Национална финансово-стопанска гимназия

ДИПЛОМЕН ПРОЕКТ

НА ТЕМА:

Управление на външни запаметяващи устройства - видове, рискове и защита

ИЗГОТВИЛ: Георги Емилов Исаев

От 12 **„з**“ клас

ПРОФЕСИЯ: „Икономист-информатик“

СПЕЦИАЛНОСТ: „Икономическа информатика“

СОФИЯ, 2025 година

СЪДЪРЖАНИЕ

1. УВОД

1.1. Въведение

Данните са сред най-ценните активи на всяка организация, а тяхната наличност, цялост и поверителност определят стабилността на бизнес процесите (Whitman & Mattord, 2018). Мобилността на съвременната работна среда и необходимостта от бърз обмен на големи обеми информация поставят външните запаметяващи устройства – USB флаш памети, външни SSD и HDD, карти с памет – в центъра на технологичната инфраструктура. Въпреки широкото разпространение на облачните услуги, физическите носители остават предпочитани при работа с обемни файлове без зависимост от интернет връзка, както и при обработка на класифицирана информация в изолирани мрежи (ENISA, 2023).

Значението на проекта произтича от двойствената роля на преносимите памети. От една страна, те улесняват ежедневната работа и обмена на данни. От друга – при липса на достатъчен контрол – създават реален риск за информационната сигурност. Според доклада на Verizon за 2023 г. значителна част от инцидентите с изтичане на данни (Data Leakage) се дължат на загубени, откраднати или неконтролирано използвани лични устройства в корпоративна среда – явление, познато като BYOD (Bring Your Own Device) (Verizon, 2023).

Рисковете обаче не се свеждат само до неоторизиран достъп. Външните носители нерядко служат за пренос на зловреден софтуер (malware), заобикаляйки мрежовите защити и защитните стени. Те са основно средство при атаки срещу т.нар. air-gapped системи – компютри, физически изолирани от интернет – което ги превръща в заплаха и за обекти от критичната инфраструктура (Langner, 2011). Управлението на тези устройства изисква не само физическа охрана, а комплексен подход, обхващащ криптиране на данните, стриктни политики за контрол на портовете и обучение на персонала (ISO/IEC 27002:2022).

1.2. Исторически преглед

Еволюцията на външните носители на информация е белязана от непрекъсната миниатюризация и нарастваща плътност на записа. Всеки нов етап разширява възможностите за пренос на данни, но същевременно поражда нови предизвикателства пред сигурността.

Началото е поставено в периода 1951–1952 г. с въвеждането на магнитните ленти – устройства като UNISERVO I и IBM 726, осигуряващи последователен достъп до данни чрез магнитен запис. Защитата по онова време е изцяло физическа: лентите се съхраняват в

охранявани зали, а рискът от кражба е минимален заради обема на самото оборудване (Mueller, 2015).

През 1971 г. IBM представя 8-инчовата дискета, първоначално предназначена за зареждане на микрокод, което поставя началото на по-голямата преносимост на данните. В периода 1976–1984 г. се появяват 5,25-инчовите, а след тях и 3,5-инчовите дискети, превърнали се в индустриален стандарт. Широкият обмен на дискети обаче поражда нов тип заплаха – първите компютърни вируси, разпространявани чрез boot-сектора. Типичен пример е вирусът Brain от 1986 г., който е сред първите образци на зловреден софтуер, пренасян физически (Tanenbaum & Bos, 2015).

Съществена промяна настъпва през 1996 г. с публикуването на спецификацията USB 1.0, въвеждаща универсален сериен интерфейс, който обединява захранването и преноса на данни в един кабел и позволява свързване на устройства без рестартиране на компютъра (hot-swap) (USB Implementers Forum, 2019). През 2000 г. на пазара излизат първите търговски USB флаш памети (DiskOnKey/ThumbDrive) с капацитет 8 MB. Липсата на движещи се части и автоматичното разпознаване от операционната система (Plug-and-Play) ги правят удобни за ежедневна употреба, но и превръщат всяко работно място в потенциална входна точка, заобикаляща мрежовите филтри (Brewer & Gill, 2008).

През 2010 г. е открит червеят Stuxnet, насочен срещу иранската ядрена програма. Той се превръща в емблематичен случай на използване на USB устройство като средство за кибератака срещу промишлени контролери в изолирана среда (Langner, 2011; Zetter, 2014). На конференцията Black Hat през 2014 г. е демонстрирана уязвимостта BadUSB, разкриваща, че заплахата може да произтича не от съдържанието на устройството, а от самия фърмуер на USB контролера, способен да емулира клавиатура и да изпълнява команди за части от секундата (Tischer et al., 2016).

След 2015 г. масовото навлизане на външни SSD с NVMe протокол и USB Type-C разширява скоростите на трансфер над 1000 MB/s (NVM Express, 2022). Тези скорости позволяват стартиране на цели операционни системи директно от външен носител (Live OS), което може да послужи за заобикаляне на локалните защити и достъп до файловата система на хост машината.

1.3. Цел и задачи

Основната цел на проекта е да извърши задълбочен анализ на технологичните и експлоатационните уязвимости при използване на външни запаметяващи устройства в корпоративна среда и на тази основа да предложи модел за управление, който осигурява баланс между оперативна съвместимост и информационна сигурност. За постигането на тази цел са определени следните задачи:

1. Класификация и технологичен анализ – разглеждане на съвременните интерфейси (USB 3.x, USB4, Thunderbolt) и свързаните с архитектурата им рискове (DMA – Direct Memory

Access), както и анализ на файловите системи (FAT32, NTFS, exFAT, APFS) с оглед на възможностите им за управление на правата за достъп (ACL) и водене на журнални записи.

2. Идентификация и категоризация на рисковете – систематизиране на заплахите, включващи физическа загуба и кражба, социално инженерство (атаки тип Baiting с подхвърлени устройства), хардуерни атаки (Rubber Ducky, BadUSB), Juice Jacking (атаки през портове за зареждане), както и оценка на риска от човешка грешка и небрежност.

3. Анализ на методите за защита – сравнение между софтуерни (BitLocker, VeraCrypt) и хардуерни (вградени в чипа) методи за криптиране (AES-256 XTS), проучване на системите за предотвратяване на загуба на данни (DLP) и тяхната ефективност при мониторинг на крайни точки, както и разглеждане на административни подходи като Whitelisting на устройства по Vendor ID/Product ID и блокиране на портове чрез Group Policy (GPO).

4. Практическа реализация – демонстриране на защитен профил в среда на Windows Server/Active Directory, който забранява записа върху външни устройства за неоторизирани потребители и налага задължително криптиране за оторизираните.

2. ТЕОРЕТИЧНА ЧАСТ

2.1.1. Видове външни запаметяващи устройства

Външните запаметяващи устройства са хардуерни средства за съхранение, пренос и архивиране на цифрова информация извън вътрешната памет на компютърната система. Те осигуряват мобилност на данните, възможност за резервно копиране и разширяване на наличния капацитет (Whitman & Mattord, 2018). Според технологията на запис, конструкцията и предназначението си външните носители се разделят на няколко основни групи: USB флаш памети, твърдотелни дискове (SSD), магнитни твърди дискове (HDD), карти с памет (SD) и оптични носители (CD/DVD). Всяка от тях притежава характеристики, които я правят подходяща за различни сценарии на употреба.

1. USB Flash drives – характеристики и приложение

USB флаш паметите са компактни преносими устройства за съхранение, базирани на NAND флаш технология. Те са сред най-масово използваните външни носители поради малките си размери, достъпната цена и лесната употреба (Brewer & Gill, 2008). В основата на всяко такова устройство стои чип с NAND флаш памет, в който информацията се записва чрез електрически заряди в полупроводникови клетки (floating-gate транзистори). За разлика от магнитните носители, NAND технологията не разчита на движещи се механични части, което я прави по-устойчива на удари и вибрации (Micheloni et al., 2010).

Всяка USB флаш памет разполага с вграден контролер, който управлява комуникацията между паметта и хост системата. Контролерът отговаря за корекцията на грешки (ECC – Error Correction Code), за износоустойчивото разпределение на записите (wear leveling) и за управлението на блоковете с лоши сектори (bad block management). Тези механизми са

определящи за надеждността на устройството, тъй като NAND клетките издържат ограничен брой цикли на запис и изтриване – обикновено между 3 000 и 100 000 в зависимост от типа памет: SLC, MLC, TLC или QLC (Bez et al., 2003).

Свързването с компютърната система се осъществява чрез интерфейса USB (Universal Serial Bus), разработен от USB Implementers Forum (USB-IF). Спецификацията е преминала през няколко ревизии: USB 2.0 осигурява теоретична скорост до 480 Mbit/s, USB 3.0 – до 5 Gbit/s, USB 3.1 Gen 2 – до 10 Gbit/s, а USB 3.2 Gen 2×2 достига 20 Gbit/s (USB Implementers Forum, 2019). Наред със скоростта е еволюирал и физическият конектор – от класическия USB Type-A до USB Type-C, който поддържа двупосочно включване и по-високи скорости на трансфер.

Типичните приложения на USB флаш паметите включват пренос на файлове между компютри, създаване на стартиращи (bootable) носители за инсталация на операционни системи, съхранение на документи и мултимедийно съдържание. В корпоративна среда те нерядко служат и за пренос на конфиденциална информация, което поражда сериозни рискове за сигурността и налага прилагането на политики за контрол на устройствата (Whitman & Mattord, 2018). Съвременните модели предлагат капацитет от 4 GB до 2 TB, като най-разпространени на пазара са тези с обем от 16 GB до 256 GB.

2. SSD (Solid State Drive) – технология и особености

Твърдотелните дискове (SSD) също използват NAND флаш памет, но са проектирани за значително по-висока производителност и капацитет в сравнение с USB флаш паметите. Това ги прави предпочитан избор както за вътрешно, така и за външно съхранение в съвременните компютърни системи (Samsung Electronics, 2023).

Архитектурата на SSD включва масив от NAND флаш чипове, контролер и кеш памет (обикновено DRAM). Контролерът координира операциите по четене и запис, управлява алгоритмите за корекция на грешки (ECC) и изпълнява wear leveling, за да разпределя записите равномерно между клетките. Той активира и функцията TRIM, която информира устройството кои блокове данни вече не са необходими и могат да бъдат освободени. Тези процеси поддържат производителността на устройството и удължават жизнения му цикъл (Samsung Electronics, 2023).

Външните SSD се предлагат в няколко форм фактора. Форматът 2.5 инча е наследен от конвенционалните лаптоп HDD и обикновено се свързва чрез SATA III с максимална скорост до 600 MB/s. По-компактният M.2 форм фактор поддържа както SATA, така и протокола NVMe (Non-Volatile Memory Express). NVMe дисковете комуникират с процесора чрез шината PCI Express (PCIe), което осигурява значително по-високи скорости – до 7 000 MB/s при PCIe Gen 4 и над 12 000 MB/s при PCIe Gen 5 (NVM Express, 2022). Външните SSD устройства обикновено се свързват с хост системата чрез USB 3.1/3.2 или Thunderbolt.

Сред основните предимства на SSD технологията са ниското време за достъп (под 0,1 ms спрямо 5–10 ms при HDD), високата скорост на последователно и произволно четене и запис, ниската консумация на енергия, безшумната работа и устойчивостта на механични въздействия. Wear leveling алгоритъмът разпределя записите равномерно между клетките, с което предотвратява преждевременното износване на определени области. Съвременните SSD дискове имат показател TBW (Total Bytes Written) от стотици терабайти, което им осигурява надежден жизнен цикъл от 5 до 10 години при стандартна употреба (Samsung Electronics, 2023).

3. HDD (Hard Disk Drive) – принцип на работа

Твърдият диск с магнитен запис (HDD) е класическо устройство за масово съхранение, което записва данни върху въртящи се дискови пластини (platters), покрити с ферромагнитен материал. Въпреки нарастващата популярност на SSD, HDD дисковете продължават да заемат значителна пазарна ниша поради ниската си цена на гигабайт и наличието на модели с много висок капацитет – до 20 TB за потребителски модели и до 30 TB за корпоративни решения (Backblaze, 2024).

Данните се записват и четат чрез магнитни глави (read/write heads), които се движат над повърхността на пластините. Всяка магнитна ориентация на микроскопична област от повърхността представлява двоична стойност (0 или 1). Пластините се въртят с постоянна скорост, измервана в обороти в минута (RPM). Обичайните стойности са 5 400 RPM за преносими и енергоспестяващи модели и 7 200 RPM за настолни дискове; за сървърни приложения се използват модели с 10 000 и 15 000 RPM (Mueller, 2015).

Един от съществените недостатъци на HDD е фрагментацията на данните. При продължителна употреба файловете се записват в несъседни сектори, което принуждава четящата глава да извършва допълнителни механични движения. Това забавя операциите по четене и влошава общата производителност. Регулярната дефрагментация – подреждането на фрагментите в последователен ред – е препоръчителна практика при файлови системи като NTFS (Tanenbaum & Bos, 2015).

Механичната конструкция определя и уязвимостта на HDD към физически въздействия. Разстоянието между четящата глава и повърхността на пластината е от порядъка на няколко нанометра – дори лек удар може да предизвика контакт между тях (т.нар. head crash) и да доведе до безвъзвратна загуба на данни. Затова външните HDD обикновено включват ударопоглъщащи корпуси и сензори за свободно падане, които паркират главите при засичане на внезапно ускорение (Mueller, 2015). Въпреки тези ограничения, HDD остава предпочитано решение за архивиране на големи обеми данни, видеонаблюдение и мрежово съхранение (NAS), където капацитетът и цената имат приоритет пред скоростта.

4. SD карти – видове и спецификации

Картите с памет SD (Secure Digital) са миниатюрни преносими носители, базирани на NAND флаш технология. Те са широко разпространени в мобилни устройства, цифрови

камери, дронове и вградени системи поради малките си размери и ниската консумация на енергия. Стандартът е въведен през 1999 г. от консорциум, включващ Panasonic, SanDisk и Toshiba, и оттогава е претърпял множество ревизии (SD Association, 2023).

SD картите се произвеждат в три физически размера: стандартен SD (32 × 24 × 2,1 mm), miniSD (21,5 × 20 × 1,4 mm) и microSD (15 × 11 × 1 mm). Форматът miniSD е практически излязъл от употреба, докато microSD доминира при смартфони, таблети и екшън камери. По капацитет спецификациите определят три категории: SDSC (Standard Capacity) – до 2 GB, SDHC (High Capacity) – от 4 до 32 GB и SDXC (Extended Capacity) – от 64 GB до 2 TB (SD Association, 2023).

Класовете на скорост имат значение при приложения, които изискват стабилен поток от данни – например видеозапис и серийна фотография. Оригиналната класификация Speed Class определя минималната последователна скорост на запис: Class 2 (2 MB/s), Class 4 (4 MB/s), Class 6 (6 MB/s) и Class 10 (10 MB/s). С нарастването на изискванията са въведени стандартите UHS (Ultra High Speed) Speed Class – UHS-I с теоретичен максимум 104 MB/s, UHS-II с до 312 MB/s и UHS-III с до 624 MB/s. За видеозапис с висока резолюция е дефиниран и Video Speed Class, където V30 гарантира минимална скорост от 30 MB/s (достатъчна за 4K видео), V60 – 60 MB/s, а V90 – 90 MB/s, подходяща за 8K видео (SD Association, 2023).

В смартфоните SD картите служат за разширяване на вътрешната памет, а в цифровите фотоапарати и видеокамери те са основният носител за запис – професионалните потребители предпочитат карти с клас V30 или по-висок, за да осигурят непрекъснат поток при запис. В областта на Интернет на нещата (IoT) и вградените системи microSD картите съхраняват фърмуер и оперативни данни, което допълнително подчертава универсалността им (Krogh, 2009).

