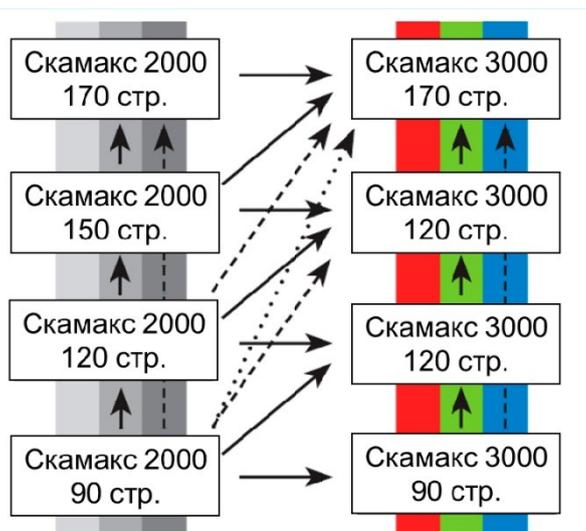
Возможность модернизации

Если в работе не требуется цветное сканирование или не нужна обратная сторона листа, то можно первоначально выбрать более экономичную полутоновую и/или одностороннюю модель ЭЛАР СКАМАКС, которую в дальнейшем легко модернизировать. Сканеры ЭЛАР СКАМАКС серии 2000 и 3000 имеют 3 направления для модернизации – по скорости, цветности и, из одностороннего в двухсторонний режим сканирования. Представленная схема наглядно иллюстрирует направления модернизации.

Если в работе не требуется цветное сканирование или не нужна обратная сторона листа, то можно первоначально выбрать более экономичную полутоновую и/или одностороннюю модель ЭЛАР СКАМАКС, которую в дальнейшем легко модернизировать. Сканеры ЭЛАР СКАМАКС серии 2000 и 3000 имеют 3 направления для модернизации – по скорости, цветности и, из одностороннего в двухсторонний режим сканирования. Представленная схема наглядно иллюстрирует направления модернизации.

Такая гибкость конфигураций позволит не приобретать оборудование «про запас», а решить. Если в работе не требуется цветное сканирование или не нужна обратная сторона листа, то можно первоначально выбрать более экономичную полутоновую и/или одностороннюю модель ЭЛАР СКАМАКС, которую в дальнейшем легко модернизировать. Сканеры ЭЛАР

СКАМАКС серии 2000 и 3000 имеют 3 направления для модернизации – по скорости, цветности и, из одностороннего в двухсторонний режим сканирования. Представленная схема наглядно иллюстрирует направления модернизации.



Такая гибкость конфигураций позволит не приобретать оборудование «про запас», а решать задачи текущего дня, модернизируя сканер именно тогда, когда это необходимо.

Удобство подключения и совместимость

Сканеры ЭЛАР СКАМАКС 2000 и 3000 поддерживают интерфейс передачи данных TCP/IP со скоростью до 1 Gigabit, совместимый со всеми наиболее распространенными операционными системами. Для простоты интеграции в архивную систему или систему обработки документов сканеры комплектуются ISIS и Twain драйверами, позволяющими беспрепятственно работать с любыми программами для сканирования, а так же комплектом для подключения к компьютеру.

Инновационные технологии

Сканеры СКАМАКС оснащены встроенными микропроцессорами, которые выполняют операции по обработке образов. Сканеры способны самостоятельно выравнивать изображения, поворачивать их на угол, кратный 90°, удалять «шумы», черные границы, преобразовывать цветные изображения в черно-белые, распознавать и пропускать пустые страницы, и многое другое.

ЭЛАР СКАМАКС серии 3000 имеют несколько форматов вывода документов за одно сканирование – от одного до трех (черно-белый + серый + цветной), то есть на выходе можно получать до 1020 изображений в минуту без существенного снижения скорости.

Сканеры ЭЛАР СКАМАКС 2000 и 3000 имеют возможность выбора скорости, что очень важно при оцифровке хрупких документов или необходимости визуально контролировать качество отсканированных образов.

Комплектация

Полный комплект поставки формируется из выбранной модели сканера с 2 импринтерами, руководства пользователя на русском языке, комплекта калибровочной бумаги из 10 листов и комплекта для подключения к компьютеру. При поставке полного комплекта обеспечивается бесплатная установка, запуск и старт-обучение персонала.

