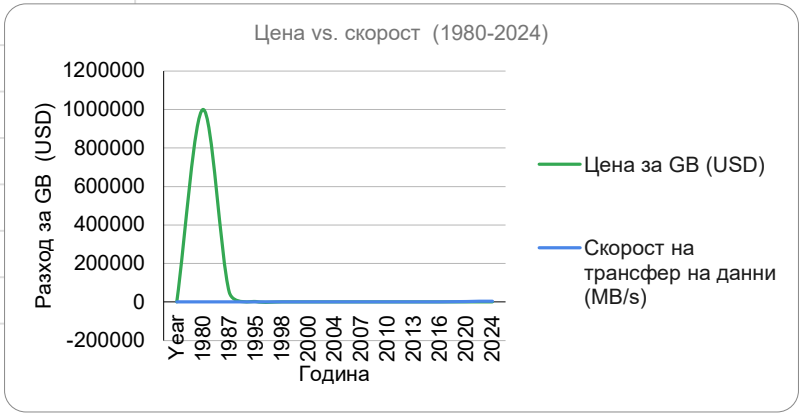
Year	Storage Type	Cost per GB ($)	Transfer Speed (MB/s)
1980	Hard Disk Drive (5.25")	1,000,000.00	0.5
1987	Hard Disk Drive (3.5")	50,000.00	2
1995	Zip Drive	2,000.00	1.4
1998	Compact Flash	400	4
2000	USB 1.1 Flash Drive	100	1
2004	USB 2.0 Flash Drive	20	30
2007	1TB External HDD	0	60
2010	SATA III SSD	2	500
2013	USB 3.0 Flash Drive	0.8	100
2016	NVMe External SSD	0.35	1000
2020	Thunderbolt 3 SSD	0.2	2800
2024	USB4 / Thunderbolt 4	0.08	3500



Интерфейс	Макс. теоретична скорост	Типична латентност	Типична употреба
USB 2.0 (Hi-Speed)	480 Mbit/s (~60 MB/s)	Висока (ms)	USB флаш памети, периферни устройства
USB 3.0 (SuperSpeed)	5 Gbit/s (~625 MB/s)	Средна	Външни HDD, USB флаш, уеб камери
USB 3.1 Gen 2 (SuperSpeed+)	10 Gbit/s (~1 250 MB/s)	Средна-ниска	Външни SSD, док станции
SATA III	6 Gbit/s (~600 MB/s)	Средна (~100 µs)	Вътрешни/външни SSD, 2.5" HDD (чрез USB мост)
NVMe over PCIe (Gen 4/Gen 5)	До 14 000 MB/s	Много ниска (~10–20 µs)	Високопроизводителни външни SSD
Thunderbolt 3/4	40 Gbit/s (~5 000 MB/s)	Ниска	Професионални външни масиви, видео продукция

Характеристика	USB Flash Drive	Външен SSD	Външен HDD	SD карта	CD/DVD
Капацитет	16 GB – 1 TB	250 GB – 4 TB	1 TB – 20 TB	16 GB – 1 TB	700 MB – 8.5 GB
Скорост четене	100–400 MB/s	500–2000 MB/s	80–160 MB/s	90–300 MB/s	1.2–22 MB/s
Цена/GB	0.05–0.15 €	0.07–0.12 €	0.02–0.04 €	0.08–0.20 €	0.01–0.03 €
Мобилност	Много висока	Висока	Средна	Много висока	Ниска
Надеждност	Средна (5–10 г.)	Висока (5–10 г.)	Средна-висока (MTBF ~1M ч.)	Средна (5–10 г.)	Висока (20–100 г.)
Типична употреба	Пренос файлове, bootable носители	Видео/снимки, бързо архивиране	Архивиране, NAS, backup	Камери, смартфони, IoT	Архивиране, дистрибуция

№	Риск	Вероятност	Въздействие	Ниво на риска
1	Заразяване със зловреден софтуер чрез USB	Висока	Критично	Много високо
2	Кражба/загуба на некриптиран носител	Висока	Критично	Много високо
3	Рансъмуер атака чрез външен носител	Средна	Критично	Висок
4	Head crash при външен HDD (при транспорт)	Средна	Високо	Висок
5	Корупция на ФС при неправилно изваждане	Висока	Средно	Висок
6	BadUSB атака (модифициран фърмуер)	Ниска	Критично	Среден
7	Износване на NAND клетки (SSD/USB)	Ниска	Средно	Нисък
8	Деградация на оптичен носител (CD/DVD)	Средна	Ниско	Нисък

Характеристика	BitLocker To Go	VeraCrypt	LUKS (dm-crypt)
ОС поддръжка	Windows (Pro/Ent.)	Windows, Linux, macOS	Linux
Алгоритми	AES-128/256 (XTS)	AES, Serpent, Twofish, каскадни	AES, Serpent, Twofish (XTS)
Скрити томове	Не	Да	Не (нативно)
Централно управление	Да (AD/GPO)	Не	Не (без допълн. инструменти)
Лиценз	Комерсиален	Безплатен (FOSS)	Безплатен (FOSS)
TPM интеграция	Да	Не	Не