5. CD/DVD носители – оптични технологии

Компактните дискове (CD) и цифровите видеодискове (DVD) са оптични носители, които записват и четат данни чрез лазерен лъч. Макар значението им в ежедневната употреба да е намаляло с навлизането на флаш технологиите и облачните услуги, оптичните дискове все още се използват за архивиране, разпространение на софтуер и мултимедия, както и в специализирани области като медицинските записи и държавния архив, където дълготрайността на данните е приоритет (Pohlmann, 2005).

Технологията на оптичния запис се основава на отражението и пречупването на лазерна светлина от повърхността на диска. При фабрично пресованите (ROM) дискове данните са представени чрез микроскопични вдлъбнатини (pits) и равнинни участъци (lands) върху поликарбонатен субстрат, покрит с отразяващ слой от алуминий. Лазерният лъч отчита разликата в отражението, която се интерпретира като двоичен сигнал. При записваемите (Recordable) дискове се използва слой от органичен багрилен материал (dye layer), който се променя необратимо под въздействието на по-мощен лазер, а при многократно

записваемите (Rewritable) дискове се прилага фазово-променлив (phase-change) материал, способен да преминава между кристално и аморфно състояние до около 1 000 цикъла (Taylor et al., 2006).

Стандартният CD побира до 700 MB данни (около 80 минути аудио) при работа с лазер с дължина на вълната 780 nm. DVD технологията използва лазер с по-къса дължина – 650 nm, което позволява значително по-голяма плътност на запис. Еднослоен едностранен DVD диск (DVD-5) побира 4,7 GB, двуслоен едностранен (DVD-9) – до 8,5 GB, а двуслоен двустранен (DVD-18) – до 17,1 GB. Съществуват два конкуриращи се формата за запис – DVD-R/RW (поддържан от DVD Forum) и DVD+R/RW (поддържан от DVD+RW Alliance), като повечето съвременни оптични устройства поддържат и двата (Taylor et al., 2006).

При правилно съхранение – без пряка слънчева светлина, при стабилна температура и ниска влажност – оптичните носители могат да запазят данните за период от 20 до 100 години (Pohlmann, 2005). Това ги прави подходящи за дългосрочно архивиране. ROM и Recordable вариантите са защитени от запис, което ги предпазва от случайно изтриване и от заразяване със зловреден софтуер, при условие че автоматичното изпълнение на съдържание от тях е деактивирано. Стандартизацията на оптичните носители е уредена чрез международни стандарти като ISO/IEC 10149 за CD-ROM (ISO/IEC 10149, 1995), което гарантира глобалната им съвместимост.

Петте разгледани категории външни запаметяващи устройства покриват широк спектър от потребности за съхранение. Изборът на конкретен тип зависи от необходимия капацитет, изискваната скорост, физическата издръжливост, условията на транспортиране и изискванията за сигурност. Доброто познаване на технологичните особености на всяко устройство е предпоставка за ефективното му управление и за ограничаване на рисковете при експлоатация.

2.1.2. Технически характеристики на външните носители

зборът на външно запаметяващо устройство зависи от няколко групи технически параметри: скорости на четене и запис, интерфейс за свързване, капацитет и надеждност. Тези характеристики определят доколко даден носител е подходящ за определен сценарий – от ежедневен обмен на файлове до архивиране на големи масиви от данни.

1. Скорости на четене и запис

Скоростта на трансфер е един от водещите показатели за всяко устройство за съхранение. В техническата документация се разграничават два типа операции: последователно (sequential) и произволно (random) четене и запис. Последователните операции се измерват в мегабайти в секунда (MB/s) и отразяват скоростта при работа с големи непрекъснати блокове данни, например при копиране на видеофайл или създаване на образ на диска. Произволните операции се измерват в IOPS (Input/Output Operations Per Second) и показват способността на устройството да обработва множество малки заявки от различни места на

носителя едновременно – типично поведение при работата на операционната система и базите данни (Micheloni et al., 2010).

При магнитните HDD последователните скорости достигат 80–160 MB/s за модели със 7 200 RPM, а произволното четене рядко превишава 100–200 IOPS поради механичните закъснения при позициониране на четящата глава (seek time) и ротационното забавяне (rotational latency). SSD устройства с SATA интерфейс достигат практическия предел на интерфейса – около 550 MB/s за последователно четене – при десетки и стотици хиляди IOPS за произволни операции. NVMe SSD от поколение PCIe Gen 4 постигат последователно четене до 7 000 MB/s и произволно четене над 1 000 000 IOPS; при PCIe Gen 5 тези стойности нарастват допълнително (Samsung Electronics, 2023). USB флаш паметите заемат междинна позиция: типичните модели с USB 3.0 осигуряват 100–400 MB/s за последователно четене, но скоростта на запис обикновено е значително по-ниска заради ограниченията на вградения контролер (Brewer & Gill, 2008).

Реалната скорост на трансфер зависи не само от самото устройство, но и от използвания интерфейс. Дори най-бързият SSD ще бъде ограничен до около 35–40 MB/s при свързване чрез USB 2.0, затова изборът на интерфейс е неразделна част от оценката на производителността (USB Implementers Forum, 2019).

2. Интерфейси за свързване

Интерфейсът определя максималната теоретична пропускателна способност между външното устройство и хост системата, а също влияе върху латентността и протокола за комуникация.

USB 2.0 (Hi-Speed), въведен през 2000 г., предлага теоретична скорост до 480 Mbit/s (около 60 MB/s), макар на практика пропускателната способност рядко да надхвърля 30–35 MB/s заради протоколно натоварване (overhead). Въпреки ограниченията си, той остава разпространен благодарение на пълната обратна съвместимост и широката поддръжка от наследени устройства (USB Implementers Forum, 2019).

USB 3.0 (SuperSpeed), стандартизиран през 2008 г., увеличава пропускателната способност десетократно – до 5 Gbit/s (около 625 MB/s теоретично, 300–400 MB/s на практика). Следващата ревизия USB 3.1 Gen 2 (SuperSpeed+) удвоява скоростта до 10 Gbit/s, а USB 3.2 Gen 2×2, въведен през 2017 г., достига 20 Gbit/s чрез два канала (lanes) по 10 Gbit/s. Всички версии запазват обратна съвместимост, като конекторът USB Type-C става задължителен за USB 3.2 Gen 2×2 (USB Implementers Forum, 2019).

SATA III (Serial ATA, ревизия 3.0) е предназначен предимно за вътрешни дискове, но се среща и при външни SSD чрез USB-SATA мост (bridge). Пропускателната му способност е 6 Gbit/s (около 600 MB/s) – достатъчна за SATA-базирани SSD, но ограничаваща за NVMe устройства (Serial ATA International Organization, 2018).

NVMe (Non-Volatile Memory Express) е протокол, проектиран специално за NAND флаш памет, който комуникира директно чрез шината PCI Express. За разлика от AHCI протокола при SATA, NVMe поддържа до 65 535 опашки с по 65 536 команди всяка, което значително намалява латентността и повишава паралелизма. При PCIe Gen 3 ×4 максималната скорост е около 3 500 MB/s, при Gen 4 ×4 – до 7 000 MB/s, а при Gen 5 ×4 – до 14 000 MB/s. Външните NVMe SSD се свързват най-често чрез USB 3.2 Gen 2 или Thunderbolt (NVM Express, 2022).

Thunderbolt, разработен от Intel съвместно с Apple, обединява PCIe и DisplayPort протоколи в един кабел. Thunderbolt 3 и 4 използват конектор USB Type-C и осигуряват 40 Gbit/s, а Thunderbolt 5 достига 80 Gbit/s (120 Gbit/s в режим Bandwidth Boost). Интерфейсът е предназначен за професионални приложения, при които се изисква максимална скорост при работа с външни NVMe масиви (Intel Corporation, 2023).

Таблица 1. Сравнителна характеристика на основните интерфейси за свързване на външни носители

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

Забележка: Реалните скорости са по-ниски от теоретичните поради протоколно натоварване (overhead), кодиране на данните и ограничения на контролера. Източници: USB-IF (2019), NVM Express (2022), Intel Corporation (2023), Serial ATA International Organization (2018).

3. Капацитет и производителност

При оценката на капацитета е необходимо да се отчита разликата между десетичното (GB – гигабайт, 1 GB = 10^9 байта) и двоичното (GiB – гибибайт, 1 GiB = 2^{30} = 1 073 741 824 байта) измерване. Производителите обозначават капацитета в GB по десетичната система, докато повечето операционни системи (и в частност Windows) показват наличното пространство в GiB, без изрично да го указват. Затова потребителите наблюдават по-малък „форматиран" капацитет от рекламирания – диск с етикет „500 GB" показва приблизително 465 GiB.

Стандартът за означаване е дефиниран от IEC 80000-13 (International Electrotechnical Commission, 2008).

При SSD устройствата достъпният капацитет допълнително се намалява от технологията Over-Provisioning (OP). Производителите резервират определен процент от общия капацитет на NAND чиповете (типично 7–28%) за вътрешни нужди на контролера – износоустойчиво разпределение (wear leveling), събиране на отпадъци (garbage collection), корекция на грешки и замяна на дефектни блокове. По-висок процент Over-Provisioning подобрява производителността и дълготрайността, особено при интензивен запис. Корпоративните SSD модели обикновено прилагат по-агресивно OP в сравнение с потребителските (JEDEC, 2016).

Латентността (latency) измерва времето между подаване на заявка за данни и получаване на отговор. При HDD тя се определя от механичните параметри – времето за търсене (seek time, типично 4–12 ms) и ротационното забавяне (средно 4,17 ms при 7 200 RPM). При SATA SSD латентността на четене е около 50–100 µs, а при NVMe SSD пада до 10–20 µs – три порядъка по-ниско спрямо HDD. Именно тази разлика обяснява забележимо по-бързото зареждане на операционни системи и приложения от SSD носители (Micheloni et al., 2010).

4. Надеждност и жизнен цикъл

Надеждността на външните носители се оценява чрез няколко стандартизирани показателя. За HDD основен параметър е MTBF (Mean Time Between Failures) – средното време между повредите, измервано в часове. Потребителските HDD обикновено имат MTBF от порядъка на 1 000 000 часа, а корпоративните модели – до 2 500 000 часа. MTBF обаче е статистически показател, получен чрез ускорени тестове върху голяма извадка, и не означава, че конкретен диск ще работи непрекъснато толкова дълго (Schroeder & Gibson, 2007). Реалните данни от експлоатацията показват, че годишният процент на повреда (AFR) при потребителски HDD варира между 1% и 3%, като нараства чувствително след четвъртата година на експлоатация (Backblaze, 2024).

За SSD надеждността се измерва основно чрез TBW (Total Bytes Written) и DWPD (Drive Writes Per Day). TBW указва общото количество данни (в терабайти), което може да бъде записано преди износване на NAND клетките, а DWPD показва колко пъти на ден цялият капацитет на диска може да бъде презаписан в рамките на гаранционния период. Например SSD с капацитет 1 TB, DWPD от 1 и гаранция от 5 години има TBW = 1 TB × 365 × 5 = 1 825 TB. Потребителските SSD обикновено имат DWPD от 0,3–0,6, докато корпоративните модели достигат 3–10 DWPD (JEDEC, 2016). Издръжливостта зависи и от типа NAND памет: SLC (Single-Level Cell) понася до 100 000 цикъла запис/изтриване, MLC (Multi-Level Cell) – около 10 000, TLC (Triple-Level Cell) – 3 000–5 000, а QLC (Quad-Level Cell) – около 1 000 цикъла (Micheloni et al., 2010).

Състоянието на HDD и SSD се наблюдава чрез технологията S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology). Тя следи набор от параметри – брой на

преразпределените сектори (Reallocated Sectors Count), общо време на работа (Power-On Hours), грешки при четене (Raw Read Error Rate) и температура. При SSD допълнително се проследяват процентът на износване (Wear Leveling Count), оставащият ресурс (Percentage Used) и общото количество записани данни (Total LBAs Written). Навременният анализ на тези показатели позволява да се предвиди евентуална повреда и да се предприемат превантивни мерки – преди всичко създаване на резервно копие – преди загубата на данни да стане необратима (Schroeder & Gibson, 2007).

При оптичните носители (CD/DVD) надеждността зависи основно от условията на съхранение. Фабрично пресованите дискове запазват данните за 20–50 години, докато записваемите (R) и многократно записваемите (RW) имат по-кратък живот – обикновено 5–15 години в зависимост от качеството на багрилния материал и условията на съхранение (температура, влажност, UV излъчване). USB флаш паметите имат типичен retention time (време на запазване на данните без захранване) от 10 до 15 години при стайна температура, макар този срок да намалява с износването на NAND клетките (JEDEC, 2016).

2.1.3. Драйвери и системна интеграция

За да бъде използвано пълноценно, едно външно запаметяващо устройство трябва не само да притежава подходящи хардуерни параметри, но и да бъде коректно разпознато и обслужено от операционната система. На практика този процес обхваща три взаимосвързани области: драйверната съвместимост с конкретната платформа, автоматичното разпознаване и монтиране на устройството (механизмът Plug and Play) и поддръжката на файловата система, с която носителят е форматиран. Windows, Linux и macOS подхождат по различен начин към всяка от тези задачи, а разликите се отразяват пряко върху достъпността и сигурността на данните.

1. Съвместимост с операционни системи

Windows разчита главно на т.нар. inbox драйвери – такива, които идват заедно с дистрибуцията на системата и не изискват отделна инсталация. Когато потребителят свърже стандартно USB устройство за масово съхранение (Mass Storage Class), системата автоматично зарежда универсалния драйвер USBSTOR.SYS, който осигурява четене и запис без допълнителна намеса (Microsoft, 2024a). Ако дадено устройство изисква специализиран драйвер, Windows го търси в локалното хранилище Driver Store или го изтегля чрез Windows Update. Драйверите, сертифицирани по програмата WHQL (Windows Hardware Quality Labs), носят цифров подпис от Microsoft – това потвърждава съвместимостта им и същевременно възпрепятства зареждането на неподписан или потенциално зловреден код на ниво ядро (Microsoft, 2024a).

В Linux поддръжката на хардуера се организира чрез модули на ядрото (kernel modules), които се зареждат динамично при откриване на ново устройство. Когато потребителят свърже USB носител от клас Mass Storage, ядрото зарежда модулите usb-storage и sd_mod и създава съответното блоково устройство (например /dev/sdb) (The Linux Kernel

Documentation, 2024). Координацията на целия процес се поема от подсистемата udev (userspace device manager) – тя прихваща събитията на ядрото (uevent), идентифицира устройството по атрибутите му и прилага правилата, записани в /etc/udev/rules.d/. Чрез тези правила администраторът може да задава права за достъп, да създава символни връзки или да стартира скриптове при включване на конкретно устройство. Възможността правилата да се филтрират по Vendor ID и Product ID превръща udev в ефективен инструмент за контрол на устройствата в корпоративна среда (Kroah-Hartman, 2007).

При macOS управлението на устройствата минава през I/O Kit – обектно-ориентирана рамка, вградена в ядрото XNU. Драйверите са организирани в йерархия от класове, всеки от които обслужва определен тип хардуер. При свързване на външен носител системата съпоставя свойствата му, публикувани в I/O Registry, с наличните драйвери и зарежда най-подходящия (Apple, 2023a). За стандартните USB устройства за масово съхранение macOS използва вградения драйвер IOUSBMassStorageClass, работещ по протокола Bulk-Only Transport. Както и при Windows, драйверите от трети страни подлежат на задължително подписване чрез механизма за нотаризация (Notarization). Допълнителна защита осигуряват Secure Boot и System Integrity Protection (SIP), въведени с версия 10.13 (High Sierra), които ограничават зареждането на неподписан код в ядрото (Apple, 2023a).

