ОБЗОР ПЕРСОНАЛИЗИРОВАННЫХ ФЛЕШ-НАКОПИТЕЛЕЙ КОРПОРАТИВНОГО КЛАССА

Королёв В.Ю.
Центр таймерных вычислительных систем Института кибернетики им. В.М. Глушкова Национальной академии наук Украины (Киев, ноябрь, 2008)
info@tau-systems.org.ua

В настоящее время флеш-накопители информации с USB-интерфейсом стали массовым мобильным устройством хранения данных, способствующих увеличению производительности труда пользователей персональных компьютеров (ПК). Расширению сферы применения флеш-накопителей на потребительском рынке способствуют: снижение относительной стоимости гигабайта памяти флеш накопителей, рост скорости передачи данных и объемов памяти при улучшении массогабаритных характеристик. Эти тенденции, по мнению аналитиков ICinsight.com, сохранятся до начала 2009 года и будут обусловлены следующими причинами:

- Перепроизводство устройств памяти класса DRAM в 2007 году вынудило компании переключиться на производство флеш памяти.
- Уменьшение покупательной способности потребителей информационной техники в США - крупного потребителя флеш чипов - по причине сначала ипотечного, а затем и финансового кризисов, в совокупности стало дополнительной причиной избытка флеш-памяти на рынке.

Указанные факторы показывают, что флеш-накопители будут доступными и востребованными мобильными устройствами хранения деловой и личной информации в течение нескольких ближайших лет.

Опрос, выполненный по заказу компании SanDisk, позволил определить, что около 77% служащих используют, купленные ими флеш накопители, как для личных, так и для связанных с работой целей. Причем сохраняемые данные относятся к категории чувствительной информации: записи о клиентах (25%), финансовая информация (17%), бизнес-планы (15%), контактная информация сослуживцев (13%), маркетинговые планы (13%), интеллектуальная собственность (6%), исходные коды программ (6%).

Опрос выявил также, что возможность переносимости информации с флеш-накопителей, оснащенных USB-интерфейсом, представляет серьезную угрозу потери и безопасности данных. Приблизительно один из десяти (12%) пользователей корпоративных ПК сообщил, что ему случалось находить флеш-накопитель в общественных местах. Более того, на вопрос о трех наиболее вероятных действиях, которые служащие предприняли, обнаружив флеш-накопитель в общественном месте, 55% указали, что они просмотрели бы данные.

Другой опрос, проведенный в 2007 году компанией Fortune в Великобритании среди ИТ-профессионалов, выявил, что две третьи ИТ-профессионалов, работающих с мобильными накопителями, не используют технологии защиты хранимых данных, несмотря на понимание возможных угроз.

Поэтому актуальной научно-прикладной задачей является разработка персонализированных флеш-накопителей с USB-интерфейсом, у которых качество защиты информации минимально зависит от человеческого фактора.

Приведем краткий обзор существующих технических решений, призванных повысить качество защиты информации в коммерческих и государственных организациях.

USB флеш-накопители фирмы Kingston

Флеш накопители с USB-интерфейсом фирмы Kingston с аппаратным шифрованием (AES-256) потока данных между устройством и хост ПК представлены семейством продуктов DataTravel: Vault (Two Partions), Vault Privacy, Secure, Privacy, Secure Privacy, Black Box. Серия Vault (Two Partions) поддерживает открытый и закрытый разделы флеш памяти, остальные продукты — только закрытый. Доступ (инициализация) к закрытой части флеш памяти выполняется с помощью консоли накопителя MyDataZone вводом сильного пароля с клавиатуры. Фабричная прошивка предоставляет 10 попыток ввода пароля, после чего устройство блокируется и его дальнейшее использование возможно только после переформатирования флеш памяти. Продукты Two Partions предполагают, что изделие находится в частной собственности физического лица, все остальные серии — в собственности организации. Продукты семейства Black Box разработаны в соответствии со стандартом FIPS-140 (уровень 2 Национального института стандартов /НИС/ США) для использования в государственных организациях.