Дополнительные устройства и опции

1. Ножная педаль управления сканером

Педаля используется для управления процессом сканирования – при нажатии педали выполняется команда, заданная пользователем. С помощью специального адаптера возможно подключение двух педалей одновременно.

2. Модуль сканирования прозрачных оригиналов

Позволяет сканировать прозрачные оригиналы и документы малой плотности.

Минимальные требования на конфигурацию рабочей станции

1. Процессор: C2D от 2.0 GHz или лучше
2. Оперативная память: от 2 GB RAM
3. Сетевая карта 1000 Mbit
4. Графический адаптер: Video 256 Mb
5. Рекомендуемая операционная система - Windows XP Professional SP2 или более новая

Технические характеристики документных сканеров ЭЛАР СКАМАКС 2000 (XXX)* / ЭЛАР СКАМАКС 3000 (XXX)*

Характеристики	ЭЛАР® СКАМАКС 2000 и 3000
Тип сканера	Высокоскоростной сканер для оцифровки документов
Варианты исполнения	Цветной двусторонний ЭЛАР СКАМАКС 3000 Д90/ Д120/ Д150/ Д170 Цветной односторонний ЭЛАР СКАМАКС 3000 С90/ С120/ С150/ С170 Черно-белый двусторонний ЭЛАР СКАМАКС 2000 Д90/ Д120/ Д150/ Д170 Черно-белый односторонний ЭЛАР СКАМАКС 2000 С90/ С120/ С150/ С170
Интерфейс оператора	Русскоязычная сенсорная панель диалогового управления со встроенной диагностикой
Скорость сканирования А4 горизонтально, 200 dpi (1 сторона / 2 стороны)	90/180, 120/240, 150/300 или 170/340 стр./мин

Разрешение	150, 200, 300, 400 и 600 dpi
Формат документов Ширина Длина Толщина** Плотность*	От 28 до 317,5 мм От 60 до 2075 До 1,2мм 30 – 280г/м2
Загрузка документов	Автоматическая из пачки с возможностью ручной подачи листов
Ёмкость автозагрузчика	500 листов (80 г/кв.м) – 50 мм
Датчик двойного листа	3 пьезокерамических ультразвуковых датчика
Программные интерфейсы	ISIS, TWAIN
Аппаратные интерфейсы	TCP/IP 1 Gigabit (1000 Мбит/сек.)
Электропитание	100-240 В / 50 Гц / 3,5 А
Габариты (ШхВхД)	510 x 365 x 650 мм
Вес	38 кг

* (XXX): название модели может иметь добавочный буквенно-цифровой код, в зависимости от комплектации поставляемого сканера дополнительными программными и аппаратными модулями.

** - максимальная толщина и плотность документов зависят от состояния и эластичности бумаги.

ПРОМЫШЛЕННЫЙ СКАНЕР СКАМАКС 5000М

Источник: <http://www.scamax.ru/modelnyj-ryad/scamax-5000/>



Промышленный сканер ЭЛАР СКАМАКС 5000М является одним из самых быстрых сканеров в мире. Данное оборудование переводит в электронный вид документы размером от трамвайного билета до конструкторских чертежей со скоростью - до 460 страниц/мин. Основные преимущества двухстороннего сканера для документов ЭЛАР СКАМАКС 5000М:

Высокая скорость сканирования - до 460 страниц в минуту

- Высокоскоростной сканер ЭЛАР Скамакс 5000 позволит оцифровывать до 460 страниц А4 в минуту! И данная высокая скорость сканирования не является предельной для 5000-ой модели: квитанции и карточки меньшего формата сканируются еще быстрее!

- Простая и надёжная транспортная система сводит к минимуму потери времени на загрузку и выгрузку документов, устранение замятий бумаги, переключивание пачек, повторное сканирование, чистку и сервис — всё то, что обычно тормозит работу. Именно за счет этого достигается огромная сменная производительность при обработке реальных документов — до 50 000 листов в день.

Формат документов — от А8 до А3

- Маленький трамвайный билет, замятая платежная квитанция, обрывок газеты, библиотечная карточка, магазинный чек — двусторонний сканер ЭЛАР® Scamax 5000М оцифрует любой документ.