2. Процес на разпознаване и монтиране (Plug and Play)

Технологията Plug and Play (PnP) дава възможност на операционната система автоматично да разпознае и конфигурира новосвързано периферно устройство. При включване на USB носител протича т.нар. USB enumeration: хост контролерът регистрира електрическа промяна на порта, нулира устройството, присвоява му уникален адрес на шината и последователно прочита неговите дескриптори – Device Descriptor, Configuration Descriptor, Interface Descriptor и Endpoint Descriptor. От Device Descriptor операционната система извлича Vendor ID (VID), Product ID (PID), класа на устройството, версията на USB протокола и максималната консумирана мощност. Комбинацията VID/PID е тази, която определя кой драйвер да бъде зареден (USB Implementers Forum, 2019).

След успешната енумерация системата монтира файловата система на устройството и я предоставя на потребителя. При Windows процесът е изцяло автоматичен – устройството получава буква на дял (drive letter) и незабавно се появява в Explorer. Допълнително управление е достъпно чрез конзолата Disk Management (diskmgmt.msc), откъдето могат да се променят буквите на дяловете, да се форматира или да се създават нови дялове (Microsoft, 2024b). В Linux монтирането може да бъде както автоматично (чрез udisks2 и графичната среда), така и ръчно – чрез командата mount:

sudo mount /dev/sdb1 /mnt/usb	закачане с автоматично разпознаване на ФС
sudo mount -t ntfs-3g /dev/sdb1 /mnt/usb	изрично указване на NTFS чрез NTFS-3G

sudo mount -t exfat /dev/sdb1 /mnt/usb	закачане на exFAT дял
sudo umount /mnt/usb	откачане преди физическо изваждане

Важна стъпка, която нерядко се подценява, е безопасното премахване на устройството (safe eject). Тя гарантира, че всички чакащи операции по запис ще бъдат завършени (flush на буферите), преди носителят да бъде физически изваден. При файлови системи без журналинг пропускането на тази процедура лесно може да предизвика корупция на данните (Tanenbaum & Bos, 2015).

3. Файлови системи

Файловата система, с която е форматиран даден външен носител, предопределя както съвместимостта му с различни операционни системи, така и възможностите за защита, журналиране и контрол на достъпа до записаните данни.

FAT32 (File Allocation Table, 32-bit) остава една от най-универсално поддържаните файлови системи – тя работи на практически всяка съвременна операционна система, вградено устройство или мултимедиен плейър. Това обаче идва с известни компромиси: максималният размер на единичен файл е ограничен до 4 GB, а на дял – до 2 TB при 512-байтови сектори (Microsoft, 2024c). Липсата на журналинг, списъци за контрол на достъпа (ACL) и криптиране на ниво файлова система означава, че всеки с физически достъп до носителя може безпрепятствено да чете и променя файловете. Въпреки тези слабости FAT32 си остава предпочитан формат за USB флаш памети и SD карти именно заради широката съвместимост.

NTFS (New Technology File System) е основната файлова система в Windows, създадена с акцент върху надеждността и контрола на достъпа. Промените в метаданните се записват в журнал (log), преди да бъдат приложени фактически – при неочаквано прекъсване на захранването системата може автоматично да възстанови консистентността си (Microsoft, 2024c). Освен журналинга NTFS предлага пълноценни списъци за контрол на достъпа (ACL), криптиране на ниво файл и директория чрез EFS (Encrypting File System), компресия на данни и квоти за дисково пространство. Когато NTFS форматиран носител се използва в среда на Linux, достъпът обикновено минава през драйвера NTFS-3G, реализиран в потребителското пространство чрез FUSE – той осигурява пълноценно четене и запис, макар и с по-ниска производителност спрямо нативната работа в Windows. В ядрото на Linux, считано от версия 5.15 насам, е включен и новият NTFS3 драйвер с нативна поддръжка (Paragon Software, 2021).

exFAT (Extended File Allocation Table) е разработена от Microsoft като по-съвременна алтернатива на FAT32, насочена специално към флаш памети и преносими носители. С нея отпада ограничението от 4 GB за единичен файл, а максималният размер на дял достига 128

PB. Вместо FAT верига за проследяване на свободното пространство exFAT използва bitmap, което намалява излишните операции по запис и е по-подходящо за флаш носители (Microsoft, 2024c). През 2019 г. Microsoft публикува спецификацията като отворена, а скоро след това тя беше включена нативно в ядрото на Linux (от версия 5.4). Слабата страна на exFAT е, че подобно на FAT32 не разполага с журналинг и ACL – при внезапно прекъсване на захранването рискът от корупция на данните е реален, а контролът на достъпа остава изцяло отговорност на операционната система.

ext4 (Fourth Extended Filesystem) е файловата система по подразбиране в повечето дистрибуции на Linux. Нейният журналинг може да работи в три режима: journal (пълно журналиране на данни и метаданни), ordered (журналиране само на метаданни, като данните се записват преди тях) и writeback (журналиране само на метаданни без гаранция за реда на записване). Контролът на достъпа следва POSIX модела (owner/group/others с разрешения read/write/execute), като допълнително се поддържат разширени атрибути (xattr) и ACL (Ts'o, 2010). Максималният размер на файл достига 16 TB, а на цялата файлова система – 1 EB при 4 KB блокове. За външен носител ext4 е разумен избор, когато устройството ще работи основно с Linux, тъй като нативна поддръжка в Windows и macOS не съществува без допълнителен софтуер.

APFS (Apple File System) е съвременната файлова система на Apple, въведена с macOS High Sierra (10.13) през 2017 г. Проектирана с мисъл за флаш и SSD носители, тя предлага вградено криптиране (AES-128 или AES-256 в режим XTS), моментални снимки (snapshots), клониране на файлове по принципа copy-on-write и споделяне на пространство между множество томове (space sharing). Целостта на данните се осигурява чрез журналиране на метаданните и контролни суми (Apple, 2023b). Извън екосистемата на Apple обаче поддръжката е ограничена – в Windows и Linux достъпът до APFS дялове е възможен единствено чрез софтуер на трети страни и по правило остава в режим само за четене.

Изборът на файлова система за външен носител винаги е компромис. Когато е необходима максимална преносимост между платформи, exFAT е най-удобният вариант, макар и без журналинг и контрол на достъпа. В среди, в които сигурността е водеща, NTFS и ext4 осигуряват както журналиране, така и ACL, а в рамките на екосистемата на Apple APFS допълва тези механизми с вградено криптиране и защита на целостта на данните.

2.1.4. Сравнителен анализ

Изборът на подходящо външно запаметяващо устройство предполага систематична съпоставка на наличните технологии по няколко основни критерия: капацитет, скорост на трансфер, цена за гигабайт, мобилност, надеждност и типично приложение. Петте категории външни носители – USB флаш памети, външни SSD, външни HDD, SD карти и CD/DVD – се различават съществено по тези параметри и всяка от тях има характерни

силни и слаби страни. Данните по-долу се базират на пазарни проучвания, технически бенчмаркове и потребителски изследвания от периода 2022–2025 г.

Таблица 2. Сравнителна характеристика на основните типове външни запаметяващи устройства

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

Забележка: Стойностите за цена/GB отразяват средни пазарни цени за Европа към второто тримесечие на 2024 г. и са ориентировъчни. Скоростите се отнасят до последователно четене при типичен интерфейс. Надеждността е обобщена оценка, базирана на TBW, MTBF и retention time. Източници: Statista (2024), Tom's Hardware (2024), Samsung Electronics (2023), Backblaze (2024), SD Association (2023).

1. Предимства и недостатъци на различните видове

a. USB Flash Drive

USB флаш паметите съчетават висока портативност с достатъчен капацитет – устройство с тегло от няколко грама побира до 1 TB данни и се побира в джоб или ключодържател. Те работят с практически всички операционни системи и устройства, поддържащи USB порт, което ги прави удобно средство за бърз обмен на файлове. При USB 3.1 или 3.2 интерфейс съвременните модели достигат скорости на последователно четене от 300–400 MB/s – достатъчно за повечето потребителски сценарии (Tom's Hardware, 2024).

Ограниченията им обаче не бива да се подценяват. Скоростта на запис обикновено е 2 до 5 пъти по-ниска от четенето поради по-опростения контролер в сравнение с пълноценните SSD. Издръжливостта на NAND клетките (най-често TLC или QLC) намалява при интензивен запис, а малкият физически размер увеличава риска от загуба или кражба – проблем с реални последици за сигурността в корпоративна среда. Според проучване на Ponemon Institute (2016) около 22 % от анкетираните са загубили USB устройство, съдържащо чувствителна информация.

б. Външен SSD

Външните SSD устройства предлагат най-добрия баланс между скорост и мобилност. С NVMe протокол и USB 3.2 Gen 2 или Thunderbolt интерфейс те достигат 1 000 до 2 000 MB/s последователно четене, т.е. до 10 пъти повече от външните HDD (Tom's Hardware, 2024). Липсата на движещи се части ги прави устойчиви на удари и вибрации – повечето модели издържат свободно падане от височина до 2 метра (Samsung Electronics, 2023). Тихата работа и ниската консумация на енергия са допълнително предимство, особено при работа с лаптоп на батерия.

Основният недостатък остава цената – макар и намаляваща, тя е 2 до 3 пъти по-висока от тази на HDD при еднакъв капацитет (Statista, 2024). Максималният достъпен обем при потребителските модели обикновено не надхвърля 4 TB, докато HDD дисковете предлагат до 20 TB. При продължителен интензивен запис някои модели понижават скоростта поради изчерпване на SLC кеша (thermal throttling и cache exhaustion), което е съществено при професионална работа с големи обеми данни.

в. Външен HDD

Твърдите дискове с магнитен запис водят по съотношение капацитет–цена. При едва 0,02–0,04 €/GB външен HDD от 4 до 8 TB осигурява икономично съхранение на големи архиви – лични колекции, медийни библиотеки, пълни резервни копия на системи. Данните от проучването на Backblaze върху над 250 000 диска показват годишна честота на повреди (AFR – Annualized Failure Rate) от около 1,7 % за 2023 г., което потвърждава приемливата надеждност на съвременните модели при стационарна употреба (Backblaze, 2024).

Ограниченията произтичат от механичната конструкция. Последователните скорости от 80–160 MB/s и особено ниската производителност при произволен достъп (~100 IOPS) правят HDD неподходящ за задачи с нужда от бърз отклик – редактиране на видео, виртуализация или стартиране на приложения от външния диск. Физическата уязвимост към удари и вибрации остава риск при транспортиране, а по-голямото тегло и размери в сравнение със SSD намаляват мобилността.

г. SD карта

SD картите са незаменими в екосистемата на мобилните и вградени устройства. Техният миниатюрен форм фактор (microSD с размери едва 15 × 11 × 1 mm) позволява интеграция в смартфони, екшън камери, дронове и IoT сензори. Спецификациите UHS-II осигуряват скорости до 312 MB/s, достатъчни за запис на 4K видео, а класът V90 гарантира непрекъснат поток от данни за 8K съдържание. Ниската консумация на енергия ги прави идеални за батерийно захранвани устройства.

Недостатъците на SD картите включват по-висока цена за гигабайт в сравнение с HDD и USB флаш паметите, особено при моделите с висок клас на скорост. Миниатюрните размери, макар и предимство от гледна точка на мобилността, увеличават риска от

физическа загуба. Издръжливостта при продължителен интензивен запис е по-ниска от тази на пълноценните SSD устройства поради по-опростения контролер и липсата на DRAM кеш в повечето модели. Освен това не всички съвременни лаптопи и настолни компютри разполагат с вграден SD четец, което налага използването на външен адаптер.

д. CD/DVD носители

Оптичните носители притежават уникално предимство в контекста на дълготрайното архивиране – при правилно съхранение фабрично пресованите дискове могат да запазят данните за 50 до 100 години. Write-once характеристиката на CD-R и DVD-R дисковете гарантира, че веднъж записаните данни не могат да бъдат променени или заразени със зловреден софтуер, което ги прави особено ценни за институционални архиви и медицински записи. Цената на единичен диск е пренебрежимо ниска, а стандартизацията по ISO/IEC осигурява глобална съвместимост.

От друга страна, оптичните носители страдат от сериозни ограничения по капацитет (до 8.5 GB за двуслоен DVD) и изключително ниски скорости на запис и четене в сравнение с всички останали категории. Физическата чупливост и чувствителността към надраскване, прах и UV излъчване правят съхранението им деликатно. Тенденцията към премахване на оптичните устройства от съвременните лаптопи и ултрабуци допълнително ограничава практическата им приложимост. Проучване на Statista (2024) показва, че пазарът на записващи оптични устройства е намалял с над 80% спрямо пика си от 2010 г.

2. Сценарии на употреба според нуждите

Изборът на външен носител не е универсален – той зависи от конкретния сценарий, в който устройството ще бъде използвано.

За масово архивиране и дългосрочно съхранение най-подходящ е външният HDD. Неговият висок капацитет (до 20 TB) и ниската цена за гигабайт го правят оптимален за създаване на пълни резервни копия (full backups) на системи и мултимедийни колекции. В комбинация с NAS (Network Attached Storage) устройство, HDD дисковете осигуряват мрежов достъп и RAID защита за допълнителна надеждност.

За работа с големи файлове и нужда от висока скорост външният SSD е безалтернативен. Професионалистите в областта на видеопродукцията, графичния дизайн и софтуерната разработка се възползват от скоростите, надхвърлящи 1 000 MB/s, за редактиране на 4K/8K видео директно от външния носител, за виртуални машини и за бързо разгръщане на работна среда при пътуване. Проучвания на Tom's Hardware (2024) потвърждават, че външните NVMe SSD устройства постигат до 90% от производителността на вътрешен SSD при свързване чрез Thunderbolt.

За ежедневен пренос на файлове и бърза размяна на данни USB флаш паметите остават най-практичното решение. Техният компактен размер, ниска цена и универсална съвместимост ги правят предпочитан избор за пренос на документи, презентации и софтуерни

инсталатори между компютри. За корпоративна употреба се препоръчват модели с хардуерно криптиране (AES-256), които предпазват данните при загуба или кражба на устройството.

За мобилни устройства, фотография и видеозапис SD картите са стандартният носител. Фотографите и видеооператорите разчитат на високоскоростни карти с клас V30 или V60 за непрекъснат запис на висококачествено съдържание, а потребителите на смартфони ги използват за разширяване на вътрешната памет. Във вградените системи и IoT устройствата microSD картите служат като основен носител за фърмуер и оперативни данни.

За дистрибуция на софтуер, институционално архивиране и write-once съхранение CD/DVD носителите запазват своята ниша. Държавните институции и медицинските заведения продължават да ги използват за архивиране на документация с правно значение, където неизменяемостта на записа е нормативно изискване. В образователната среда оптичните носители се прилагат за разпространение на учебни материали и софтуерни лицензи в региони с ограничен интернет достъп.

Всеки тип външен носител заема определена ниша, определена от баланса между техническите му характеристики и изискванията на потребителя. Не съществува единствен „най-добър" носител – оптималният избор е функция на конкретните нужди по отношение на капацитет, скорост, мобилност, цена и сигурност. Познаването на предимствата и ограниченията на всяка технология позволява информирано решение, което минимизира рисковете и максимизира ефективността на управлението на данни.