Стандарт FIPS 140-2 утвержден американским и канадским правительствами. При тестировании изделий проверяют их криптографические и шифрующие модули на соответствие заявленным спецификациям. Это дорогостоящий процесс в ходе которого проверяют включенные в продукт подсистемы безопасности устройства от сторонних производителей, а также выполняют тестирования на наличие черных ходов, недостатков, и др. слабых мест. FIPS 140-2 становится требованием для многих государственных учреждений и корпораций, заинтересованных в сохранении конфиденциальности чувствительных данных.

Для повышения производительности работы флеш-накопителей семейства DataTravel в устройствах используется два независимых процессора: контроллер флеш памяти и USB-интерфейса и криптографический сопроцессор. Ключи для криптографических алгоритмов обеспечивает генератор истинно случайных чисел. Изделие имеет стальной водонепроницаемый корпус.

Основные характеристики флеш накопителей фирмы Kingston с аппаратной системой защиты информации представлены в табл. 1.

Таблица 1. Характеристики USB-флеш накопителей фирмы Kingston семейства DataTravel Vault

Ёмкость, ГБ	Стоимость изделия семейства DataTravel, долл. США					Скорость чтения/ записи, МБ/с
	Vault	Privacy	Secure	Secure Privacy	Black Box	
1	68	79	—	—	—	15/10
2	104	116	—	—	130	24/10
4	164	173	162	177	193	
8	270	294	277	300	327	
16	507	527	—	—	—	

Серым цветом выделен столбик, соответствующий серии продуктов DataTrave Vault Two Partions, которые имеют открытый и закрытый разделы.

Таблица 2. Сравнение всех флеш-накопителей фирмы Kinstone с аппаратным шифрованием потока данных между устройством хранения информации и хост-ПК

Название продукта	**Предполагаемый пользователь**	**Характеристики защищенности продукта**	**Ёмкость памяти, ГБ**	**Скорость чтения/записи, МБ/с**
DataTraveler Secure	Корпорация	256-AES аппаратное шифрование, ПО защиты доступа к файлам (MyDataZone)	1ГБ - 8ГБ	**1ГБ - 4ГБ:** До 24МБ/с До 20МБ/с **8ГБ:** До 24МБ/с До 10МБ/с
DataTraveler Secure - Privacy Edition	Корпорация	Доступ к зашифрованному содержимому памяти по паролю	1ГБ - 8ГБ	**1ГБ - 4ГБ:** До 24МБ/с До 20МБ/с **8ГБ:** До 24МБ/с До 10МБ/с
DataTraveler Vault	Государственная структура	256-AES аппаратное шифрование, сборка в США, совместимость с TAA, ПО защиты доступа к файлам (DTVaultLock)	1ГБ - 16ГБ	**2ГБ - 16ГБ:** До 24МБ/с До 10МБ/с **1ГБ:** До 15МБ/с До 10МБ/с
DataTraveler Vault - Privacy Edition	Государственная структура	Доступ к зашифрованному содержимому памяти по паролю, сборка в США, совместимость с TAA	1ГБ - 16ГБ	**2ГБ - 16ГБ:** До 24МБ/с До 10МБ/с **1ГБ:** До 15МБ/с До 10МБ/с
DataTraveler BlackBox FIPS 140-2 ур. 2	Государственная структура	Доступ к зашифрованному содержимому памяти по паролю, FIPS 140-2 уровень 2, самотестирование систем защиты	2ГБ - 8ГБ	До 24МБ/с До 20МБ/с

USB- флеш накопители фирмы SanDisk

Линейка USB флеш накопителей SanDisk с системой повышенной защиты информации представлена тремя продуктами под торговой маркой SanDisk Cruzer: Professional, Enterprise, FIPS. Все устройства этой линейки обеспечивают аппаратное шифрование потока данных алгоритмом AES с ключами длинной 256 бит, между USB-накопителем и хост-компьютером. Флеш-накопители серии Professional имеют открытую (общедоступную) и закрытую части памяти, а Enterprise и FIPS — только закрытую. Доступ пользователя к закрытой части осуществляется вводом сильного пароля с клавиатуры ПК. Использование накопителей серии Professional предполагает, что устройство находится в частной собственности физического лица. Продукты серии Enterprise и FIPS должны быть собственностью организации, которая будет выдавать их служащим. Для управления жизненным циклом флеш-накопителей (создание записи о флеш пользователе, контроль данных, копируемых на носитель, удаление записи из системы) Enterprise и FIPS компания SanDisk предлагает программный комплекс CMC (Central Management and Control).