- Металлические скрепки на документах не выводят этот сканер из строя, а тончайшие самокопирующиеся бланки для быстрого сканера Скамакс — обычные документы.

- Сканирование документов любого формата (от А8 до А3) любой толщины (от кальки до картона) в любом разрешении (от 200 до 400 dpi) возможно как посредством автоматической загрузки из пачки документов любых типов, так и вручную — одиночной загрузкой документов в сканер.

100%-ное исключение втягивания сдвоенных листов

- Встроенный ультразвуковой датчик безошибочно остановит загрузку двойного листа тончайшей кальки и тут же пропустит толстую карточку. Для детектора двойной протяжки *промышленного сканера* для документов ЭЛАР® СКАМАКС 5000М не важна толщина или длина бумаги — он «чувствует» именно количество втягиваемых листов.

- *Двусторонний сканер* остановит слипшиеся документы еще до того, как они будут втянуты внутрь. Оператор устранит проблему за секунду, не открывая сканер и повторно не сканируя документ!

Эргономичность дизайна и удобство работы промышленного сканера Скамакс

- Фронтальная загрузка и выгрузка документов созданы специально для удобства и более высокой производительности сканировщика — оператору даже не требуется вставать.

- Специальная подставка для контрольного монитора позволит не отворачиваться от сканера.

- Особое удобство — электропривод автоматически подстраивает высоту рабочего стола СКАМАКС 5000М индивидуально для каждого оператора.

Единственный в мире двухсторонний промышленный сканер с модулем микрофильмирования

- В качестве дополнительной возможности высокоскоростного сканера ЭЛАР® СКАМАКС 5000М является возможность синхронной съёмки сканируемых документов на 16-миллиметровую микроплёнку без потери скорости сканирования и качества отсканированного образа.

- Модуль микрофильмирования удовлетворяет самым высоким требованиям к долговечности и достоверности документов архива, позволяя создавать массив страховых копий документов, не прерывая процесса сканирования.

Уникальная диалоговая сенсорная панель управления

- Сенсорная панель сканера обеспечивает небывалую простоту и удобство работы оператора. Простые пиктограммы кнопок управления, полные текстовые и графические сообщения, меню помощи и подсказки выполнены на русском языке.

- Все операции не требуют лишних операций с «мышью» и переключения внимания на монитор.

Промышленная надёжность конструкции для долговременной интенсивной работы

- Высокая скорость сканирования Скамакса превратит оцифровку огромных потоков документов в отлаженное автоматизированное производство.

- Промышленная конструкция сканера на протяжении многих лет выдерживает круглосуточный режим эксплуатации с максимальной нагрузкой.

- Неизнашиваемый, практически бесшумный механизм протяжки основан на уникальном ремневом транспорте документов при полном отсутствии роликов и пластиковых деталей в тракте сканера.

- Кажущийся несложным механизм можно сравнить только с точной механикой швейцарских часов — это лучшая немецкая сталь и тончайшая обработка. Попытки скопировать сканер в Китае, России и Польше провалились — не удалось воспроизвести качество узлов.

- Сменные элементы ЭЛАР® СКАМАКС 5000М — это только недорогие втягивающие ремешки и лампы. Именно поэтому обычные для массового сканирования затраты на «расходники» при использовании быстрого сканера ЭЛАР® СКАМАКС 5000М просто незаметны.

Промышленный сканер ЭЛАР® СКАМАКС 5000М превратит сканирование огромных потоков документов в отлаженное автоматизированное производство и на протяжении многих лет станет вашим незаменимым помощником.

**Технические характеристики промышленного сканера
ЭЛАР СКАМАКС 5000М**

Характеристики	ЭЛАР® СКАМАКС 5000М	
Тип сканера	Промышленный	
Варианты исполнения	Односторонний (simplex), двусторонний (duplex)	
Интерфейс оператора	русскоязычная сенсорная панель диалогового управления	
Скорость сканирования	A4 горизонтально (1 сторона /2 стороны)	230/ 460 стр./мин
Разрешение	200, 300, 400 dpi	
Повышение качества образов	Встроенный модуль двухкоординатного динамического контраста	
Формат документов	Ширина документов Длина документов Толщина документов	От 28 до 320 мм От 60 мм до неограниченной От кальки до картона
Загрузка документов	Автоматическая из пачки Одиночная ручная подача Высота пачки, листов (плотность бумаги 80 г/м2) Контроль двойной прояжки по длине листа Ультразвуковой контроль двойной протяжки	+ + 500 + +
Программные интерфейсы	ISIS, TWAIN	
Аппаратные интерфейсы	SCSI-3 UW / LVDS; Low Voltage Differencial Videoport	
Электропитание	115-230 В / 50 Гц / 2 А	
Габариты	Длина x ширина x высота Вес	1280 x 850 x 1050 мм 110 кг
Дополнительное оборудование	Модуль надпечатки документов после сканирования Фильтры цветовой отсечки Модуль сканирования прозрачных документов Модуль микрофильмирования (16 мм) Фильтр отсечки света Пылевой фильтр	