3. ПРАКТИЧЕСКА ЧАСТ

Теоретичната рамка, изградена в раздел 2.1, очертава технологичните основи на външните запаметяващи устройства – видове, характеристики, интерфейси и файлови системи. Практическата част пренася фокуса към реалните заплахи, свързани с използването на тези устройства, и към конкретните технически и организационни мерки за тяхното управление. Анализът следва логиката на рамката за управление на риска (Risk Management Framework) съгласно NIST SP 800-37 (NIST, 2018) и принципите на системата за управление на информационната сигурност (ISMS) по ISO/IEC 27001 (ISO/IEC, 2022).

3.1. Анализ на рисковете при управление на външни носители

Управлението на рисковете, свързани с външните запаметяващи устройства, изисква систематично идентифициране, оценка и третиране на заплахите, които могат да компрометират поверителността, целостта и наличността на данните. Стандартът ISO/IEC 27005 (ISO/IEC, 2022b) дефинира риска като комбинация от вероятност за настъпване на нежелано събитие и тежест на последиците от него. В контекста на външните носители

рисковете се групират в пет основни категории: физически повреди и механични дефекти, заплахи от зловреден софтуер, загуба на данни, неоторизиран достъп и човешки фактор.

1. Физически повреди и механични дефекти

Външните носители са изложени на широк спектър от физически въздействия, които могат да доведат до частична или пълна загуба на данни. При HDD устройствата основният рисков фактор е контактът между четящата глава и магнитната пластина (head crash), който може да бъде предизвикан от удар, вибрация или внезапно прекъсване на захранването. Флаш-базираните устройства (USB, SSD, SD карти) са по-устойчиви на механични въздействия, но остават уязвими към екстремни температури, статично електричество (ESD – Electrostatic Discharge) и влага. Оптичните носители (CD/DVD) са чувствителни към надраскване, UV излъчване и деформация при високи температури (Mueller, 2015). Вероятността от физическа повреда е средна до висока при мобилна употреба и ниска при стационарно съхранение, а въздействието варира от частична деградация на данните до пълна неработоспособност на устройството.

2. Заплахи от зловреден софтуер (Malware, Ransomware)

Външните носители са един от класическите вектори за разпространение на зловреден софтуер. Механизмът на заразяване включва няколко подхода: автоматично изпълнение на зловреден код чрез функцията AutoRun/AutoPlay (особено разпространено при по-стари версии на Windows), маскиране на изпълними файлове като документи чрез промяна на иконите и разширенията, експлоатиране на уязвимости в USB стека на операционната система (т.нар. BadUSB атаки, при които фърмуерът на USB контролера е модифициран), както и заразяване чрез скрити дялове или boot сектори. Рансъмуерът представлява особено опасна разновидност, тъй като криптира файловете на устройството и изисква откуп за декриптиращия ключ. Според доклада на ENISA Threat Landscape 2023, USB устройствата остават сред петте най-използвани начални вектори за атаки в корпоративна среда, като 37% от целевите атаки срещу индустриални системи използват USB носители като входна точка (ENISA, 2023). Вероятността е висока, а въздействието – критично, особено при инфраструктури от типа на SCADA/ICS.

3. Риск от загуба на данни

Загубата на данни може да настъпи вследствие на хардуерна повреда, софтуерна грешка, корупция на файловата система или случайно изтриване от потребителя. При файлови системи без журналинг (FAT32, exFAT) рискът от корупция при внезапно прекъсване на записа е значително по-висок в сравнение с журналиращите системи (NTFS, ext4). Липсата на актуални резервни копия (backups) трансформира техническия инцидент в бизнес катастрофа. Според проучване на Kroll Ontrack, 67% от случаите на загуба на данни при външни носители се дължат на хардуерна повреда, 14% – на софтуерни грешки, а 10% – на случайно потребителско действие (Kroll Ontrack, 2022). Вероятността от загуба на данни

при липса на backup стратегия е висока, а въздействието зависи от критичността на информацията – от незначително до катастрофално за организацията.

4. Неоторизиран достъп и кражба на информация

Компактният размер на повечето външни носители (особено USB флаш памети и microSD карти) ги прави лесни за кражба или загуба, което създава директен риск от неоторизиран достъп до съхраняваните данни. При липса на криптиране всеки, който получи физически достъп до устройството, може да прочете цялото му съдържание без каквито и да било ограничения – файловите системи FAT32 и exFAT не предлагат механизми за контрол на достъпа. Дори при NTFS, която поддържа ACL, достъпът може да бъде заобиколен чрез зареждане на алтернативна операционна система от bootable USB. Проучването на Ponemon Institute (2016) установява, че 50% от служителите в корпоративна среда използват некриптирани USB устройства за пренос на служебна информация, а средната цена на инцидент с изтичане на данни от загубен или откраднат носител възлиза на 3.86 милиона щатски долара. Вероятността е висока, а въздействието – критично, особено когато носителят съдържа лични данни, защитени от GDPR, или класифицирана информация.

5. Човешки фактор и грешки при работа

Човешкият фактор е основен катализатор за повечето инциденти, свързани с външните носители. Типичните грешки включват: изваждане на устройството без безопасно демонтиране (safe eject), което води до корупция на файловата система; свързване на непознати USB устройства към корпоративни системи; използване на един и същ носител за лична и служебна информация; пренебрегване на политиките за криптиране и антивирусно сканиране; и липса на маркировка и инвентаризация на устройствата. Социалното инженерство (social engineering) експлоатира човешкото любопитство – целенасочено оставени USB устройства на публични места (т.нар. USB drop attack) се свързват от 45–98% от намерилите ги лица, според експерименти на университета в Илинойс (Tischer et al., 2016). Вероятността от човешка грешка е висока, а въздействието варира в зависимост от конкретния сценарий.

6. Матрица за оценка на риска

Систематичната оценка на рисковете изисква съпоставяне на вероятността за настъпване на всеки риск с тежестта на потенциалните последици. Следната матрица класифицира осемте основни риска, свързани с външните носители, по скала с четири нива: ниска, средна, висока и критична. Методологията следва препоръките на NIST SP 800-30 (NIST, 2012) и ISO/IEC 27005 (ISO/IEC, 2022b).

Таблица 3. Матрица за оценка на риска при управление на външни носители

№	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

Забележка: Нивото на риска се определя като комбинация от вероятност и въздействие съгласно методологията на NIST SP 800-30 (NIST, 2012).

Ефективното управление на тези рискове изисква прилагане на подход, обхващащ три фази: детекция (откриване на заплахата преди или по време на нейното реализиране), реакция (ограничаване на щетите и неутрализиране на заплахата) и възстановяване (връщане на системите и данните в нормално работно състояние). Детекцията включва антивирусно сканиране при включване на устройство, мониторинг на USB събития чрез SIEM системи и анализ на S.M.A.R.T. данни за превантивно откриване на хардуерни проблеми. Реакцията обхваща изолиране на заразеното устройство, блокиране на порта и уведомяване на отговорния екип по сигурността. Възстановяването се основава на наличието на актуални резервни копия и на документирани процедури за възстановяване при бедствие (Disaster Recovery Plan) съгласно NIST SP 800-34 (NIST, 2010).

3.2. Мерки за защита на данните

Защитата на данните, съхранявани на външни носители, се реализира чрез комбинация от технически и административни мерки, обхващащи четири основни направления: криптиране на информацията, антивирусна защита, стратегии за създаване на резервни копия и контрол на достъпа. Тези мерки съответстват на контролите, дефинирани в NIST SP 800-53 (NIST, 2020) и ISO/IEC 27001 Annex A (ISO/IEC, 2022), и следват принципа на защита в дълбочина (Defense in Depth).

1. Криптиране на информацията

Криптирането на данни в покой (encryption at rest) е основна мярка за защита на информацията при физическа загуба или кражба на носителя. Три широко използвани решения покриват основните операционни системи и сценарии на употреба.

BitLocker е вградено решение за пълнодисково криптиране (Full Disk Encryption – FDE) в професионалните и корпоративните издания на Windows. BitLocker To Go разширява тази функционалност към преносими устройства – USB флаш памети и външни дискове. Криптирането се извършва чрез алгоритъма AES (Advanced Encryption Standard) с дължина на ключа 128 или 256 бита в режим XTS (XEX-based Tweaked CodeBook mode with CipherText Stealing). При корпоративно разгръщане BitLocker се интегрира с TPM (Trusted Platform Module) за съхранение на ключовете и с Active Directory Domain Services за централизирано управление на ключовете за възстановяване (recovery keys). Груповите политики (GPO) позволяват принудително изискване на криптиране за всички преносими устройства, свързвани към корпоративни работни станции (Microsoft, 2024d).

VeraCrypt е безплатен инструмент с отворен код за криптиране на дискове и дялове, наследник на TrueCrypt. Той поддържа множество алгоритми за криптиране – AES-256, Serpent, Twofish, Camellia, както и каскадни комбинации (например AES-Twofish-Serpent), които осигуряват допълнително ниво на защита. VeraCrypt предлага две ключови функционалности, отсъстващи в повечето комерсиални продукти: скрити томове (hidden volumes) за правдоподобно отричане (plausible deniability) и преносим режим (traveler mode), при който софтуерът може да се стартира директно от самия USB носител без инсталация на хост системата (IDRIX, 2023). **Криптиране на USB устройство с VeraCrypt става чрез следните стъпки:**

1. Изтегляне и инсталиране на VeraCrypt от официалния сайт (veracrypt.fr). При необходимост от преносим режим – извличане на портативната версия директно на USB устройството.

2. Стартиране на VeraCrypt и избор на „Create Volume" → „Encrypt a non-system partition/drive" за криптиране на целия USB носител или „Create an encrypted file container" за създаване на криптиран контейнер с определен размер.

3. Избор на тип том – „Standard VeraCrypt volume" за обичайна употреба или „Hidden VeraCrypt volume" при нужда от правдоподобно отричане.

4. Конфигуриране на алгоритъма за криптиране – препоръчителна комбинация: AES-256 за криптиране и SHA-512 за хеширане. При повишени изисквания за сигурност може да се използва каскадна схема AES-Twofish-Serpent.

5. Задаване на силна парола (минимум 20 символа, включващи главни и малки букви, цифри и специални символи) или използване на файл-ключ (keyfile) за допълнителна автентикация.

6. Форматиране на тома с избраната файлова система (exFAT за крос-платформена съвместимост, NTFS за Windows среда). VeraCrypt генерира случаен ключ чрез движенията на мишката на потребителя за повишаване на ентропията.

7. Монтиране на криптирания том чрез VeraCrypt – избор на свободна буква на устройството, въвеждане на паролата и натискане на „Mount". След приключване на работата – задължително демонтиране чрез „Dismount".

LUKS (Linux Unified Key Setup) е стандартната спецификация за дисково криптиране в Linux, реализирана чрез модула dm-crypt на ядрото. LUKS съхранява метаданните за криптирането (включително множество ключови слотове – до 8 различни пароли за едно устройство) в стандартизиран хедър в началото на дяла. Криптирането се извършва чрез AES-256 в режим XTS, а за извличане на ключа от паролата се използва функцията PBKDF2 или Argon2id (от LUKS2), която забавя целенасочено процеса на хеширане за защита срещу brute-force атаки. Практическата настройка на LUKS се осъществява чрез инструмента cryptsetup:

sudo cryptsetup luksFormat /dev/sdb1	инициализиране на LUKS криптиране
sudo cryptsetup luksOpen /dev/sdb1 secure_usb	отключване на криптирания дял
sudo mkfs.ext4 /dev/mapper/secure_usb	форматиране с ext4
sudo mount /dev/mapper/secure_usb /mnt/usb	монтиране
sudo umount /mnt/usb	демонтиране
sudo cryptsetup luksClose secure_usb	заключване на криптирания дял

Таблица 4. Сравнение на решенията за криптиране на външни носители

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

2. Антивирусна защита и автоматично сканиране

Автоматичното сканиране на външните носители при включване е ключова превантивна мярка срещу разпространението на зловреден софтуер. В Windows средата Microsoft Defender Antivirus поддържа функцията за сканиране на сменяемите устройства (Removable Drive Scanning), която може да бъде активирана чрез групова политика:

Computer Configuration → Administrative Templates → Windows Components →

Microsoft Defender Antivirus → Scan → Scan removable drives → Enabled

Допълнително, чрез PowerShell може да се настрои автоматично сканиране при монтиране:

Set-MpPreference -DisableRemovableDriveScanning $false

В Linux средата ClamAV е водещото решение с отворен код за антивирусна защита. Автоматичното сканиране при включване на USB устройство може да се реализира чрез комбинация от udev правила и скрипт:

/etc/udev/rules.d/99-usb-scan.rules

ACTION=="add", SUBSYSTEM=="block", KERNEL=="sd[b-z]1",

RUN+="/usr/local/bin/scan_usb.sh %k"

Скриптът scan_usb.sh монтира устройството в временна директория, изпълнява clamscan с актуализирана база от сигнатури и докладва резултатите в системния журнал. При откриване на заплаха устройството се демонтира автоматично и се изпраща известие до администратора.

Политиките за антивирусна защита на преносими носители включват: задължително сканиране преди предоставяне на достъп до съдържанието, ежедневно обновяване на сигнатурните бази, забрана за AutoRun/AutoPlay за всички сменяеми устройства и периодично пълно сканиране на всички свързани носители. NIST SP 800-83 (NIST, 2013) препоръчва организациите да поддържат централизирана система за управление на антивирусната защита, която осигурява единна политика за всички крайни точки (endpoints), включително преносимите устройства.

3. Стратегии за създаване на резервни копия (Backups)

Създаването на резервни копия е основна мярка за осигуряване на възстановяемост на данните при инцидент. Широко приетата стратегия 3-2-1 предвижда поддържане на поне три копия на данните, съхранявани на два различни типа носители, като едно от копията се намира на отделена географска локация (извън сайта). Тази стратегия, популяризирана от фотографа Питър Крог (Krogh, 2009) и препоръчана от US-CERT, минимизира риска от едновременна загуба на всички копия вследствие на единичен инцидент – например пожар, наводнение или рансъмуер атака. Разграничават се три основни типа резервно копиране:

а. Пълно копие (Full Backup)

Чрез пълното копие се копират всички избрани данни независимо от предходни операции. Предимства: най-бързо възстановяване, пълна самостоятелност на всяко копие. Недостатъци: най-голям обем на съхранение и най-дълго време за създаване.

б. Инкрементално копие (Incremental Backup)

Този вид копие копира само данните, променени след последното копие от какъвто и да е тип. Предимства: минимален обем на съхранение и най-бързо създаване. Недостатъци: възстановяването изисква последното пълно копие плюс всички последващи инкрементални копия, което увеличава времето и сложността на процеса.

в. Диференциално копие (Differential Backup)

С негова помощ се копират всички данни, променени след последното пълно копие. Предимства: по-бързо възстановяване от инкременталния подход (необходимо е само последното пълно копие плюс последното диференциално). Недостатъци: обемът нараства прогресивно с времето между пълните копия.

Инструментите за създаване на резервни копия обхващат широк спектър от решения. В Linux средата rsync е стандартният инструмент за инкрементално копиране, който поддържа компресия, SSH тунелиране и частичен трансфер:

```
rsync -avz --delete /home/user/documents/ /mnt/backup_usb/documents/
```

Veeam Backup & Replication е комерсиално решение от корпоративен клас, което поддържа резервно копиране на физически и виртуални машини с възможност за гранулирано възстановяване на отделни файлове. Duplicati е безплатен инструмент с отворен код, който поддържа криптирани инкрементални копия към локални и облачни дестинации, включително външни USB дискове (Duplicati Team, 2023).

4. Контрол на достъпа

Контролът на достъпа до външните носители се реализира на няколко нива: физическо, логическо и административно. Принципът на минималните привилегии (Least Privilege), дефиниран в NIST SP 800-53 контрол AC-6 (NIST, 2020), изисква потребителите да получават само онези права за достъп, които са необходими за изпълнение на конкретните им задачи.