Накопители SanDisk Cruser FIPS отличаются от Enterprise полным соответствием нормам FIPS 140-2 (уровень 2 НИС США), что позволяет использовать их не только в коммерческих, но и в государственных организациях. В накопителях FIPS для исключения доступа к ключам шифрования микросхема запрессована в эпоксидный компаунд.

В табл. 1 представлены основные характеристики рассмотренных продуктов фирмы SanDisk.

Таблица 1. Основные характеристики флеш накопителей SanDisk Cruzer с аппаратным шифрованием

Название продукта семейства SanCruser	Ёмкость памяти, ГБ	Стоимость, дол. США	Скорость чтения/записи данных, МБ/с	Наличие открытой и закрытой зон
Professional	1	63,95	24/20	открытая и закрытая зоны
	2	76,41		
	4	91,73		
	8	165,41		
Enterprise	1	63,99		только закрытая зона
	2	99,22		
	4	137,99		
	8	243,99		
FIPS	1	69,24		
	2	112,99		
	4	154,99		
	8	263,99		

USB-флеш накопители фирмы IronKey

Флеш-накопители компании IronKey обеспечивают аппаратное шифрование AES-128 режим CBC, что, по мнению разработчиков, достаточно для защиты чувствительной коммерческой информации. Семейство продуктов IronKey состоит из серий: Basic, Personal и Enterprise. В маркетинговых материалах компания IronKey подчеркивает, что в её изделиях используется опыт разработок военного назначения. Поэтому все семейства продуктов соответствуют стандартам НИС США FIPS: 140-2 (уровень 2); 186-2; 197.

Аутентификация пользователя флеш-накопителя обеспечивается вводом символов с клавиатуры с помощью панели управления паролями. В случае 10 последовательных неудачных попыток ввода пароля флеш-память надежно стирается, что гарантируется запатентованым IronKey алгоритмом. Хеш функции (SHA-256) паролей хранятся в специализированном чипе, выполняющем криптографические операции. Ключи криптографических алгоритмов: 128 бит DRNG, PKI 2048-бит RSA обеспечивает генератор истинно случайных чисел. Все серии накопителей фирмы IronKey предоставляют доступ к файлам только после аутентификации пользователя.

Серии накопителей IronKey: Basic, Personal, Enterprise наращивают информационные сервисы в порядке перечисления. Накопители серий Basic и Personal предназначены для личного использования и имеют одинаковую стоимость. Basic серия обеспечивает минимальный сервис с помощью оболочки Control Panel: управление файлами и обновлениями, резервное копирование, смена паролей. Серия Personal добавляет к сервисам Basic возможности безопасной работы в Интернете на основе специально сконфигурированной переносимой версии браузера Mozila FireFox: промежуточные данные Web-сессий сохраняются на флеш, предоставляются также сервисы сохранения паролей и проверки сайтов на безопасность.

Накопители серии Enterprise предназначены для организаций и сопровождаются программным обеспечением для поддержки политик управления жизненным циклом накопителей, резервным сохранением данных с нескольких устройств, системой идентификации пользователей с помощью разовых паролей (на одну сессию) фирмы RSASecurID, а также он-лайн поддержкой компании IronKey.

Накопители IronKey используют NAND SLC флеш память, обеспечивающую более 10^5 циклов чтения записи. Изделия имеет стальной корпус, водонепроницаемы в соответствии с военным стандартом, микросхемы запечатаны в эпоксидный компаунд, защиту от физического проникновения обеспечивает встроенный детектор. В табл. 1 приведена стоимость накопителей и скорости передачи данных.

Таблица 1. Характеристики флеш-накопителей IronKey Basic и Personal

Ём-кость, ГБ	Стоимость, долл. США	Скорость чтения/записи, МБ/с
1	79	30/20
2	109	
4	149	
8	299	

для серии Enterprise нет данных на сайте производителя.