ЧИТАЛЬНЫЙ АППАРАТ MICROVUE RF 35

Источник: <http://www.micrography.ru/modelnyj-ryad/reading-devices/a-reading-device-microvue-rf-35/>



Читальный аппарат MicroVue RF 35

Читальный аппарат для просмотра микрофильмов 35 мм MicroVue RF 35 является настольным просмотрным аппаратом, разработанным для определенных потребительских потребностей. Показывая легкодоступные средства управления, RF35 прост в использовании и спроектирован таким образом, чтобы гарантировать надежные рабочие характеристики. RF 35 проектирует ясное и точное изображение с вертикальным просмотром, проектируя его вертикально на экране.

Технические характеристики MicroVue RF 35

Габаритные размеры	365x530x580 mm
Размер экрана	360x360 mm
Вес	10Kg
Рабочее место	320x368 mm
Кратность	12x, 27x
Цвет экрана	голубой
Проекция	задняя часть экрана
Электропитание	220/240Вольт
Лампа	13.8 В/85 Вт

Характерные особенности:

- Привлекательный, компактный дизайн
- 360 градусов вращения изображения
- Двойная линза - 12х, 27х -стандарт
- Двухнаправленная переменная скорость
- Вертикальный просмотр



EXTEK 3150 SILVER DUPLICATOR

Источник: <http://www.micrography.ru/modelnyj-ryad/duplicator-microforms/printers-3150-silver-duplicator/>



Extek 3150 — высокоскоростной дубликатор, предназначенный для копирования микрофильмов на рулонную галогеносеребряную пленку шириной 16/35/70/105 мм.

Основные преимущества Extek 3150

- Универсальный дубликатор поддерживающий любые типы рулонной пленки и позволяющий копировать пленки длиной до 35 м
- Высокая скорость дублицирования позволяет копировать до 40 тыс. метров пленки в смену

Другие особенности

- Промышленный стандарт
- Регулируемая скорость и интенсивность засветки
- Самая скоростная модель

- Надежное исполнение, долговечность
- Минимальное обслуживание и регулировка
- Самый совершенный вакуумный метод прижима пленок – гарант резкости.

- Уникальные возможности при использовании модуля последовательного программирования оптической плотности.

Технические характеристики:

Оригинал	микрофильм на галогенидо- серебряной, диазо- или везикулярной пленке на катушках 30.5 м.
Копия	на галогенидосеребряной пленке для копирования шириной 16/35/70/105 мм, катушки 305 м.
Скорость копирования	до 100 м/мин
Лампа	галогенная
Мощность лампы, Вт	250
Электропитание – В/Гц/А	220 / 50 / 8
Метод прижима пленки	вакуумный
Размеры, см	
Extek 3150	165 x 104 x 61
Extek 3150T	77 x 104 x 61
Требования к помещению	темная комната (степень освещенности определяется используемой пленкой)

Базовая комплектация:

- Аппарат Extek 3150T
- Вакуумная голова на 35 мм

Дополнительные опции:

- Вакуумная голова на 16 мм
- Петлевой модуль
- Вакуумная голова на 105 мм
- Модуль последовательного программирования оптической плотности
- Ширина пленки от конфигурации 16/35/70/105



ПРОСМОТРОВЫЙ СТОЛ SOLAR ДЛЯ 16/35 ММ МИКРОПЛЕНКИ

Источник: <http://www.micrography.ru/modelnyj-ryad/accessories/screening-buffet-for-solar-16-35-mm-microfilm/>



Просмотровый стол Solar предназначен для использования в процессе контроля качества отснятых и проявленных микрофильмов 16/35 мм. Основными преимуществами аппарата являются: простота использования, ручная или автоматическая перемотка пленки, изменяемая скорость движения пленки (быстро/медленно), ножная педаль управления.