На ниво операционна система контролът се реализира чрез:

Забрана на AutoRun/AutoPlay – премахва възможността за автоматично изпълнение на код от сменяеми носители. В Windows тази настройка се конфигурира чрез GPO:

```
Computer Configuration → Administrative Templates → Windows Components →
AutoPlay Policies → Turn off AutoPlay → Enabled (All drives)
```

Ролеви контрол на достъпа (RBAC – Role-Based Access Control) – определя какви операции могат да извършват различните потребителски роли спрямо външните устройства. Например: стандартните потребители имат достъп само за четене, екипът по сигурност има пълен достъп, а гостовите акаунти нямат никакъв достъп до сменяеми устройства.

Device Whitelisting – разрешава свързването само на предварително одобрени устройства, идентифицирани чрез уникалната комбинация от Vendor ID (VID), Product ID (PID) и сериен номер. В Windows тази политика се конфигурира чрез Device Installation Restrictions в GPO:

Computer Configuration → Administrative Templates → System →

Device Installation → Device Installation Restrictions →

Allow installation of devices that match any of these device IDs → Enabled

В Linux аналогичен контрол се постига чрез USBGuard – демон, който прилага бели и черни списъци за USB устройства:

Примерна конфигурация на USBGuard

sudo usbguard generate-policy > /etc/usbguard/rules.conf

sudo systemctl enable --now usbguard

NIST Cybersecurity Framework (NIST, 2024) категоризира тези мерки в рамките на функцията „Protect" (PR), по-специално контролите PR.AC (Access Control) и PR.DS (Data Security), като подчертава необходимостта от многослойна защита, комбинираща технически и административни контроли.

3.3. Организационна практика в корпоративна среда

Техническите мерки за защита на данните постигат пълния си потенциал единствено когато са вградени в последователна организационна рамка от политики, процедури и контролни механизми. Ефективното управление на външните носители в корпоративна среда обхваща четири взаимосвързани области: политики за контрол на устройствата (Device Control), административен контрол и одит, процедури за сигурно изтриване на данни и съответствие с нормативни изисквания.

1. Политики за използване на флаш памет (Device Control)
Политиката за контрол на устройствата (Device Control Policy) е формален документ, който регламентира условията, при които служителите могат да използват преносими запаметяващи устройства в рамките на организацията. Добре структурираната политика намалява повърхността на атака и осигурява проследимост на действията с преносими носители. По-долу е представена примерна рамка за Device Control Policy, базирана на

препоръките на NIST SP 800-53 (NIST, 2020) и ISO/IEC 27001 Annex A контрол A.8.3 (ISO/IEC, 2022):

Примерна политика за контрол на преносими запаметяващи устройства:

1. Обхват и приложимост – Политиката обхваща всички преносими запаметяващи устройства (USB флаш памети, външни HDD/SSD, SD карти, оптични носители), използвани от служители, контрагенти и посетители в помещенията и мрежите на организацията.

2. Класификация и инвентаризация – Всяко преносимо устройство, използвано за служебни цели, се регистрира в централния инвентарен регистър с уникален идентификатор (сериен номер, VID/PID), определен отговорен служител и ниво на класификация на данните, които ще бъдат съхранявани.

3. Задължително криптиране – Всички преносими устройства, съдържащи служебна информация, се криптират чрез одобрен от организацията инструмент (BitLocker To Go, VeraCrypt или LUKS) с минимална дължина на ключа AES-256.

4. Антивирусно сканиране – Всяко преносимо устройство се сканира автоматично при свързване към корпоративна работна станция. Устройства с открит зловреден софтуер се изолират незабавно.

5. Ограничение по одобрен списък (Whitelisting) – Свързването на преносими устройства е разрешено само за устройства, включени в одобрения списък на организацията. Неодобрени устройства се блокират автоматично.

6. Забрана за лична употреба – Използването на лични преносими устройства за достъп до корпоративни данни е забранено, освен при изрично писмено одобрение от отдела по информационна сигурност.

7. Процедура за пренос на данни – Преносът на класифицирана информация чрез преносими устройства изисква предварително одобрение от непосредствения ръководител и регистриране на операцията в журнала за пренос на данни.

8. Сигурно изтриване при излизане от употреба – Преди повторна употреба, предаване или унищожаване, всяко преносимо устройство преминава през процедура за сигурно изтриване съгласно NIST SP 800-88 (NIST, 2014).

9. Обучение на персонала – Всички служители преминават ежегодно обучение относно рисковете, свързани с преносимите устройства, и задълженията си по настоящата политика.

10. Санкции при нарушение – Нарушаването на политиката може да доведе до дисциплинарни мерки, включително ограничаване на достъпа до ИТ ресурси, писмено

предупреждение или прекратяване на трудовия договор при повторно или умишлено нарушение.

2. Административен контрол и одит

Административният контрол осигурява техническото налагане на политиките и възможността за проследяване на действията с преносими устройства. Трите основни инструмента за реализиране на административен контрол са груповите политики (GPO), системите за управление на мобилни устройства (MDM) и системите за управление на събития по сигурността (SIEM).

Груповите политики (Group Policy Objects – GPO) в Windows среда позволяват централизирано конфигуриране на ограниченията за преносими устройства за всички компютри в домейна. Ключовите GPO настройки включват:

- Removable Storage Access: задаване на права за четене, запис или пълна забрана за различни класове сменяеми устройства.
- Device Installation Restrictions: ограничаване на инсталацията на устройства по клас, VID/PID или сериен номер.
- BitLocker Drive Encryption: принудително изискване за криптиране на сменяеми носители.
- Audit Removable Storage: активиране на журналиране на всички операции за достъп до сменяеми устройства.

MDM (Mobile Device Management) решенията като Microsoft Intune и VMware Workspace ONE разширяват контрола върху устройства, които не са част от Active Directory домейн – включително BYOD (Bring Your Own Device) лаптопи и мобилни устройства. MDM позволява дистанционно прилагане на политики за криптиране, блокиране на USB портове и изтриване на данни при загуба на устройството.

SIEM (Security Information and Event Management) системите агрегират, корелират и анализират журналните записи (logs) от множество източници за откриване на подозрителна активност. При мониторинг на преносимите устройства SIEM системите обработват събития като свързване на ново USB устройство (Event ID 6416 в Windows Security Log), копиране на големи обеми данни към сменяем носител, опити за свързване на неодобрени устройства и промени в конфигурацията на Device Control политиките.

Примерен шестстъпков одитен процес за управление на преносими носители:

1. Планиране – Дефиниране на обхвата на одита (организационни единици, типове устройства, период), критериите за оценка (съответствие с вътрешната политика и ISO/IEC 27001) и екипа за провеждане.

2. Събиране на доказателства – Извличане на журнални записи от GPO, SIEM и MDM; преглед на инвентарния регистър на устройствата; проверка на конфигурациите за криптиране и антивирусна защита на случайна извадка от работни станции.

3. Анализ на съответствието – Съпоставяне на събраните доказателства с изискванията на Device Control Policy. Идентифициране на несъответствия: некриптирани устройства, неодобрени VID/PID комбинации, липсващи журнални записи.

4. Тестване на контролите – Провеждане на контролирани тестове: опит за свързване на неодобрено USB устройство, проверка дали AutoRun е деактивиран, опит за копиране на данни без необходимите привилегии.

5. Докладване – Изготвяне на одитен доклад с констатации, класификация на несъответствията по тежест (критично, високо, средно, ниско) и препоръки за коригиращи действия.

6. Проследяване – Определяне на срокове и отговорници за прилагане на коригиращите мерки. Провеждане на последващ контролен одит за потвърждаване на ефективността на предприетите действия.

3. Процедури за сигурно изтриване на данни

Сигурното изтриване на данни от преносими носители е критична стъпка при излизане на устройството от употреба, при преразпределяне между служители или при изпращане за ремонт. Стандартното изтриване чрез операционната система (delete, format) не премахва физически данните – то само маркира заеманото пространство като свободно, а информацията остава възстановима чрез специализиран софтуер (напр. Recuva, PhotoRec, TestDisk). NIST SP 800-88 Revision 1 (NIST, 2014) дефинира три нива на изтриване:

Логическо изчистване (Clear) – презаписване на всички адресируеми области на носителя с нули, единици или произволни данни чрез един или повече проходи. Този метод е ефективен срещу софтуерни средства за възстановяване, но може да бъде преодолян чрез лабораторни техники при магнитни носители. Инструменти: shred (Linux), cipher /w (Windows), DBAN (Darik's Boot and Nuke).

```
# Пример с shred в Linux – презаписване в три прохода
sudo shred -vzn 3 /dev/sdb
```

Криптографско изтриване (Purge – Cryptographic Erase) – унищожаване на криптографския ключ, с който данните са били криптирани, което прави целия съхраняван обем нечетим. Този метод е особено ефективен за SSD устройства, при които традиционното презаписване не гарантира достигане до всички NAND клетки поради механизмите за wear leveling и over-provisioning. Предпоставка е устройството да е било криптирано предварително (чрез BitLocker, VeraCrypt, LUKS или хардуерно SED криптиране). При SSD устройства с

поддръжка на ATA Secure Erase или NVMe Format командата, фърмуерът може да извърши вътрешно криптографско изтриване:

```
# NVMe Secure Erase в Linux
sudo nvme format /dev/nvme0n1 --ses=1
```

Физическо унищожаване (Destroy) – физическо разрушаване на носителя чрез раздробяване (shredding), дегаусиране (degaussing – само за магнитни носители), изгаряне или химическо разтваряне. Това е единственият метод, гарантиращ абсолютна невъзстановимост на данните, и се прилага за носители с най-висока класификация на информацията. Стандартът DoD 5220.22-M (U.S. Department of Defense, 2006) исторически е дефинирал процедурата с три прохода на презаписване, но актуалните препоръки на NIST SP 800-88 го заместват с по-съвременни методи, подходящи за различните технологии (NIST, 2014).

Примерна стандартна оперативна процедура (SOP) за сигурно изтриване:

1. Идентификация – Определяне на типа на носителя (HDD, SSD, USB, SD, CD/DVD) и нивото на класификация на съхраняваните данни (публични, вътрешни, поверителни, строго поверителни).

2. Избор на метод – Съгласно нивото на класификация: Clear за публични и вътрешни данни; Purge (криптографско изтриване) за поверителни данни; Destroy за строго поверителни данни.

3. Архивиране – Проверка дали данните, които все още са необходими, имат актуално резервно копие преди изтриването.

4. Изпълнение – Провеждане на избрания метод за изтриване с използване на одобрените инструменти. За SSD устройства – криптографско изтриване или ATA Secure Erase/NVMe Format. За HDD – презаписване в три прохода или дегаусиране. За CD/DVD – физическо раздробяване.

5. Подвърждение – Потвърждаване на успешното изтриване чрез опит за четене на носителя с инструмент за възстановяване на данни. При Clear и Purge – проверка за наличие на остатъчни данни.

6. Документиране – Регистриране на операцията в журнала за сигурно изтриване с посочване на: дата, отговорен служител, тип на носителя, сериен номер, приложен метод и резултат от верификацията.

7. Разпореждане – Предаване на устройството за повторна употреба (след Clear/Purge) или за физическо унищожаване (след Destroy), съгласно вътрешните правила на организацията.

4. Съответствие с нормативни изисквания (GDPR)
Общият регламент относно защитата на данните (GDPR – Regulation (EU) 2016/679) въвежда задължения за организациите, обработващи лични данни на граждани на Европейския съюз, които имат пряко отношение към управлението на преносимите запаметяващи устройства. Член 32 от GDPR изисква прилагането на „подходящи технически и организационни мерки" за осигуряване на ниво на сигурност, съответстващо на риска, включително „криптиране на личните данни" и „способност за гарантиране на постоянната поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване" (European Parliament, 2016).

В контекста на външните носители тези изисквания се конкретизират в следните задължения: криптиране на всички преносими устройства, съдържащи лични данни (член 32, параграф 1, буква „а"); водене на регистър на дейностите по обработване, включително преноса на данни чрез преносими носители (член 30); уведомяване на надзорния орган в срок от 72 часа при установяване на нарушение на сигурността на данните, включително загуба на некриптиран носител с лични данни (член 33); и сигурно изтриване на личните данни при изтичане на целта на обработването или при поискване от субекта на данните (член 17 – „право на изтриване") (European Parliament, 2016).

ISO/IEC 27001 Annex A предоставя рамката от контроли, чрез която организациите могат да демонстрират съответствие с GDPR. Контролите A.8.3 (Handling of Assets), A.10.1 (Cryptographic Controls), A.11.2 (Equipment) и A.18.1 (Compliance with Legal and Regulatory Requirements) са пряко свързани с управлението на преносимите носители (ISO/IEC, 2022).

3.4. Практически примери и препоръки

Реалните инциденти, свързани с външни запаметяващи устройства, илюстрират практическата значимост на рисковете и мерките, описани в предходните раздели. Анализът на конкретни казуси позволява извличане на приложими поуки (Lessons Learned) и подчертава критичността на последователния подход към информационната сигурност.

Казус 1: Stuxnet – целенасочена атака чрез USB носител
През 2010 г. е открит компютърният червей Stuxnet, който е проектиран да саботира иранската ядрена програма чрез атака на системите за управление на центрофугите в съоръжението в Натанз. Stuxnet се разпространява първоначално чрез USB флаш памети, експлоатирайки четири нулеви уязвимости (zero-day vulnerabilities) в Windows, включително уязвимостта в обработката на LNK файлове (CVE-2010-2568). След проникване в мрежата червеят се разпространява латерално и целенасочено модифицира логиката на програмируемите логически контролери (PLC) на Siemens SIMATIC S7-300, като променя скоростта на въртене на центрофугите, докато едновременно с това изпраща нормални телеметрични данни към операторите. Резултатът е физическо увреждане на приблизително 1 000 центрофуги.

Изведени поуки: Stuxnet демонстрира, че дори физически изолирани мрежи (air-gapped networks) са уязвими чрез вектора на преносимите устройства. Инцидентът подчертава необходимостта от: строг контрол на USB портовете в критични инфраструктури, сканиране на всички преносими носители преди свързване, прилагане на принципа на минималните привилегии и сегментиране на мрежата дори в рамките на изолирани среди.

Казус 2: Изтичане на данни от Heathrow Airport (2017)

През октомври 2017 г. жител на Лондон открива USB флаш памет на улица в западната част на града. Устройството съдържа 76 папки с некриптирана чувствителна информация, свързана със сигурността на летище Хийтроу – включително маршрути на кралицата, карти на тунелите, разписания на патрули и CCTV позиции. Разследването установява, че устройството принадлежи на служител на летището, който е копирал документите за лична употреба без разрешение. Британският орган за защита на данните (ICO) налага глоба от 120 000 паунда на Heathrow Airport Holdings за нарушение на Data Protection Act 1998, като изрично посочва липсата на криптиране на преносимите устройства и неадекватните политики за контрол като основни причини за инцидента.

Изведени поуки: Случаят с Хийтроу илюстрира комбинирания ефект на човешкия фактор и липсата на технически контроли. Задължителното криптиране на преносимите устройства би направило данните нечетими за всеки, който намери устройството. Инвентаризацията и device whitelisting биха предотвратили копирането на класифицирана информация на неодобрен носител. Обучението на персонала относно рисковете от пренос на данни извън корпоративната среда е от критична важност.