USB-флеш накопители фирмы Kanguru

Фирма Kanguru предлагает две серии накопителей с аппаратным шифрованием потока данных AES-256: Defender и Defender Pro. Аутентификация пользователя осуществляется вводом пароля с клавиатуры. Количество попыток ввода пароля равно десяти. Принципиальное различие между сериями заключается в скорости передачи данных, которую определяет выбор NAND флеш-памяти. Для Defender — это MLC-технология, а для Defender Pro — SLC. Обе серии флеш-накопителей обеспечивают 10^4 циклов чтения-записи. Основные характеристики флеш накопителей фирмы Kanguru сведены в табл. 1.

Таблица 1. Характеристики USB-флеш накопителей с аппаратным шифрованием потока данных

Ём-кость, ГБ	Defender		Defender Pro	
	Стоимость, долл. США	Скорость чтения/записи, МБ/с	Стоимость, долл. США	Скорость чтения/записи, МБ/с
1	49,95	15/7	64,95	30/15
2	69,95		84,95	
4	99,95		129,95	
8	149,95		229,95	
16	249,95		—	

На сегодняшний день только серия MicroDriveAES прошла сертификацию FIPS-140 уровень 2. Основные характеристики флеш-накопителей серии MicroDriveAES сведены в табл. 2.

Таблица 1. Характеристики флеш-накопителей MicroDriveAES Kanguru

Ём-кость, ГБ	Стоимость, долл. США	Скорость чтения/записи, МБ/с
1	65,99	6/5
2	89,95	
4	119,95	
8	199,95	

Также фирма Kanguru предлагает серию накопителей BioAES с двухфакторной аутентификацией пользователя: сканирование отпечатка пальца и ввод пароля с клавиатуры. Разрешающая способность сканера 500 dpi, вероятность ложного срабатывания 10^{-6}, вероятность неверного отклонения доступа 10^{-4}. Количество хранимых флеш-накопителем отпечатков пальцев равно десяти. Основные характеристики флеш-накопителей серии BioAES приведены в табл. 2.

Таблица 2. Характеристики USB-флеш накопителей Kanguru BioAES

Ёмкость, ГБ	Стоимость, долл. США	Скорость чтения/записи, МБ/с
1	79,95	10/5
2	99,95	
4	129,95	
8	179,95	

Все рассмотренные серии флеш-накопители фирмы Kanguru проходят сертификацию по стандарту FIPS-140 уровень 2.

USB-флеш накопители Pivot plus фирмы Imation

Серия Pivot plus фирмы Imation обеспечивает аппаратное шифрование AES-256 всех данных накопителя. Аутентификация пользователя обеспечивается вводом пароля с клавиатуры, который должен состоять как минимум из 7 букв и цифр. В случае 7 последовательных неудачных попыток аутентификации устройство блокируется. В серии Pivot plus все данные сохраняются в закрытой зоне накопителя. Предусмотрен также мастер-пароль для использования накопителей в вычислительной сети корпорации. Скорость передачи данных производитель не указал.

В табл. 1 представлены характеристики накопителей серии Pivot plus.

Таблица 1. Характеристики USB-флеш накопителей фирмы Imation

Ём-кость, ГБ	Стоимость, долл. США
1	67
2	109,99
4	135,99
8	219,99
16	н/д

USB-флеш накопители фирмы Verbatim

Фирма Verbatim выпустила накопители серии Store 'n' Go с аппаратным шифрованием потока данных по алгоритму AES. В Европе это серии Business Secure (AES-256) и Executive (AES-128). Предлагаются в США 3 серии: Corporate Secure FIPS Edition (AES-256 ECB; FIPS-140 lev.2), Corporate Secure (AES-256), PRO (AES-256). Аутентификация пользователя выполняется с помощью ввода пароля с клавиатуры, количество попыток равно десяти. Серия PRO поддерживает открытую и закрытую зоны флеш-памяти с помощью программы V-Safe Security, а Corporate Secure — только закрытую. Серия Store 'n' Go Corporate Secure совместима с ПО mTrust, предназначенного для централизованного управления и контроля корпоративных мобильных накопителей данных. Основные технические характеристики накопителей Store 'n' Go серий с аппаратной защитой информации сведены в табл. 1.