Технические характеристики

Используемые форматы пленки	16/35 мм катушечная микропленка, 3М картриджи, 35мм картриджи
Перемотка пленки	Ручная или автоматическая
Электропитание	230 Вольт, 50 Гц, 100 Ватт
Габаритные размеры	400 x 300 x 190 мм
Вес	5 кг

МИКРОСКОП MESSWELK – 75X

Источник: <http://www.micrography.ru/modelnyj-ryad/accessories/microscope-messwelk-75kh-/>



MESSWELK – 75X – маленький, легкий, удобный, высококачественный переносной измерительный микроскоп для точных измерений со светлой оптикой и первостепенной разрешающей способностью.

Технические характеристики

- Кратность увеличения - 75x
- Поле зрения - Ø 3,30 мм
- Измерительная область - 3 мм

Исполнение

- Измерительная шкала - вращающаяся
- Вращающееся внешнее кольцо с делением шкал 0,1 мм
- Резиновый глазной окуляр
- Нижняя часть корпуса из плексигласа для оптимального проникновения света
- Металлический корпус матовый для исключения бликов
- Размер - Ø 41,5 x 122 мм

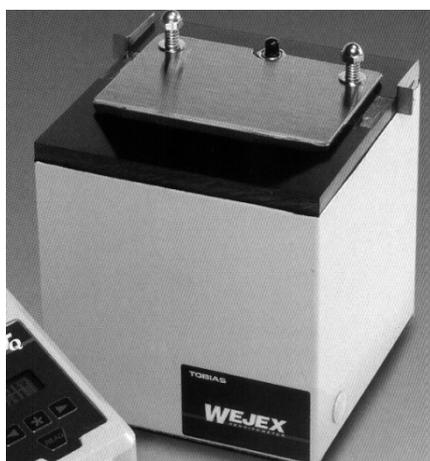
Комплектация поставки

- Измерительный микроскоп
- Измерительная шкала - стандартная
- Футляр



СЕНСИТОМЕТР WEJEX 1S

Источник: <http://www.micrography.ru/modelnyj-ryad/accessories/sensitometr-wejex-1s/>



Сенситометр Wejex 1S предназначен для тестовой экспозиции микрофильма. Экспозиция выполняется при помощи надежного источника света со стабильными параметрами. Встроенный блок компенсации отслеживает и предотвращает изменения интенсивности свечения, вызванные значительными колебаниями в сети питания и старением источника. На тестовом микрофильме проводится экспозиция с нанесением «серого клина» состоящего из 21 шага от темного до светлого с приращением 0.15 D. После химико-фотографической обработки микрофильма значения оптической плотности указанные пленке необходимо сравнить с реальными значениями, полученными на денситометре.

Технические характеристики

Размер «клина»	21 шаг
Длительность экспозиции	0.1, 0.2, 0.4, 0.8, 1.6, 3.2 с
Электропитание	220 В, 50 Гц, 25 Вт
Размеры	241 x 203 x 114 мм
Вес	2.7 кг

ЦИФРОВОЙ ДЕНСИТОМЕТР X-RITE 301

Источник: <http://www.micrography.ru/modelnyj-ryad/accessories/digital-densitometer-x-rite-301/>



Цифровой денситометр X-Rite 301 предназначен для измерения оптической плотности микроформ. X-Rite 301 предоставляет высочайшую точность, повторяемость и аккуратность измерений оптической плотности до 5.0D черно-белых пленок, что позволяет разглядеть тончайшие и незаметные детали изображения, чего нельзя сделать невооруженным взглядом.

Основными техническими характеристиками данного оборудования являются: наличие подсвечиваемой базовой площадки 9x21 см, питание –230 В, 80 ВА, рабочая температура +10-/ +40 С, габаритные размеры устройства достигают 270x380x160 мм при массе 3,8 кг.