Казус 3: Успешно внедряване на Device Control в IBM

IBM е сред първите глобални корпорации, въвели цялостна политика за забрана на преносимите запаметяващи устройства. През 2018 г. компанията обявява глобална забрана за използване на сменяеми носители за данни от всичките си приблизително 350 000 служители. Политиката се реализира чрез комбинация от GPO ограничения, MDM политики, DLP (Data Loss Prevention) агенти на крайните точки и SIEM мониторинг. Като алтернатива на физическите носители IBM предоставя на служителите си достъп до вътрешна облачна платформа за сигурен трансфер на файлове. Според вътрешни данни на компанията, тази мярка е довела до 50% намаление на инцидентите, свързани с изтичане на данни чрез преносими носители, в рамките на първата година от внедряването.

Изведени поуки: Случаят на IBM показва, че цялостната забрана на преносимите носители е реалистична дори в глобална организация от този мащаб, при условие че се предостави адекватна алтернатива за легитимните бизнес нужди. Успехът на политиката зависи от комбинацията между технически контроли (GPO, DLP), административни мерки (политики, обучение) и осигуряване на удобни алтернативни канали за пренос на данни.

Инструменти за мониторинг

Ефективният мониторинг на действията с преносими устройства изисква специализирани инструменти, които осигуряват видимост, контрол и одитна следа.

USBGuard е инструмент с отворен код за Linux, който реализира бели и черни списъци за USB устройства на ниво ядро. USBGuard прехваща устройствата преди зареждане на драйвера и позволява или блокира достъпа според предварително дефинирани правила, базирани на VID, PID, сериен номер, интерфейсен клас и други атрибути. Инструментът поддържа интерактивен режим (IPC), в който администраторът получава известие и ръчно одобрява или отхвърля ново устройство.

Windows Device Control (Microsoft Defender for Endpoint) предоставя централизирано управление на политиките за преносими устройства в корпоративна Windows среда. Решението позволява гранулиран контрол – разрешаване, блокиране или ограничаване до четене (read-only) за конкретни класове устройства, VID/PID комбинации или отделни устройства. Всички действия се журналират и могат да се визуализират в Microsoft 365 Defender портала.

Endpoint DLP (Data Loss Prevention) решенията – включително Microsoft Purview DLP, Symantec DLP и Digital Guardian – проследяват и контролират потока на чувствителна информация към преносими устройства. DLP агентите анализират съдържанието на файловете в реално време и прилагат правила, базирани на класификацията на данните – например блокиране на копиране на файлове, съдържащи ЕГН или номера на кредитни карти, към USB носител.

SIEM платформите (Splunk, Graylog, Elastic SIEM) осигуряват централизирана агрегация, корелация и визуализация на събитията от всички крайни точки. Примерна заявка за търсене на USB събития в Splunk:

```
index=windows sourcetype=WinEventLog:Security EventCode=6416
| stats count by Device_Description, Account_Name, ComputerName
| sort -count
```

Тази заявка извлича всички събития за свързване на ново PnP устройство (Event ID 6416), групира ги по описание на устройството, потребител и компютър и ги подрежда по честота – което позволява бързо идентифициране на аномални модели.

Следният чеклист обобщава ключовите мерки за управление на преносимите запаметяващи устройства, като всяка практика е свързана с една от петте функции на NIST Cybersecurity Framework (NIST, 2024)

Таблица 5. Чеклист с добри практики и съответствие с NIST CSF

№	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)

3.5. Сравнителен анализ на решения за защита на външни носители

Описаните в предходните подраздели мерки за защита – криптиране, административен контрол, Device Whitelisting – се реализират чрез различни технологични решения, всяко от които притежава специфични предимства и ограничения. Таблица 6 представя съпоставка на петте основни решения по четири критерия: поддържана платформа, възможност за централно управление, ценови модел и ниво на защита.

Таблица 6. Сравнителен анализ на решения за защита на външни носители

Решение	Платформа	Централно управление	Цена	Ниво на защита
BitLocker To Go	Windows Pro/Ent	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–Висока

Забележка: Нивото на защита е обобщена оценка, базирана на комбинацията от криптографска сила, устойчивост на атаки и зрялост на технологията.

BitLocker To Go е предпочитаният избор в хомогенни Windows среди, управлявани чрез Active Directory. Интеграцията с GPO позволява централизирано налагане на задължително криптиране за преносими носители, автоматично архивиране на ключовете за възстановяване в AD DS и одит на операциите. Основното ограничение е платформената зависимост – криптираните носители се отключват нативно само в Windows Pro и Enterprise, а в macOS и Linux е необходим софтуер от трети страни с ограничена функционалност (Microsoft, 2024d).

VeraCrypt предоставя най-високо ниво на гъвкавост и криптографска сила. Поддръжката на каскадни алгоритми (например AES-Twofish-Serpent), скрити томове (hidden volumes) и преносим режим (traveler mode) го правят подходящ за сценарии с повишени изисквания за сигурност. Същевременно липсата на централно управление ограничава приложимостта му в големи организации – всеки потребител управлява криптирането самостоятелно, което увеличава риска от човешка грешка (IDRIX, 2023).

LUKS (Linux Unified Key Setup) е стандартното решение за криптиране на блокови устройства в Linux среда. С поддръжка на до осем ключови слота и съвременни алгоритми за деривация на ключове (Argon2id) LUKS осигурява надеждна защита. Ограничението е аналогично на BitLocker – липса на нативна крос-платформена съвместимост.

GPO/MDM контролът чрез Group Policy Objects (в Windows) или решения за управление на мобилни устройства като Microsoft Intune (в хибридни и облачни среди) позволява централизирано управление на достъпа до преносими носители без необходимост от криптиране на самото устройство. Тези политики работят на ниво операционна система и правоприлагане, а не на ниво данни, което означава, че защитават от неоторизиран достъп, но не и от последиците при физическа кражба на вече записани данни.

USB Whitelisting (Device Whitelisting) е допълваща мярка, която ограничава свързването само до предварително одобрени устройства, идентифицирани по Vendor ID, Product ID и сериен номер. В Windows тя се реализира чрез GPO или Microsoft Defender for Endpoint Device Control, а в Linux – чрез USBGuard. Нивото на защита зависи от стриктността на инвентарния регистър и от устойчивостта на идентификаторите срещу подправяне (spoofing).

В практически условия оптималната стратегия комбинира няколко от изброените решения. За корпоративна Windows среда с Active Directory препоръчителната комбинация включва: GPO за ограничаване на достъпа по роли (раздел 2.2.6), BitLocker To Go за задължително криптиране на одобрените устройства и Device Whitelisting за допускане само на инвентаризирани носители. Този тристъпков модел адресира едновременно контрола на достъпа (кой може да използва устройства), защитата на данните (криптиране в покой) и управлението на устройствата (само одобрени носители).

3.6. Практическа демонстрация: GPO контрол и BitLocker To Go в среда на Active Directory

Демонстрацията се извършва в среда на Windows Server с Active Directory Domain Services (AD DS). Демонстрацията обхваща: създаване на организационна структура (OU) с две групи потребители, конфигуриране на GPO за забрана на записа за неоторизирани потребители и налагане на задължително BitLocker To Go криптиране за оторизираните.

Стъпка 1. Организационна структура (OU)
В Active Directory Users and Computers (dsa.msc) се създава следната йерархия:

```
Domain: corp.local
└── OU: USB-Policy
    ├── OU: USB-Allowed    (потребители с право на запис върху USB)
    │   └── Security Group: GRP_USB_Allowed
    └── OU: USB-Blocked    (потребители без право на запис върху USB)
        └── Security Group: GRP_USB_Blocked
```

Разпределението на потребителите между двете OU определя приложимия GPO. Потребители, които по естеството на работата си имат нужда от пренос на данни чрез USB (напр. ИТ администратори, инженери), се включват в GRP_USB_Allowed. Всички останали потребители се разполагат в GRP_USB_Blocked.

Стъпка 2. GPO за забрана на записа – „USB-Block-Write"
В Group Policy Management Console (gpmc.msc) се създава нов GPO с име „USB-Block-Write" и се свързва (Link) с OU: USB-Blocked.

Настройки:

1. Отворете Group Policy Management Editor

2. Навигирайте до: Computer Configuration → Policies → Administrative Templates → System → Removable Storage Access

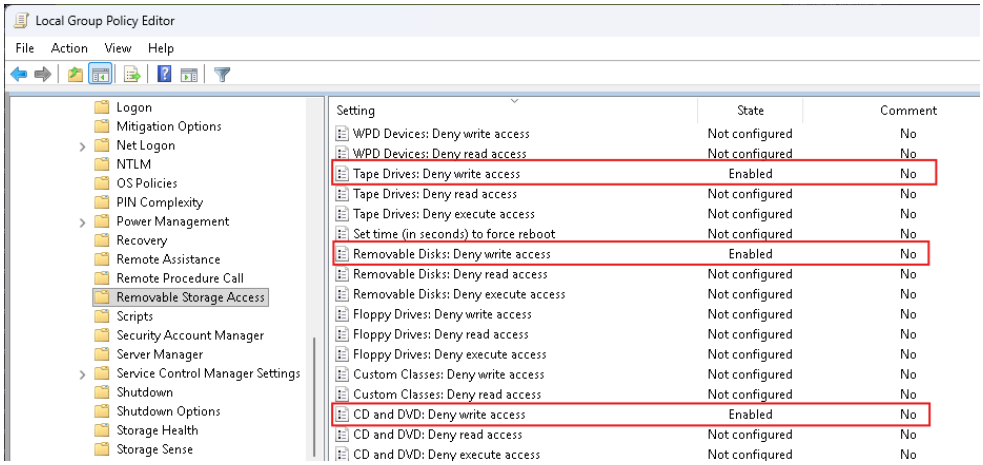
3. Активирайте следните настройки:

- Removable Disks: Deny write access → Enabled
- CD and DVD: Deny write access → Enabled
- Tape Drives: Deny write access → Enabled

4. Навигирайте до: Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Object Access

5. Активирайте: Audit Removable Storage → Success, Failure

Тази конфигурация позволява на потребителите от OU: USB-Blocked да четат съдържанието на USB устройства, но забранява записването. Всеки опит за запис се отбелязва в Windows Event Log.



***Фиг. 1**: Екранна снимка от Group Policy Management Editor → Computer Configuration → Policies → Administrative Templates → System → Removable Storage Access; настройките "Tape Drives: Deny write access", "Removable Disks: Deny write access" и "CD and DVD: Deny write access" са включени (Enabled) и подчертани в червено.*

Стъпка 3. GPO за задължително криптиране – „USB-Require-BitLocker"
Създава се втори GPO с име „USB-Require-BitLocker" и се свързва с OU: USB-Allowed.

Настройки:

1. Навигирайте до: Computer Configuration → Policies → Administrative Templates → Windows Components → BitLocker Drive Encryption → Removable Data Drives

2. Активирайте:

- 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 on removable data drives → Checked

- Choose how BitLocker-protected removable drives can be recovered → Enabled

  → Save BitLocker recovery information to AD DS for removable data drives → Checked

3. Навигирайте до: Computer Configuration → Policies → Administrative Templates → System → Removable Storage Access

- Removable Disks: Deny write access → Not Configured (записът е разрешен, но само след криптиране)

Тази конфигурация позволява на потребителите от OU: USB-Allowed да използват USB устройства за четене и запис, но само при условие, че носителят е криптиран с BitLocker. При свързване на некриптирано устройство системата предлага активиране на BitLocker To Go.

***Фиг. 2**: Диалогов прозорец за активиране на BitLocker при свързване на некриптирано устройство.*

***Източник**: Microsoft Learn (2024)*

Стъпка 4. Прилагане и верификация

След създаването на GPO обектите се прилагат към целевите OU:

1. Изпълнете gpupdate /force на тестова работна станция, членуваща в съответната OU

2. Рестартирайте работната станция за пълно прилагане на политиките

3. Верифицирайте чрез gpresult /r, че съответният GPO е приложен

Стъпка 5. Очаквани резултати

Таблица 7. Сравнение на достъпа до преносими устройства по роли

Операция	USB-Allowed (GRP_USB_Allowed)	USB-Blocked (GRP_USB_Blocked)
Четене от USB устройство	Разрешено	Разрешено

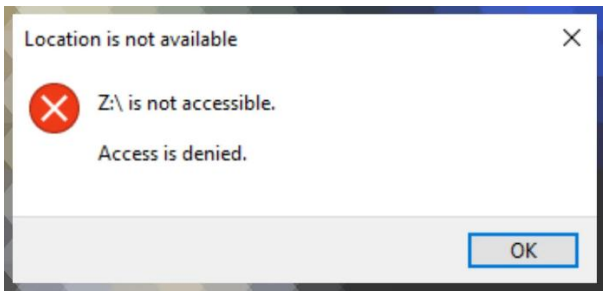
Запис върху USB устройство	Разрешено (само при активиран BitLocker)	Забранено (Deny write access)
Криптиране с BitLocker To Go	Задължително за запис	Не е приложимо
Одит (Event Log)	Да – Event ID 4663 (успешен достъп)	Да – Event ID 4663 (отказан достъп)

Сценарий А – Оторизиран потребител (OU: USB-Allowed):

Потребителят свързва USB флаш памет. Ако носителят вече е криптиран с BitLocker, системата изисква парола за отключване, след което предоставя пълен достъп за четене и запис. Ако носителят не е криптиран, системата показва диалогов прозорец за активиране на BitLocker To Go с избор на парола (минимум 8 символа) и метод за архивиране на ключа за възстановяване (AD DS). След успешно криптиране записът е разрешен.

Сценарий Б – Неоторизиран потребител (OU: USB-Blocked):

Потребителят свързва USB флаш памет. Системата разпознава устройството и разрешава четене – файловете се виждат в Explorer и могат да бъдат отворени. При опит за копиране на файл върху устройството или за създаване на нов файл системата показва съобщение „Access Denied" (Достъпът е отказан). В Event Viewer се записва Event ID 4663 с резултат „Failure", съдържащ информация за потребителя, устройството и времевия маркер.



***Фиг. 3**: Съобщение „Access Denied" при опит за запис от потребител в OU: USB-Blocked*

***Източник**: Windows Report – Location Is Not Available Access is Denied*

4. ЗАКЛЮЧЕНИЕ

Настоящата дипломна работа представя цялостен анализ на управлението на външните запаметяващи устройства, обхващащ както технологичните основи, така и практическите аспекти на тяхната сигурна експлоатация в съвременната информационна среда. Изследването следва структуриран подход – от класификацията на устройствата и техните характеристики, през системната интеграция и сравнителния анализ, до идентифицирането на рисковете и формулирането на конкретни мерки за защита.

В теоретичната част са разгледани петте основни категории външни носители – USB флаш памети, твърдотелни дискове (SSD), твърди дискове с магнитен запис (HDD), карти с памет (SD) и оптични носители (CD/DVD). Анализът на техническите характеристики – скорости на четене и запис, интерфейси за свързване (USB 2.0/3.x, SATA III, NVMe, Thunderbolt), капацитет, латентност и надеждност – показва, че всяка технология заема определена ниша, определена от баланса между производителност, мобилност, цена и дълготрайност. Не съществува универсално „най-добро" устройство; оптималният избор е функция на конкретните изисквания на потребителя или организацията.

Изследването на драйверите и системната интеграция разкрива, че трите водещи операционни системи – Windows, Linux и macOS – реализират поддръжката на външните носители чрез различни механизми (USBSTOR.SYS, udev/kernel modules и I/O Kit), като всяка от тях предоставя специфични възможности за контрол на достъпа. Процесът на USB enumeration и технологията Plug and Play осигуряват автоматично разпознаване и монтиране, но същевременно разширяват повърхността на атака – всяко свързано устройство е потенциален вектор за компрометиране на системата. Изборът на файлова система (FAT32, NTFS, exFAT, ext4, APFS) директно влияе върху нивото на защита, като файловите системи без журналинг и контрол на достъпа (FAT32, exFAT) създават допълнителни рискове.