Таблица 1. Техническо-экономические характеристики флеш-накопителей фирмы Verbatim, предлагаемые в Европе

Ёмкость, ГБ	Business Secure		Executive	
	Скорость чтения/записи, МБ/с	Стоимость, долл. США	Скорость чтения/записи, МБ/с	Стоимость, долл. США
1	11/8	н/д	30/12	н/д
2		н/д		н/д
4		н/д		н/д
8		н/д		н/д
16		н/д		н/д

Таблица 2. Техническо-экономические характеристики флеш-накопителей фирмы Verbatim, предлагаемые в США

Ёмкость, ГБ	Скорость чтения/записи, МБ/с		Corporate Secure FIPS Edition	Corporate Secure	PRO
	Corporate Secure	PRO	Стоимость, долл. США	Стоимость, долл. США	Стоимость, долл. США
1	24/20	30/12	36,78	36,78	—
2			144,79	144,79	—
4			255,92	255,92	31,23
8			284,38	269,27	45,83
16			—	—	76,99

В накопителях FIPS для исключения доступа к ключам шифрования микросхема запрессована в эпоксидный компаунд.

USB-флеш-накопители mxisecurity.com

Флеш-накопители компании mxisecurity — это продукты для государственных и коммерческих организаций, которым требуется высокий уровень защиты конфиденциальной информации от несанкционированного доступа. На флеш-памяти поддерживается два раздела: закрытый, доступ к которому осуществляется после аутентификации и открытый, где разрешен доступ только для чтения.

Фирма Mxisecurity производитель флеш-накопителей с аппаратным шифрованием (осуществляемым контролером накопителя без участия центрального процессора хост-ПК) потока данных по алгоритму AES-256 CBC, решила дополнить стандартную парольную аутентификацию с ограниченным количеством попыток биометрической аутентификацией (для новых изделий). Таким образом, новые устройства имеет двухфакторную аутентификацию пользователя и трехфакторную для запуска программ с накопителя (пароль, отпечаток пальца и уникальный цифровой номер-идентификатор флеш).

Выпускается четыре серии продуктов: StealthMini(ClipDrive Secure и ClipDrive), StealthMXP, StealthMXP Passport, OutBarkerMXP. Сопоставление характеристик продуктов приведено в табл. 1. Продукты StealthMXP и OutBarkerMXP поддерживают аутентификацию нескольких (до пяти) пользователей.

Табл. 1. Сравнение характеристик продуктов для безопасного транспорта информации mxisecurity

№	Название продукта	Парольная аутентификация	Биометрическая аутентификация	Аппаратно-программное шифрование	Цифровые идентичности и криптосервисы	Управление жизненным циклом	Соответствие FIPS-140, уровень 2
1	Stealth Mini	+		+		+	
2	StealthMXP Passport	+		+	+	+	+
3	StealthMXP	+	+	+	+	+	+
4	OutBarkerMXP	+	+	+	+	+	+

Управление жизненным циклом осуществляется с помощью разработанного фирмой mxisecurity ПО Access Enterprise.

Табл. 2. Объём памяти и стоимость ClipDrive Secure

Объём памяти, ГБ	Стоимость, долл. США
0,128	35,99
0,256	39
0,512	45
1	59
2	109
4	169

Табл. 3. Объём памяти и стоимость ClipDrive

Объём памяти, ГБ	Стоимость, долл. США
0,256	25,86
0,512	29,89
1	44,26
2	74,86
4	133,76

Табл. 4. Объём памяти и стоимость Stealth MXP

Объём памяти, ГБ	Стоимость, долл. США
0,512	187
1	189
2	212
4	257
8	389
16	598

Табл. 5. Объём памяти и стоимость Stealth MXP Passport

Объём памяти, ГБ	Стоимость, долл. США
0,512	129
1	139
2	149
4	189
8	339
16	575

Флеш-накопители серии OutBarkerMXP предполагают ношение пользователем всего десктопа с собой для чего необходим большой объем памяти. Конструктивно накопители серии OutBarkerвыполнены в форм-факторе цифрового бумажника.

Табл. 6. Объём памяти и стоимость OutBarker MXP

Объём памяти, ГБ	Стоимость, долл. США
80	379
120	429
160	479
250	549
320	669

Продукты серии OutBarkerMXP снабжаются внутренним источником питания для работы при пониженном питании USB-порта, что характерно для некоторых ноутбуков в автономном режиме работы.

