Vysoká škola ekonomická v Praze

Šifrování systémového disku C: a datového disku D: ve standardním image

verze 001 ze dne 12.12.2018

Microsoft nabízí pro šifrování disků v systému Windows 10 nástroj BitLocker. Funguje relativně jednoduše a provozní zatížení systému je nepatrné. V rámci VŠE jsme pro Vás připravili návod, jak zašifrovat data na stanici (notebooku), která má standardní image. Při postupování pomocí tohoto návodu je při zapomenutí klíče nebo poškození hardware možné rozšifrování Helpdeskem CI. Pro šifrování je nutné být administrátorem systému a být připojen v síti VŠE, a to z důvodů, že se do sítového prostředí uloží klíč, který je nutný pro rozšifrování disku.

Před vlastním šifrováním doporučuje aktuální data zálohovat, a to buď na přenosný disk nebo přes aplikaci Microsoft OneDrive nebo do ownCloudu Cesnetu.

Přes volbu Start najdeme volbu Spravovat nástroj Bitlocker



U disku C – zapneme volbu *Zapnout nástroj BitLocker*, bude probíhat kontrola konfigurace počítače.

Nastroj BitLocker Drive Encryp	tion			
	cí panely » Všechny položky Ovládacích panelů » Nástroj BitLock	er Drive Encryption	✓ ♂ Prohledat Ovládací p	anely
Hlavní ovládací panel	Náctroi Pitlockor Drive Eponation			
	Pokud u svých jednotek použijete nástroj BitLocker, lépe ochr	áníte své soubory a složky před		
	neautorizovaným přístupem.			
	Jednotka operačního systému			
	OSDisk (C:) Nástroj BitLocker vypnut		C	9
		beker		
		×		
🐙 Nástroj BitLocker Drive Enc	ryption (C:)			
Kontrola konfigurace pr	očítače			
kontrolu koninguruce pe			0)
Mastroj BitLocker overuje, zda minut.	pocitac spinuje pozadavky na system. Tato operace muze trvat nekoli	IK		
		J USB Flash.		
laké jsou požadavky nástroje B	tLocker na systém?			

Vlastní instalace nástroje BitLocker bude provedena v několika krocích. Zde může nastat odchylka podle konfigurace počítače.

Před vlastním zašifrování je nutné aktivovat TPM čip, který bývá součástí počítačů a notebooků, vlastní aktivace TPM čipu se provede instalační utilitou sama, ale bude se vyžadovat součinnost ze strany uživatele. Na některých starších počítačích může být potřeba zapnout TPM v BIOSu (provede na požádání Helpdesk) Jednotlivé kroky popisu následující dialogové okno, kde stiskneme tlačítko *Další*

		×	
÷	Nástroj BitLocker Drive Encryption (C:)		
	Instalace nástroje BitLocker Drive Encryption		
	Při zapnutí nástroje BitLocker provede počítač následující kroky:		
	Připravit jednotku pro nástroj BitLocker		
	Zapnout zabezpečovací hardware TPM		
	Zašifrovat jednotku		
	Jaké jsou požadavky nástroje BitLocker na systém?		
	<u>D</u> alší Zrušit		

Jsme znovu varování, že je nutné data zálohovat a systém nás informuje, což že doba šifrování závisí na velikosti a obsahu jednotky.

		\times
←	Nástroj BitLocker Drive Encryption (C:)	
	Příprava jednotky pro nástroj BitLocker	
	K zapnutí nástroje BitLocker bude použita existující jednotka nebo nepřidělené volné místo na pevném disku.	
	⊘ Podrobnosti	
	Upozornění:	
	Před pokračováním je vhodné zazálohovat nepostradatelné soubory a data. Použít k zálohování službu Historie souborů	
	1 Tento proces může v závislosti na velikosti a obsahu jednotky chvíli trvat.	
	Další Zruš	it

Disk C je upraven, tak aby se na disku vytvořila část pro zavedení systému, která nesmí být šifrována, a tudíž se musí jednat o jiný oddíl než oddíl s operačním systémem. Jeho velikost je malá cca do 350 MB.

		×
~	Rev Nástroj BitLocker Drive Encryption (C:)	
	Příprava jednotky pro nástroj BitLocker	
	Počítač nevypínejte ani nerestartujte před dokončením tohoto procesu.	
	 Zmenšování jednotky C: Probíhá vytváření nové systémové jednotky Přímava jednotlovana pístna Piel pelez 	
	Stav:	
	Zrušit	
		×
÷	Rev Nástroj BitLocker Drive Encryption (C:)	
	Příprava jednotky je dokončena.	
	Instalační program nástroje BitLocker nemohl přesunout prostředí Windows Recovery Environment r novou systémovou jednotku. Toto prostředí nebude možné nadále používat, dokud nebude ručně povoleno a přesunuto na systémovou jednotku.	ia
	Pro dokončení přípravy systémové jednotky na šifrování musí nástroj BitLocker restartovat počítač.	
	Restartovat <u>n</u> yn	í

Po restartu by průvodce sám měl naběhnout do dialogového okna *Nástoj BitLocker Drive Encryption (C:)* Stiskneme tlačítko *Další*. Systém bude zapínat TPM čip, a tak opět musíme restartovat.