Сравнителният анализ на петте категории устройства потвърждава, че технологичното многообразие изисква диференциран подход към управлението. Външните HDD дискове остават оптимални за масово архивиране поради ниската си цена за гигабайт, SSD устройствата са безалтернативни при нужда от висока скорост, USB флаш паметите са най-практичният вариант за ежедневен обмен на файлове, SD картите доминират в мобилната екосистема, а оптичните носители запазват нишата си в дългосрочното архивиране с гарантирана неизменяемост на записа.

Практическата част на работата демонстрира, че рисковете, свързани с външните носители, обхващат пет основни категории: физически повреди, заплахи от зловреден софтуер (включително рансъмуер и BadUSB атаки), загуба на данни, неоторизиран достъп и човешки фактор. Матрицата за оценка на риска, изградена по методологията на NIST SP 800-30 и ISO/IEC 27005, идентифицира заразяването със зловреден софтуер чрез USB и кражбата или загубата на некриптиран носител като рискове с критично ниво, изискващи приоритетно адресиране.

Предложените мерки за защита формират многопластов модел, следващ принципа на защита в дълбочина (Defense in Depth). Криптирането на данни в покой – чрез BitLocker To Go, VeraCrypt или LUKS – неутрализира последиците от физическа загуба или кражба. Антивирусната защита и автоматичното сканиране при включване на устройство противодействат на заплахите от зловреден софтуер. Стратегията за резервни копия 3-2-1 осигурява възстановяемост при загуба на данни. Контролът на достъпа – чрез Device

Whitelisting, деактивиране на AutoRun/AutoPlay и ролеви контрол (RBAC) – ограничава повърхността на атака.

Организационната рамка, включваща Device Control политики, административен контрол чрез GPO и MDM, одитни процедури и процеси за сигурно изтриване на данни съгласно NIST SP 800-88, осигурява системност и проследимост. Съответствието с GDPR (Регламент (ЕС) 2016/679) и ISO/IEC 27001 гарантира нормативната адекватност на предложения модел за управление.

Анализът на реални инциденти потвърждава практическата значимост на изследваните въпроси. Случаят Stuxnet (2010) демонстрира, че дори физически изолирани мрежи (air-gapped) са уязвими чрез вектора на преносимите устройства, като последиците могат да засегнат критична инфраструктура. Инцидентът с летище Хийтроу (2017) илюстрира комбинирания ефект на човешкия фактор и липсата на технически контроли – некриптиран USB носител с чувствителна информация е открит на публично място, водейки до глоба от 120 000 паунда. Успешният опит на IBM с пълна забрана на преносимите носители за 350 000 служители доказва, че цялостният подход е реалистичен дори в глобален мащаб, при условие че се предоставят адекватни алтернативи за легитимните бизнес процеси.

Чеклистът с десет добри практики, съпоставен с петте функции на NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover), предоставя приложима методическа основа за организации от различен мащаб. Инвентаризацията на устройствата, класификацията на данните, задължителното криптиране, Device Whitelisting, антивирусното сканиране, SIEM мониторингът, процедурите за реакция при инцидент, стратегията за резервни копия и сигурното изтриване на данни формират цялостна система, покриваща жизнения цикъл на информационната сигурност.

Въз основа на проведеното изследване могат да бъдат формулирани следните основни изводи:

1. Външните запаметяващи устройства остават критичен компонент от информационната инфраструктура, въпреки нарастващата популярност на облачните технологии. Физическата преносимост, независимостта от интернет връзка и високата скорост на локален достъп ги правят незаменими в множество сценарии – от работа с класифицирана информация в изолирани мрежи до мобилна фотография и видеопродукция.
2. Рисковете, свързани с тези устройства, са реални, многоаспектни и с потенциално катастрофални последици. Еволюцията на заплахите – от ранните boot-секторни вируси, разпространявани чрез дискети, до усъвършенствани атаки като BadUSB и Stuxnet – показва, че атакуващите непрекъснато адаптират методите си към новите технологии.
3. Ефективното управление на външните носители изисква интегриран подход, комбиниращ технически контроли (криптиране, антивирусна защита, контрол на

портовете), организационни мерки (политики, одит, обучение) и съответствие с нормативните изисквания (GDPR, ISO/IEC 27001). Нито една единична мярка не може да осигури достатъчна защита сама по себе си – необходим е принципът на защита в дълбочина.

4. Човешкият фактор остава най-непредвидимата и трудно контролируема променлива. Техническите контроли минимизират повърхността на атака, но устойчивата сигурност зависи от информираността и дисциплината на потребителите, което подчертава значението на регулярното обучение и повишаването на осведомеността.

Перспективите за бъдещо развитие в тази област включват няколко ключови направления. Навлизането на USB4 и Thunderbolt 5 с пропускателна способност до 120 Gbit/s ще увеличи както възможностите за продуктивност, така и потенциалните рискове от бързо ексфилтриране на данни. Масовото въвеждане на хардуерно криптиране в самите устройства (Self-Encrypting Drives – SED) ще опрости управлението на ключовете. Развитието на технологии за изкуствен интелект в областта на поведенческия анализ (UEBA – User and Entity Behavior Analytics) ще подобри детектирането на аномална активност, свързана с преносими устройства.

Особено перспективна е интеграцията с платформи за управление на мобилни устройства (MDM) като Microsoft Intune, която позволява централизирано прилагане на политики за преносими носители не само в рамките на локален домейн, но и в хибридни и изцяло облачни среди. Автоматизираният одит на USB събития чрез SIEM платформи от ново поколение – по-конкретно Microsoft Sentinel – ще осигури корелация на журналните записи от крайните точки в реално време и ще съкрати времето за реакция при инцидент. Прилагането на DLP (Data Loss Prevention) политики чрез решения като Microsoft Purview ще позволи автоматично класифициране и блокиране на чувствително съдържание при опит за копиране върху външни носители, предотвратявайки изтичането на данни още преди то да се случи.

Усъвършенстването на архитектурите с нулево доверие (Zero Trust Architecture) – основани на принципа „никога не вярвай, винаги верифицирай" – ще наложи третирането на всяко устройство, включително преносимите носители, като потенциално компрометирано до доказване на противното. В съчетание с непрекъсната автентикация и адаптивен контрол на достъпа Zero Trust подходът ще промени фундаментално начина, по който организациите управляват взаимодействието с външните запаметяващи устройства.Реализирането на поставената цел – разработване на комплексен модел за управление на външните запаметяващи устройства, гарантиращ баланс между оперативна съвместимост и информационна сигурност – е постигнато чрез систематичния анализ на технологичната база, рисковете, мерките за защита и организационните практики. Предложеният модел е приложим както в корпоративна среда, така и в публичния сектор и критичната

инфраструктура, като неговата ефективност зависи от последователното прилагане на всички компоненти – технически, организационни и нормативни.

5. ПРИНОСИ

Въз основа на проведеното изследване могат да бъдат формулирани следните приноси на настоящата дипломна работа:

1. Систематизиран технологичен анализ на петте основни категории външни запаметяващи устройства – USB флаш памети, твърдотелни дискове (SSD), твърди дискове с магнитен запис (HDD), карти с памет (SD) и оптични носители (CD/DVD). Анализът обхваща ключовите технически параметри – скорости на четене и запис, интерфейси за свързване (USB 2.0/3.x, SATA III, NVMe, Thunderbolt), капацитет, латентност и надеждност – и е представен в сравнителна таблица (Таблица 2), улесняваща избора на носител съобразно конкретни изисквания.

2. Разработена матрица за оценка на рисковете (Таблица 3), класифицираща осем основни заплахи при използването на външни носители по вероятност и въздействие съгласно методологията на NIST SP 800-30 и ISO/IEC 27005. Матрицата е подкрепена с актуални статистически данни от ENISA (37 % от целевите атаки срещу индустриални системи се осъществяват чрез USB), Ponemon Institute (средна цена на инцидент с изтичане на данни – $3,86 милиона) и Verizon DBIR (2023), което я превръща в приложим инструмент за оценка на риска в корпоративна среда.

3. Предложен многопластов модел за защита на външните запаметяващи устройства, следващ принципа на защита в дълбочина (Defense in Depth). Моделът интегрира три взаимно допълващи се слоя: административен контрол чрез GPO (Group Policy Object) и политики за ограничаване на достъпа до преносими носители; контрол на устройствата чрез Device Whitelisting по Vendor ID, Product ID и сериен номер; и криптиране на данни в покой чрез AES-256 (BitLocker To Go, VeraCrypt или LUKS). Предложеният модел е съпоставен с изискванията на ISO/IEC 27001 Annex A и NIST SP 800-53.

4. Сравнителен анализ на три реални инцидента с различен мащаб и характер – кибератаката Stuxnet (2010), изтичането на данни от летище Хийтроу (2017) и глобалната забрана на преносимите носители в IBM (2018). Анализът извежда конкретни уроци за всеки казус: необходимостта от строг контрол на портовете дори в изолирани (air-gapped) мрежи, ефектът на комбинирания човешки и технически фактор при некриптирани устройства и доказателството, че цялостната забрана е реалистична в глобален мащаб при осигуряване на алтернативни средства за обмен на данни.

5. Разработен чеклист с десет добри практики за управление на външни носители (Таблица 5), съпоставени с петте функции на NIST Cybersecurity Framework 2.0 (Identify, Protect, Detect, Respond, Recover) и контролите на ISO/IEC 27001 Annex A. Чеклистът покрива целия жизнен цикъл на информационната сигурност – от инвентаризация на устройствата и

класификация на данните, през криптиране, Device Whitelisting и SIEM мониторинг, до процедури за реакция при инцидент и сигурно изтриване по NIST SP 800-88. Той предоставя приложима методическа основа за организации от различен мащаб.

6. ПРИЛОЖЕНИЯ

Приложение А. Примерна конфигурация на Device Control Policy (Microsoft Defender for Endpoint)

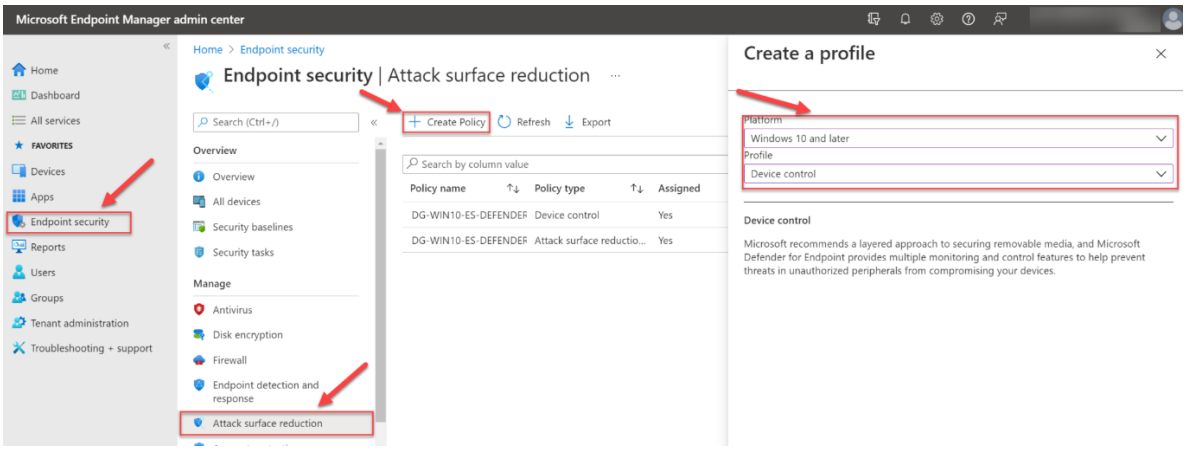
Следната XML конфигурация дефинира политика за контрол на преносими устройства, която разрешава достъп само до одобрени USB устройства, идентифицирани по Vendor ID и Product ID. Неодобрените устройства получават достъп само за четене.

```
<PolicyRule Id="DenyWriteToUnapprovedUSB">
  <Name>Забрана за запис върху неодобрени USB устройства</Name>
  <IncludedIdList>
    <RemovableMediaDevices />
  </IncludedIdList>
  <ExcludedIdList>
    <VendorId>0781</VendorId>   <!-- SanDisk -->
    <ProductId>5591</ProductId>  <!-- Ultra Flair USB 3.0 -->
    <VendorId>0951</VendorId>   <!-- Kingston -->
    <ProductId>1666</ProductId>  <!-- DataTraveler 100 G3 -->
  </ExcludedIdList>
  <Entry>
    <Type>Deny</Type>
    <Options>
      <AccessMask>Write</AccessMask>
    </Options>
    <Notification>
      <Message>Записът върху неодобрени USB устройства е забранен. Обърнете се към ИТ отдела за одобрение.</Message>
    </Notification>
  </Entry>
```

```
</PolicyRule>
<PolicyRule Id="AuditAllUSBConnections">
  <Name>Одит на всички USB свързвания</Name>
  <IncludedIdList>
    <RemovableMediaDevices />
  </IncludedIdList>
  <Entry>
    <Type>AuditAllow</Type>
    <Options>
      <AccessMask>Read,Write,Execute</AccessMask>
    </Options>
  </Entry>
</PolicyRule>
```

Идентификаторите VendorId и ProductId се извличат от Device Manager (Диспечер на устройства) или чрез командата:

```
Get-PnpDevice -Class DiskDrive | Select-Object InstanceId, FriendlyName\
```



Фиг. 4. *Microsoft Defender for Endpoint – Device Control Policy в административния портал*

Източник*: Appel (n.d.)*

Приложение Б. Примерна GPO конфигурация за контрол на преносими устройства

Конфигурацията по-долу описва настройките на Group Policy Object (GPO), приложим към организационна единица (OU) с неоторизирани потребители. Настройките се достъпват чрез Group Policy Management Editor (gpmc.msc).

Б.1. Забрана за запис върху преносими устройства

Път: Computer Configuration → Policies → Administrative Templates → System → Removable Storage Access

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

Б.2. Ограничаване на инсталирането на устройства по клас

Път: Computer Configuration → Policies → Administrative Templates → System → Device Installation → Device Installation Restrictions

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)

Б.3. Задължително криптиране с BitLocker за преносими носители

Път: Computer Configuration → Policies → Administrative Templates → Windows Components → BitLocker Drive Encryption → Removable Data Drives

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	

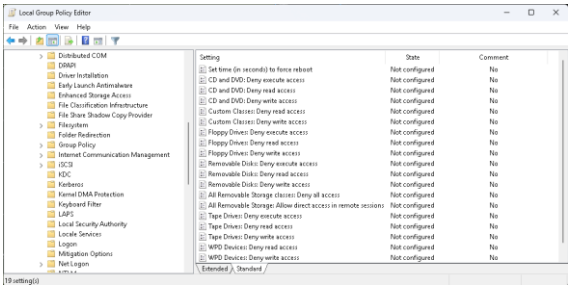
Б.4. Одит на преносими устройства

Път: Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Object Access

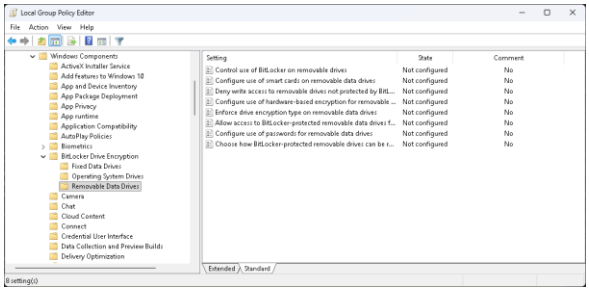
Настройка	Стойност
Audit Removable Storage	Success, Failure
Audit PNP Activity	Success

Събитията се записват в Windows Event Log:

- Event ID 6416: Ново PnP устройство е разпознато
- Event ID 4663: Опит за достъп до обект на преносим носител



***Фиг. 5**: Group Policy Management Editor – настройки за Removable Storage Access*



***Фиг. 6**: Group Policy Management Editor – BitLocker Removable Data Drives*

Приложение В. Шаблон за инвентаризация на USB устройства

Следният шаблон служи за регистриране и проследяване на всички одобрени USB устройства в организацията. Попълва се от ИТ администратора при първоначална регистрация и се актуализира при всяка промяна на статуса.