Из всех рассмотренных флеш-накопителей с аппаратной защитой информации, продукты StealthMXP и OutBarkerMXP фирмы mxisecurity характеризуются самым полным набором криптосервисов: спецконтейнеры для симметричных, ассиметричных ключей и разовых хешированных ключей (HOTP), разовая генерация паролей (OATH), шифрование AES-256 CBC, хеш-функции SHA-1 и SHA-256, переключаемый HMAC, RSA шифрование, цифровая подпись и генератор случайных чисел и ключей (1024/2048/3072 битные), генеторатор токенов для SAML WS-trust, поддержка совместимости с системами RSAsecureID и Entrust. Поэтому фирма mxisecurity утверждает, что её продукты удовлетворят самых требовательных пользователей.

К сожалению на сайте фирмы (www.mxisecurity.com) отсутствуют данные о скорости чтения/записи флеш-накопителей.

Выполним анализ собранных данных для флеш накопителей корпоративного назначения средней ёмкости 4 ГБ. Усредненные характеристики мобильных накопителей информации с USB интерфейсом с аппаратной защитой информацией представлены в табл. 1.

Таблица 1. Характеристики USB-флеш накопителей корпоративного класса с объемом памяти 4 ГБ и аппаратной защитой информации

№	Фирма производитель	Стоимость, долл. США	Скорость чтения|записи, МБ/с	Серверное ПО для УЖЦ накопителя
1	Kingston	191	24|10	—
2	SanDisk	144	24|20	CMC
3	IronKey	149	30|20	my.IronKey.com
4	Verbatim	130	30|12	mTrust
5	Kanguru	130	30|15	—
6	Imation	133	н/д	—
7	Mxisecurity	189	н/д	ACCESS Enterprise

УЖЦ — управление жизненным циклом.

Рассмотренные корпоративные флеш накопители используют аутентификацию пользователя с помощью ввода надежного пароля с клавиатуры ПК с ограниченным числом попыток, пакеты данных между флеш и ПК шифруются алгоритмом AES-256, файлы хранятся в закрытой зоне памяти устройства. Изделия, позиционируемые на рынке как профессиональные, поддерживают также открытую зону, размер которой устанавливается в настройках мобильного устройства хранения. Таким образом, в случае кражи, подмены или потери накопителя чувствительная информация остается недоступной злоумышленникам. Аппаратное шифрование потока данных между хост-компьютером и флеш-накопителем обеспечивает существенное увеличение защищенности чувствительной информации при работе вне безопасной корпоративной сети, в которой специализированные программы контролируют потоки данных и порты. Поэтому не существует исключительно высокоуровневых программных решений, которые прошли сертификацию FIPS.

Рассмотрим функциональные возможности характеризующие накопители с аппаратной защитой информации.

1. Характеристики системы защиты информации накопителей.
   1.1. Аутентификация пользователя.
      1.1.1. Однофакторная (имя пользователя и пароль, вводимый с клавиатуры).
      1.1.2. Двухфакторная (сканер отпечатка пальца, имя пользователя и пароль, вводимый с клавиатуры).
   1.2. Аппаратный алгоритм шифрования.
      1.2.1. AES с 256-битными ключами шифрования).
         1.2.1.1. CBC-способ шифрования блоков.
         1.2.1.2. EBC-способ шифрования блоков.
      1.2.2. AES с 128-битными ключами шифрования.
         1.2.2.1. CBC-способ шифрования блоков.
         1.2.2.2. EBC-способ шифрования блоков.
   1.3. Способ разграничения и защиты доступа к памяти флеш-накопителя.
      1.3.1. Использование только закрытого раздела памяти с зашифрованными данными пользователя.
      1.3.2. Использование открытого раздела памяти (для чтения и записи либо только для чтения) и закрытого раздела памяти с зашифрованными данными пользователя.
   1.4. Сертификация.
      1.4.1. Сертифицированные по стандарту FIPS-140-2 уровень 2.
      1.4.2. Не сертифицированные.
   1.5. Способ реализации алгоритма генерации случайных чисел.
      1.5.1. Алгоритм генерирования случайных чисел в соответствии с криптографическими критериями качества.
      1.5.2. Алгоритм преобразование данных физического процесса в случайную последовательность в соответствии с криптографическими критериями качества.
   1.6. Реализация криптосервисов.
      1.6.1. Базовый набор сервисов (хеш-функции, ассиметричные алгоритмы и т.п.).
      1.6.2. Расширенный набор сервисов (базовые сервисы, разовые ключи, поддержка защищенного запуска приложений и пр.).
2. Эксплуатационные характеристики.
   2.1. Возможность записи уникального идентификатора в память флеш-накопителя (работы систем управления жизненным циклом накопителей).
   2.2. Количество пользователей флеш-накопителя.
      2.2.1. Один пользователь.
      2.2.2. Несколько пользователей.
   2.3. Портабельное программное обеспечение и ПО для управления жизненным циклом накопителя.
   2.4. Объем памяти устройства хранения.
   2.5. Скорость чтения/записи флеш-накопителя.
      2.5.1. Низкая (6/5).
      2.5.2. Средняя (15-12/10).
      2.5.3. Высокая (30/25).
   2.6. Защита от воздействий окружающей среды и механических воздействий.
      2.6.1. Базовая защита (пластиковый корпус).
      2.6.2. Высокая защита: влагостойкойкий и ударопрочный корпус.