Nástroj BitLocker Drive Encryption (C:) \leftarrow

Z	apnout zabezpečovací hardware TPM
	Před zapnutím hardwaru TPM pro tento počítač vyjměte všechny disky CD, DVD nebo jednotky USB Flash a restartujte počítač.
	Po restartování počítače postupujte podle pokynů k zapnutí čipu TPM.

Coj	e čip TPM?			
			<u>R</u> estartovat	Zrušit

Je pravděpodobné, že pro vlastní aktivaci TPM čipu, budete muset být součinni. Např. na Allin-One od HP je nutná akceptace přes klávesu F1.

Tpm Ppi	hp
A configuration change was requested to enable, activate, and allow a user to take ownership of this computer's TPM (Trusted Platform Module)	
NOTE: This action will turn on the TPM	
Press F1 = Accept	

Opět se vrátím do průvodce, kde jsme splnili dva z požadovaných bodů a můžeme přistoupit na vlastní šifrování jednotky. Pokračujeme volbou Další.

 \times

		×	
÷	🎭 Nástroj BitLocker Drive Encryption (C:)		
	Instalaça pástraia Bitl askar Driva Franchian		
	Instalace hastroje Billocker Drive Encryption		
	Při zapnutí nástroje BitLocker provede počítač následující kroky:		
	✓ Připravit jednotku pro nástroj BitLocker		
	Zapnout zabezpečovací hardware TPM		
	Zašifrovat jednotku		
	Jaké jsou požadavky nástroje BitLocker na systém?		
	alší Zrušit		

Při šifrování jsme dotázáni na režim šifrování. Od verze Windows 10 volíme nový šifrovací algoritmus XTS-AES

		\times
÷	Nástroj BitLocker Drive Encryption (C:)	
	Zvolte požadovaný režim šifrování.	
	Windows 10 (verze 1511) zavádí nový režim šifrování disku (XTS-AES). Tento režim poskytuje dodatečnou podporu pro integritu, ale není kompatibilní se staršími verzemi Windows.	
	Pokud jde o vyměnitelnou jednotku, kterou budete chtít použít ve starší verzi Windows, měli byste zvolit režim kompatibility.	
	Pokud jde o pevnou jednotku nebo pokud budete tuto jednotku používat jenom v zařízeních minimálně s Windows 10 (verze 1511) nebo novějším vydáním, měli byste zvolit nový režim šifrování	
	Nový režim šifrování (nejlepší pro pevné disky v tomto zařízení)	
	<u>R</u> ežim kompatibility (nejlepší pro disky, které se můžou přemisťovat mimo toto zařízení)	
	Další Zrušit	

V posledním kroku můžeme zvolit, aby se provedla systémová kontrola (testuje se práce s klíči v TPM a další), jinak se hned spustí šifrování disku a při nějakých komplikacích ho již nemusíme rozšifrovat.

		×
÷	Nástroj BitLocker Drive Encryption (C:)	
	Jste připraveni zašifrovat tuto jednotku?	
	Šifrování může v závislosti na velikosti jednotky chvíli trvat.	
	Během šifrování jednotky můžete pokračovat v práci, avšak počítač bude pravděpodobně pracovat pomaleji.	
	✓ Spustit kontrolu systému nástroje BitLocker	
	Tato kontrola systému zaručí, že bude moci nástroj BitLocker před zašifrováním jednotky správně přečíst obnovovací a šifrovací klíč.	
	Nástroj BitLocker před šifrováním restartuje počítač.	
	Poznámka: Tato kontrola může chvíli trvat, ale je doporučena, aby bylo zajištěno, že bude vybraná metoda odemykání fungovat, aniž by bylo nutné zadávat obnovovací klíč.	
	Pokračovat Zrušit	:
Po۱	volbě Pokračovat, se dopracujeme k Restartu počítače.	
Ą	Nástroj BitLocker Drive Encryption	
6	Počítač je nutné restartovat.	

<u>Spravovat nástroj BitLocker</u> Tímto se zašifruje disk C, informace o šifrovacím klíči se uloží do TPM čipu a do objektu počítač v Active Directory.

Restartovat později

Restartovat nyní

Abychom zašifrovali i úložiště dokumentů – potřebujeme zašifrovat i disk D. Znovu tedy musíme zavolat nástroj Bitlockeru. Poté, co se nám zobrazí utilita, uvidíme, že disk C je již zašifrován (je totiž dostupná volba *Vypnout nástroj BitLocker*), zatímco u disku D máme volbu *Zapnout nástroj Bitlocker*, kterou není zavoláme.