№	Добра практика	NIST CSF функция
1	Поддържане на инвентарен регистър на всички преносими устройства с уникални идентификатори	Identify (ID)
2	Класификация на данните по ниво на чувствителност преди съхранение на преносим носител	Identify (ID)
3	Криптиране на всички преносими устройства чрез AES-256 (BitLocker, VeraCrypt, LUKS)	Protect (PR)
4	Прилагане на Device Whitelisting – разрешаване само на одобрени устройства (по VID/PID/сериен №)	Protect (PR)
5	Деактивиране на AutoRun/AutoPlay за всички сменяеми устройства в цялата организация	Protect (PR)
6	Автоматично антивирусно сканиране при включване на преносим носител	Detect (DE)
7	Мониторинг на USB събития чрез SIEM с настроени правила за аномална активност	Detect (DE)
8	Документирана процедура за реакция при инцидент с преносимо устройство	Respond (RS)
9	Прилагане на стратегия 3-2-1 за резервни копия с включване на поне един външен носител	Recover (RC)
10	Сигурно изтриване на данни (Clear/Purge/Destroy) преди излизане от употреба, съгласно NIST SP 800-88	Recover (RC)

Решение	Платформа	Централно управление	Цена	Ниво на защита
BitLocker To Go	Windows Pro/Enterprise	Да (AD/GPO)	Включена в ОС	Висока
VeraCrypt	Win/Linux/macOS	Не	Безплатна (FOSS)	Много висока
LUKS (dm-crypt)	Linux	Не	Безплатна (FOSS)	Висока
GPO/MDM контрол	Windows/Azure	Да	Включена/лиценз	Висока
USB Whitelisting	Windows/Linux	Да	Варира	Средна до висока

Операция	USB-Allowed (GRP_USB_Allowed)	USB-Blocked (GRP_USB_Blocked)
Четене от USB устройство	Разрешено	Разрешено
Запис върху USB устройство	Разрешено (само при активиран BitLocker)	Забранено (Deny write access)
Криптиране с BitLocker To Go	Задължително за запис	Не е приложимо
Одит (Event Log)	Да – Event ID 4663 (успешен достъп)	Да – Event ID 4663 (отказан достъп)

Настройка	Стойност
Removable Disks: Deny write access	Enabled
Removable Disks: Deny read access	Not Configured
All Removable Storage classes: Deny all access	Not Configured
CD and DVD: Deny write access	Enabled
Tape Drives: Deny write access	Enabled

Настройка	Стойност
Prevent installation of devices not described by other policy settings	Enabled
Allow installation of devices that match any of these Device Instance IDs	Enabled (списък с одобрени ID)
Prevent installation of devices using drivers that match these device setup classes	Enabled {36FC9E60-C465-11CF-8056-444553540000} (USB Mass Storage)

Настройка	Стойност
Deny write access to removable drives not protected by BitLocker	Enabled
Control use of BitLocker on removable drives	Enabled
→ Allow users to apply BitLocker protection: Checked	
→ Allow users to suspend and decrypt: Unchecked	
Choose how BitLocker-protected removable drives can be recovered	Enabled
→ Allow data recovery agent: Checked	
→ Save BitLocker recovery information to AD DS: Checked	

Настройка	Стойност
Audit Removable Storage	Success, Failure
Audit PNP Activity	Success

№	VID	PID	Сериен номер	Производител	Модел	Потребител	Отдел	Дата на регистрация	Статус
1	781	5591	4C53000121	SanDisk	Ultra Flair 64GB	Иванов, П.	ИТ	15.01.2025	Активен
2	951	1666	E0D55EA573	Kingston	DT100 G3 32GB	Петрова, М.	Счетов.	22.02.2025	Активен
3	8564	1000	AA00000489	Transcend	JetFlash 128GB	Георгиев, Д.	Маркет.	10.03.2025	Деактив.
4	–	–	–	–	–	–	–	–	–

№	Стъпка	Изпълнено
1.1	Идентифициране на устройството (VID/PID/сериен номер)	[ ]
1.2	Резервно копие на необходимите данни (ако има такива)	[ ]
1.3	Презаписване с нули/единици/произволни стойности (минимум 1 пас)	[ ]
1.4	Верификация чрез четене на случайни блокове	[ ]
1.5	Документиране: устройство, метод, дата, отговорник	[ ]

№	Стъпка	Изпълнено
2.1	Идентифициране на устройството и тип (HDD/SSD/NVMe)	[ ]
2.2	Резервно копие на необходимите данни (ако има такива)	[ ]
2.3	Изпълнение на Secure Erase / Cryptographic Erase:	[ ]
2.4	Верификация: четене на целия носител, потвърждаване на липса на възстановими данни	[ ]
2.5	Документиране: сертификат за изтриване с подпис	[ ]

№	Стъпка	Изпълнено
3.1	Идентифициране на устройството (VID/PID/сериен номер)	[ ]
3.2	Избор на метод за физическо унищожаване:	[ ]
3.3	Извършване на унищожаването от оторизиран персонал	[ ]
3.4	Визуална верификация: устройството е физически неразпознаваемо и неработоспособно	[ ]
3.5	Документиране: протокол за унищожаване с подпис на двама свидетели, снимков материал	[ ]
3.6	Актуализиране на инвентарния регистър (Приложение В) – статус „Унищожен"	[ ]

Критерий	Clear	Purge	Destroy
Клас на данните	Нисък–среден	Висок	Най-висок
Носителят остава	В организацията	Напуска контрола	Не – унищожен
Време	Минути–часове	Минути–часове	Минути
Цена	Ниска	Ниска–средна	Средна–висока
Гаранция	Средна	Висока	Абсолютна
Стандарт	NIST SP 800-88 (Clear)	NIST SP 800-88 (Purge)	NIST SP 800-88 (Destroy)