Приведенный набор характеристик реализован только в отдельных накопителях некоторых фирм-производителей, а большинство изделий, представленных на рынке, удовлетворят лишь ограниченному множеству приведенных показателей.

Разработчики корпоративных флеш-накопителей гарантируют безопасность работы служащих с этими мобильными устройствами и вне офиса на любых компьютерах (не являющихся частной собственностью организации) с помощью подсистем обнаружения хакерских атак, объектом которых является процесс обмена данными и командами с компьютером. Заметим, что в настоящее время существует множество программ-шпионов, позволяющих получить пароль, введенный с клавиатуры. Как правило, пароли меняются не чаще раза в месяц. Если внутри сети организации ведется учет используемого ПО и проверка файлов, приносимых служащими, то вне корпорации гарантировать защиту процесса ввода пароля практически невозможно. Следовательно, при использовании флеш-накопителей вне организации аутентификация пользователя с помощью ввода сложных паролей не может гарантировать защиту чувствительной информации от несанкционированного доступа.

На потребительском рынке представлено множество мобильных устройств хранения данных с биометрической защитой — со сканирующей линейкой протяжного типа (разрешающая способность около 500 dpi) для считывания отпечатка пальца. В ЦТВС ИК тестировалось два флеш накопителя потребительского класса от разных производителей с биометрической защитой. Чтобы обеспечить надежность ввода отпечатка пальца, производители предлагают ввести отпечатки нескольких пальцев левой и правой рук в систему и несколько вариантов изображений каждого отпечатка пальца. Количество попыток аутентификации пользователя с помощью ввода отпечатка пальца неограниченно, что позволило в некоторых случаях войти в систему другому пользователю с 30-40 попыток. Кроме того, биометрическая система дублируется аутентификацией с клавиатуры, что с точки зрения надежности приравнивает биометрическую систему к рассмотренной выше, базирующей на вводе пароля с клавиатуры. Отметим, что эти устройства не имеют сертификации НИС США.

Интересным решением является разработка фирмы Corsair — PadLock USB-флеш-накопитель со встроенной панелью для набора PIN-кода. Недостатком такого решения является ограниченное количество комбинаций (10^4) и относительное неудобство эксплуатации, связанное с необходимость набора цифр PIN-кода с десяти миниатюрных кнопок, расположенных в два параллельных ряда на корпусе накопителя вставленного в USB-порт.

Аутентификации пользователя с помощью BIK-технологии, не изменяя суть аутентификации с помощью пароля, позволяет увеличить защищенность хранимой информации, так как введенные секретные BIK-ключи не покидают устройство. Первый этап аутентификации использует только питание USB-порта компьютера, процедура проверки ключа выполняется контроллером внутри устройства. На втором этапе в устройство поступают данные, введенные с клавиатуры, а на выходе с устройства в высокоуровневую программу поступает сложный пароль. Таким образом, использование BIK-ключа для аутентификации пользователя флеш-накопителя позволяет защитить процесс ввода пароля от считывания шпионскими программами при работе на компьютере, не контролируемом корпоративной системой безопасности.