Особенности:

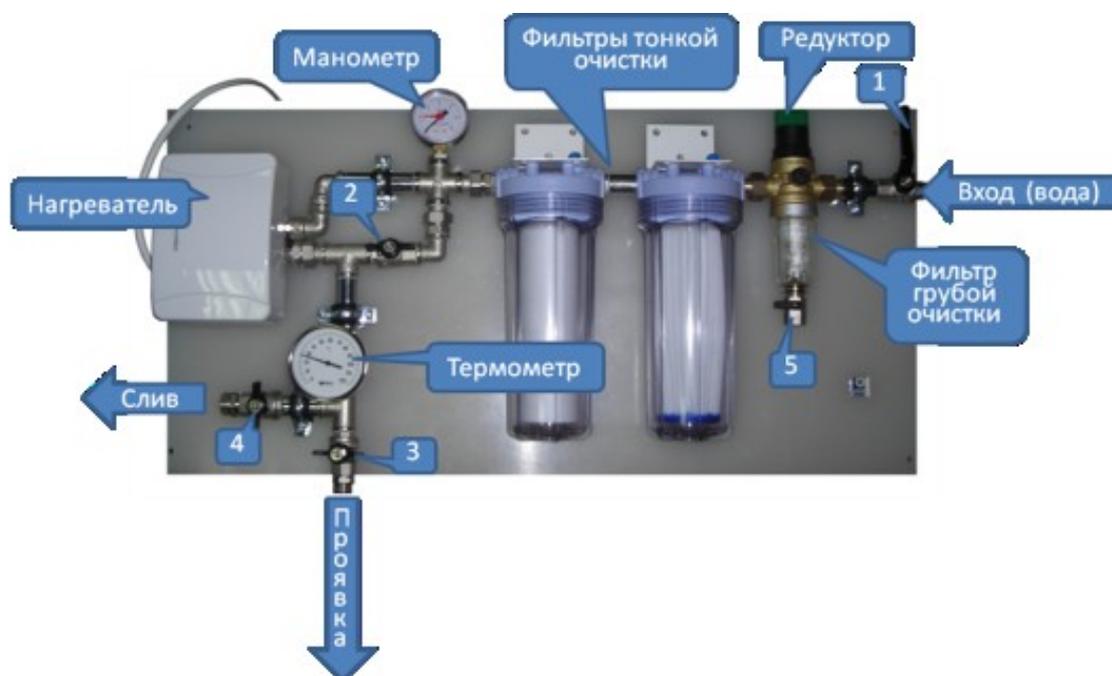
- электронная память для хранения абсолютных и относительных значений оптической плотности «серебряных» микропленок;
- прибор 3-го поколения;
- автоматическое обнуление;
- автоматическое измерение и вычисление относительного значения оптической плотности;
- просмотрный столик с подсветкой;
- модульная конструкция;

диапазон измеряемой оптической плотности: 0 до 5.0 D (апертура 2 и 3 мм, опция – 5 мм) стабильность scale-фактора: 1.0 %.

ПУНКТ ВОДОПОДГОТОВКИ ЭЛАР

Источник: <http://www.micrography.ru/modelnyj-ryad/accessories/paragraph-water-treatment-elar/>

Пункт водоподготовки предназначен для подачи воды в системы промывки пленки провочных машин настольного и напольного исполнения. Основными техническими характеристиками данного оборудования являются: потребляемая мощность – 4.4 кВт; номинальное напряжение – 230 В; входное водяное давление – не менее 2 бар; расход воды - от 1,5 до 10 литров в мин.; температура нагрева воды – до 38⁰С.



ЗМІСТ

Передмова.....	1
Роб Шарп: В защиту миграции.....	2
Флэшки в 2 раза опаснее, чем вы думаете	4
Как продлить жизнь «флэшкам».....	6
Как защитить и сохранить данные на портативном носителе.....	9
Надежно ли хранение данных на CD/DVD дисках?.....	16
Микрографическая камера УКМ–3.....	19
Универсальный сканер микрофильмов 16/35 и микрофиш А6 Imagelink 2400/3000 DV Plus.....	21
Поточный сканер СКАМАКС 2000/3000.....	22
Промышленный сканер Скамакс 5000М	28
Читальный аппарат MicroVue RF 35.....	32
Exttek 3150 Silver Duplicator.....	33
Просмотровый стол Solar для 16/35 мм микроплёнки.....	35
Микроскоп MESSWELK – 75X.....	36
Сенситометр Wejex 1S.....	37
Цифровой денситометр X-Rite 301.....	38
Пункт водоподготовки ЭЛАР.....	39