Ą	Nástroj BitLocker Drive Encryption			- 0	×
÷	$ ightarrow ~ \uparrow i i i i i i i i i i i i i i i i i i$	nely 🔸 Všechny položky Ovládacích panelů 🔸 Nástroj BitLocker Drive Encryption	~ Ö	Prohledat Ovládací panely	Q,
	Hlavní ovládací panel	Nástroj BitLocker Drive Encryption			?
		Pokud u svých jednotek použijete nástroj BitLocker, lépe ochráníte své soubory a složky před neautorizovaným přístupem.			
		Pro vaši bezpečnost některá nastavení spravuje správce systému.			
		Jednotka operačního systému			
		OSDisk (C:) Nástroj BitLocker provádí šifrování.		\bigcirc	
		Zálohovat obnovovací klíč Vypnout nástroj BitLocker			
		Pevné datové jednotky			
		Data (D:) Nástroj BitLocker vypnut			
		Sapnout nástroj BitLocker			
	Viz také	Vyměnitelné datové jednotky – Bitl ocker. To Go			
•	Správa čipu TPM	Chcete-li použít nástroj BitLocker To Go, vložte vyměnitelnou jednotku USB Flash.			
4	Sprava disku Probláčení o zásadách ochrany				
	osobních údajů				

Objeví se okno, v kterém jsou omezené možnosti (nastavené správcem systému). Jedinou dostupnou volbou je nyní volba *Automaticky odemykat tuto jednotku v tomto počítači*. Zaškrtnete-li tuto volbu, pak se objeví tlačítko *Další* v průvodci

		×
\leftarrow	🏘 Nástroj BitLocker Drive Encryption (D:)	
	-	
	Zvolte, jak chcete odemknout tuto jednotku.	
	 Některá nastavení jsou spravována správcem systému. 	
	Odemknout jednotku pomocí <u>h</u> esla	
	Hesla by měla obsahovat malá a velká písmena, číslice, mezery a symboly.	
	<u>Z</u> adejte své heslo.	
	Zadejte heslo znovu.	
	Odemknout jednotku pomocí či <u>p</u> ové karty	
	Je nutné vložit čipovou kartu. Při odemykání jednotky bude požadován PIN kód čipové karty.	
	Automaticky odemykat tuto jednotku v tomto počítači	
	<u>D</u> alší Zrušit	t

Volíme opět režim šifrování pro disk D.

A Stroj BitLocker Drive Encryption (D:)

Zvolte požadovaný režim šifrování.

Windows 10 (verze 1511) zavádí nový režim šifrování disku (XTS-AES). Tento režim poskytuje dodatečnou podporu pro integritu, ale není kompatibilní se staršími verzemi Windows.

Pokud jde o vyměnitelnou jednotku, kterou budete chtít použít ve starší verzi Windows, měli byste zvolit režim kompatibility.

Pokud jde o pevnou jednotku nebo pokud budete tuto jednotku používat jenom v zařízeních minimálně s Windows 10 (verze 1511) nebo novějším vydáním, měli byste zvolit nový režim šifrování

Nový režim šifrování (nejlepší pro pevné disky v tomto zařízení)

O Režim kompatibility (nejlepší pro disky, které se můžou přemisťovat mimo toto zařízení)

|--|

Tlačítkem Zahájit šifrování v následujícím okně zahájíme šifrování disku D.

÷	Nástroj BitLocker Drive Encryption (D:)		×
	Jste připraveni zašifrovat tuto jednotku?		
	Jednotka se v tomto počítači automaticky odemkne.		
	Šifrování může v závislosti na velikosti jednotky chvíli trvat.		
	Soubory budou chráněny až po dokončení šifrování.		
		Za <u>h</u> ájit šifrování	Zrušit

O dokončení šifrování jste informování následujícím dialogovým oknem.



Pokud zavoláte opětovně *Nástroj pro BitLocker*, uvidíte, že zašifrovány jsou oba disky.

🏘 Nástroj BitLocker Drive Encrypti	on			>
$\leftarrow \ ightarrow \ $	Prohledat Ovládací panely			
Hlavní ovládací panel	Nástroj BitLocker Drive Encryption			
	Pokud u svých jednotek použijete nástroj BitLo neautorizovaným přístupem.	ocker, lépe ochráníte své soubory a složky před		
	Pro vaši bezpečnost některá nastavení sp	ravuje správce systému.		
	Jednotka operačního systému			
	OSDisk (C:) Nástroj BitLocker zapi	nut		\bigcirc
		 Pozastavit ochranu Zálohovat obnovovací klíč Vypnout nástroj BitLocker 		
	Pevné datové jednotky			
	Data (D:) Nástroj BitLocker zapnut			\bigcirc
Viztalzé		 Zálohovat obnovovací klíč Vypnout automatické odemknutí Vypnout nástroj BitLocker 		
Správa čipu TPM				
💔 Správa disků	Vyměnitelné datové jednotky – Bitl	ocker To Go		
Prohlášení o zásadách ochrany osobních údajů	Chcete-li použít nástroj BitLocker To Go, vle	ožte vyměnitelnou jednotku USB Flash.		

Doporučujeme na počítač vhodným způsobem poznamenat jméno počítače (popis ikonky počítače na ploše ve formátu "Počítač VSE-xxxx", kde xxxxx je pětimístné číslo). Tento údaj je třeba v případě poškození počítače pro rozšifrování disku mimo původní počítač. Bez znalosti jména může být obtížné nalezení správného dešifrovacího klíče v AD.

 \times