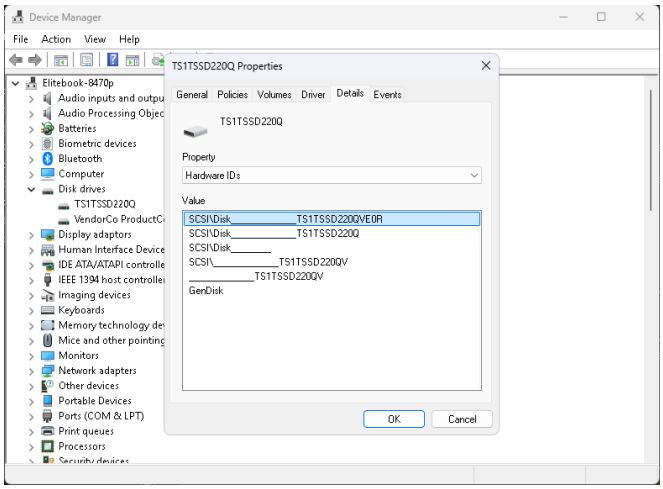
№	VID	PID	Сериен номер	Произв.	Модел	Потреб.	Отдел	Дата на рег.	Статус
1	781	5591	4C53000121	SanDisk	Ultra Flair 64GB	Иванов, П.	ИТ	15.01.2025	Активен
2	951	1666	E0D55EA573	Kingston	DT100 G3 32GB	Петрова, М.	Счетов.	22.02.2025	Активен

3	8564	1000	AA00000489	Transcend	JetFlash 128GB	Георгиев, Д.	Маркет.	10.03.2025	Деактив.
4									

Инструкции за попълване:

1. VID и PID се извличат от Device Manager → Properties → Details → Hardware Ids (формат: USB\VID_xxxx&PID_xxxx)
2. Серийният номер се извлича от свойствата на устройството или чрез PowerShell:

   Get-PnpDevice -Class DiskDrive | Get-PnpDeviceProperty -KeyName DEVPKEY_Device_SerialNumber
3. Статус: „Активен", „Деактивиран" или „Изгубен/Откраднат"
4. При статус „Изгубен/Откраднат" се инициира процедура за реакция при инцидент съгласно GDPR чл. 33 (уведомяване в рамките на 72 часа)



***Фиг. 7**: Device Manager – Properties → Details → Hardware Ids на USB устройство*

Приложение Г. Чеклист за сигурно изтриване на данни по NIST SP 800-88 Rev. 1

Чеклистът се прилага при извеждане от експлоатация, преразпределение или унищожаване на външен носител, съдържащ чувствителна информация. Изборът на ниво зависи от класификацията на данните и изискванията на организационната политика.

Ниво 1: Clear (Логическо изтриване)

Приложимост: Данни с нисък и среден клас на чувствителност. Носителят остава в рамките на организацията.

№	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	[ ]

Инструменти:

- Windows: cipher /w:D:\
- Linux: shred -vfz -n 3 /dev/sdb
- DBAN: Стартиране от bootable носител

Ниво 2: Purge (Криптографско изтриване)

Приложимост: Данни с висок клас на чувствителност. Носителят напуска контрола на организацията (препродажба, връщане по гаранция).

№	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	Прочитане на целия носител, потвърждаване на липса на възстановими данни	[ ]
2.5	Документиране: сертификат за изтриване с подпис	[ ]

Изпълнението на Secure Erase се случва по следните начини:

- NVMe: nvme format /dev/nvme0n1 --ses=1
- SATA SSD: hdparm --security-erase NULL /dev/sda
- HDD: Презаписване в 3+ паса (DoD 5220.22-M)
- Криптирани устройства: Унищожаване на ключа

Ниво 3: Destroy (Физическо унищожаване)

Приложимост: Данни с най-висок клас на чувствителност (класифицирана информация, лични данни по GDPR). Единственият метод, гарантиращ 100% невъзможност за възстановяване.

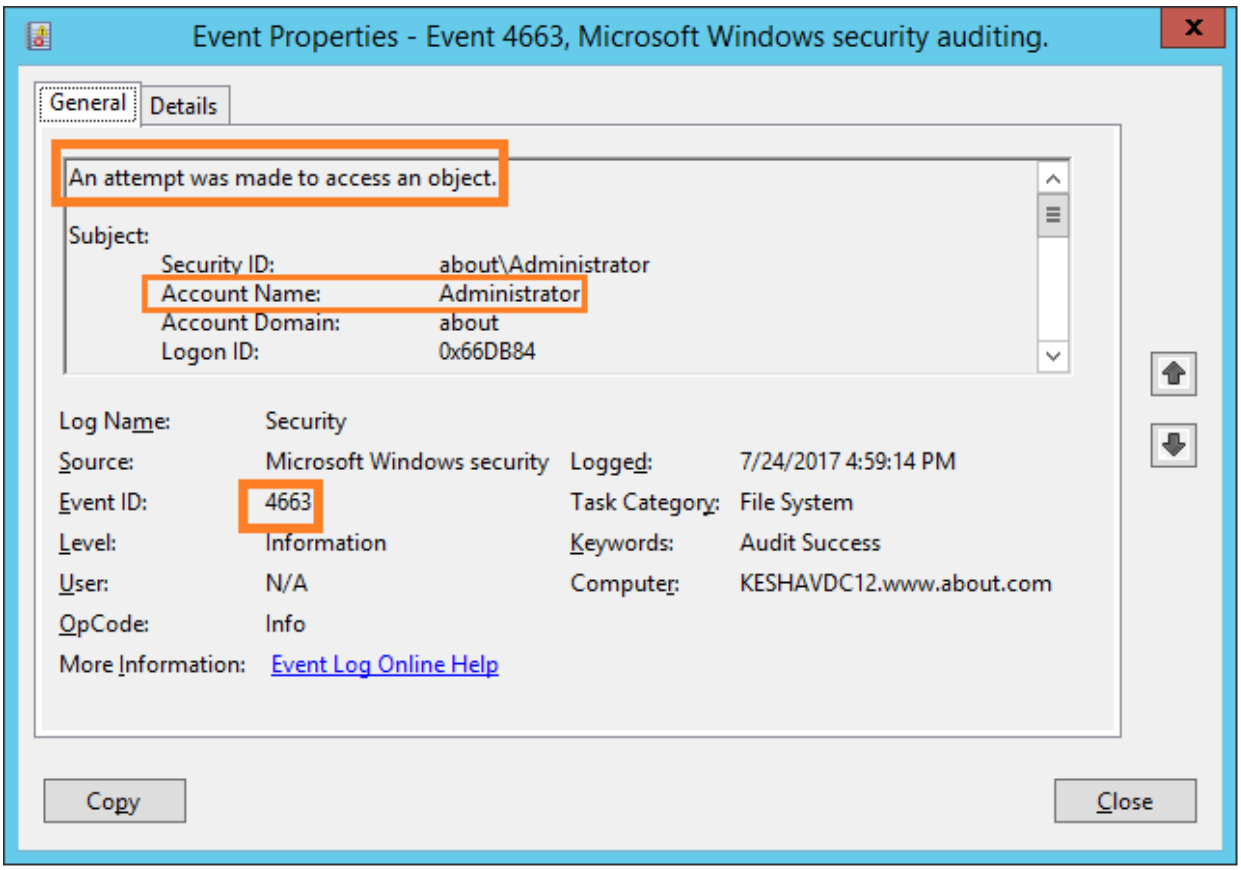
№	Стъпка	Изпълнено
3.1	Идентифициране на устройството (VID/PID/сериен номер)	[ ]
3.2	Избор на метод за физическо унищожаване	[ ]
3.3	Извършване на унищожаването от оторизиран персонал	[ ]
3.4	Визуална верификация - устройството е физически неразпознаваемо и неработоспособно	[ ]
3.5	Документиране чрез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

Методите за унищожаване включват:

- Шредиране (индустриален шредер, размер на частиците ≤ 2 mm за флаш памети)
- Дегаусиране (само за HDD – магнитни носители)
- Изгаряне в контролирана среда (лицензиран оператор)
- Химическо разтваряне (за NAND чипове)

Таблица за избор на ниво на изтриване:

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)



7. ЛИТЕРАТУРА

1. Apple. (2023a). I/O Kit Fundamentals. Apple Developer Documentation. https://developer.apple.com/documentation/iokit
2. Apple. (2023b). Apple File System Reference. Apple Developer Documentation. https://developer.apple.com/documentation/foundation/file_system/about_apple_file_system
3. Backblaze. (2024). Hard Drive Stats for 2023. Backblaze Blog. https://www.backblaze.com/blog/hard-drive-stats-for-2023/
4. Bez, R., Camerlenghi, E., Modelli, A., & Visconti, A. (2003). Introduction to Flash Memory. Proceedings of the IEEE, 91(4), 489–502.
5. Brewer, J. E., & Gill, M. (2008). Nonvolatile Memory Technologies with Emphasis on Flash. Wiley-IEEE Press.
6. Crozier, R. (2018). IBM bans all staff from using removable storage devices. IT News. https://www.itnews.com.au/news/ibm-bans-all-staff-from-using-removable-storage-devices-492061
7. Duplicati Team. (2023). Duplicati 2 User's Manual. https://docs.duplicati.com/
8. ENISA. (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

9. European Parliament. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.
10. Goodman, J. (2011). Memory Cards: Understanding SD, SDHC, and SDXC. Que Publishing.
11. ICO. (2018). Heathrow Airport Limited: Monetary Penalty Notice. Information Commissioner's Office. https://ico.org.uk/action-weve-taken/enforcement/heathrow-airport-limited/
12. IDRIX. (2023). VeraCrypt Documentation. https://veracrypt.fr/en/Documentation.html
13. Intel Corporation. (2023). Thunderbolt Technology Overview. Intel Corporation.
14. International Electrotechnical Commission. (2008). Quantities and units — Part 13: Information science and technology (IEC 80000-13). IEC.
15. International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Information security controls (ISO/IEC Standard No. 27002:2022).
16. ISO/IEC. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.
17. ISO/IEC. (2022b). ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks. International Organization for Standardization.
18. ISO/IEC 10149. (1995). Information technology — Data interchange on read-only 120 mm optical data discs (CD-ROM). International Organization for Standardization.
19. JEDEC. (2016). JEDEC JESD218B.01: Solid-State Drive (SSD) Requirements and Endurance Test Method. JEDEC Solid State Technology Association.
20. Kroah-Hartman, G. (2007). Linux Kernel in a Nutshell. O'Reilly Media.
21. Krogh, P. (2009). The DAM Book: Digital Asset Management for Photographers (2nd ed.). O'Reilly Media.
22. Kroll Ontrack. (2022). Data Loss Index: Annual Report 2022. Kroll Ontrack.
23. Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy, 9(3), 49–51.
24. Micheloni, R., Crippa, L., & Marelli, A. (2010). Inside NAND Flash Memories. Springer.
25. Microsoft. (2024a). Windows Hardware Quality Labs (WHQL). Microsoft Learn. https://learn.microsoft.com/en-us/windows-hardware/drivers/install/whql-release-signature
26. Microsoft. (2024b). Disk Management Overview. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/storage/disk-management/overview-of-disk-management

27. Microsoft. (2024c). Comparison of FAT32, NTFS, and exFAT. Microsoft Learn. https://learn.microsoft.com/en-us/troubleshoot/windows-client/backup-and-storage/fat-hpfs-and-ntfs-file-systems
28. Microsoft. (2024d). BitLocker Overview. Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/
29. Microsoft. (2024e). Microsoft Defender for Endpoint Device Control. Microsoft Learn. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-control-overview
30. Mueller, S. (2015). Upgrading and Repairing PCs (22nd ed.). Que Publishing.
31. NIST. (2010). NIST SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems. National Institute of Standards and Technology.
32. NIST. (2012). NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments. National Institute of Standards and Technology.
33. NIST. (2013). NIST SP 800-83 Rev. 1: Guide to Malware Incident Prevention and Handling for Desktops and Laptops. National Institute of Standards and Technology.
34. NIST. (2014). NIST SP 800-88 Rev. 1: Guidelines for Media Sanitization. National Institute of Standards and Technology.
35. NIST. (2018). NIST SP 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations. National Institute of Standards and Technology.
36. NIST. (2020). NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology.
37. NIST. (2024). NIST Cybersecurity Framework 2.0. National Institute of Standards and Technology. https://www.nist.gov/cyberframework
38. NVM Express. (2022). NVM Express Base Specification, Revision 2.0. NVM Express, Inc.
39. Paragon Software. (2021). NTFS3: New NTFS file system driver merged into Linux kernel 5.15. Paragon Software Group.
40. Pohlmann, K. C. (2005). The Compact Disc Handbook. A-R Editions.
41. Ponemon Institute. (2016). The State of USB Drive Security. Ponemon Institute Research Report.
42. Samsung Electronics. (2023). SSD White Paper: Reliability and Endurance. Samsung Semiconductor.
43. Scarfone, K., Souppaya, M., & Dadier, M. (2007). Guide to Storage Security Recommendations for Other Than System Administrators (NIST Special Publication 800-111). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-111
44. Schroeder, B., & Gibson, G. A. (2007). Disk Failures in the Real World: What Does an MTTF of 1,000,000 Hours Mean to You? Proceedings of the 5th USENIX Conference on File and Storage Technologies (FAST '07), 1–16.

45. SD Association. (2023). SD Specifications Part 1: Physical Layer Simplified Specification. SD Association.
46. Serial ATA International Organization. (2018). Serial ATA Revision 3.5a Specification. SATA-IO.
47. Statista. (2024). External Storage Devices – Market Data & Forecasts. Statista Digital Market Insights. https://www.statista.com/outlook/tmo/consumer-electronics/storage-media/
48. Tanenbaum, A. S., & Bos, H. (2015). Modern Operating Systems (4th ed.). Pearson.
49. Taylor, J., Johnson, M. R., & Crawford, C. G. (2006). DVD Demystified (3rd ed.). McGraw-Hill.
50. The Linux Kernel Documentation. (2024). USB Mass Storage driver. https://www.kernel.org/doc/html/latest/usb/mass-storage.html
51. Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016). Users Really Do Plug in USB Drives They Find. Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), 306–319.
52. Tom's Hardware. (2024). Best External SSDs 2024: Portable Drives for PC and Mac. Tom's Hardware. https://www.tomshardware.com/best-picks/best-external-ssds
53. Ts'o, T. (2010). ext4 – The Next Generation of the ext2/ext3 Filesystem. Proceedings of the Linux Symposium.
54. U.S. Department of Defense. (2006). DoD 5220.22-M: National Industrial Security Program Operating Manual. U.S. Department of Defense.
55. USB Implementers Forum. (2019). Universal Serial Bus 3.2 Specification. USB-IF.
56. USBGuard Project. (2023). USBGuard Documentation. https://usbguard.github.io/
57. Vacca, J. R. (2013). Computer and Information Security Handbook (2nd ed.). Morgan Kaufmann.
58. Verizon. (2023). 2023 Data Breach Investigations Report. Retrieved from https://www.verizon.com/business/resources/reports/dbir/
59. Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security (6th ed.). Cengage Learning.
60. Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishers.