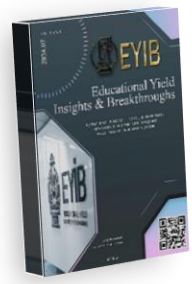
EYIB
EDUCATIONAL YIELD INSIGHTS & BREAKTHROUGHS
TA'LIMGA OID TUSHUNCHALAR VA YUTUQLAR
ISSN:3060-4648
Vol.6 №2
https://eyib.uz



USB qurilmalarida mavjud axborot xavfsizligi usul va vositalari tahlili

Qaxramonov Elbek Quvondiq o‘g‘li

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, axborot xavfsizligi kafedrasi katta o‘qituvchisi
eljon.mail@gmail.com

Annotatsiya

ushbu maqolada USB qurilmalar xavfsizligini ta’minlash uchunishlab chiqilgan va foydalanilayotgan dasturiy vositalar, ularning turlari tahlil etilgan. Windows operatsion tizimlarida qo‘llanilishi mumkin bo‘lgan eng yaxshi vositalar, ularning afzallik va kamchiliklari ko‘rib chiqilib samarali yechimlar taklif etilgan.

Kalit so‘zlar: BitLocker, VeraCrypt, USB Disk Security, Endpoint Protector, GiliSoft USB Encryption, Windows, Linux, shifrlash, USB.

Bugungi kunda USB qurilmalar xavfsizligini ta’minlash uchun ko‘plab dasturiy vositalar mavjud. Ular orasida eng mashhurlari quyidagilar:

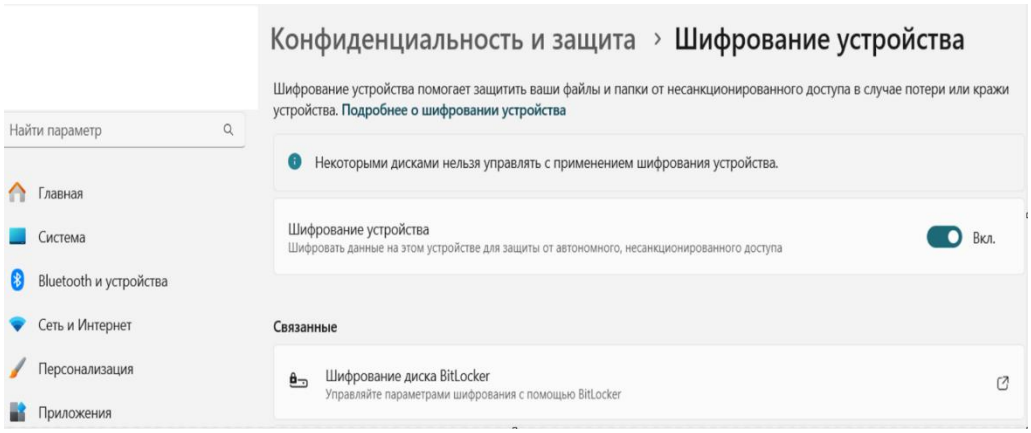
- BitLocker (Windows OS tomonidan taqdim etilgan);
- VeraCrypt (ochiq manbali shifrlash vositasi);
- USB Disk Security (maxsus antivirus va monitoring vositasi);
- Endpoint Protector (korporativ nazorat vositasi);
- GiliSoft USB Encryption (shaxsiy ma’lumotlarni himoyalash uchun).

1-rasm. USB qurilmalarini himoyalash dasturiy vositalari

Ushbu dasturlarni tahlil qilishda quyidagi mezonlarga e’tibor beramiz: foydalanish qulayligi, xavfsizlik darajasi, ishlash tezligi, moslashuvchanlik va narxi

BitLocker. BitLocker — bu Microsoft tomonidan Windows operatsion tizimiga o‘rnatilgan diskni to‘liq shifrlash (full disk encryption) vositasidir. Foydalanuvchi yoki tizim tomonidan belgilangan parol yoki TPM (Trusted Platform Module) yordamida diskni shifrlaydi. Disk o‘g‘irlanganda yoki yo‘qotilganda ma’lumotlar o‘qilmasligini kafolatlaydi. Ushbu vosita operatsion tizimda operatsion tizim disklari va tashqi USB qurilmalarni shifrlashi mumkin.

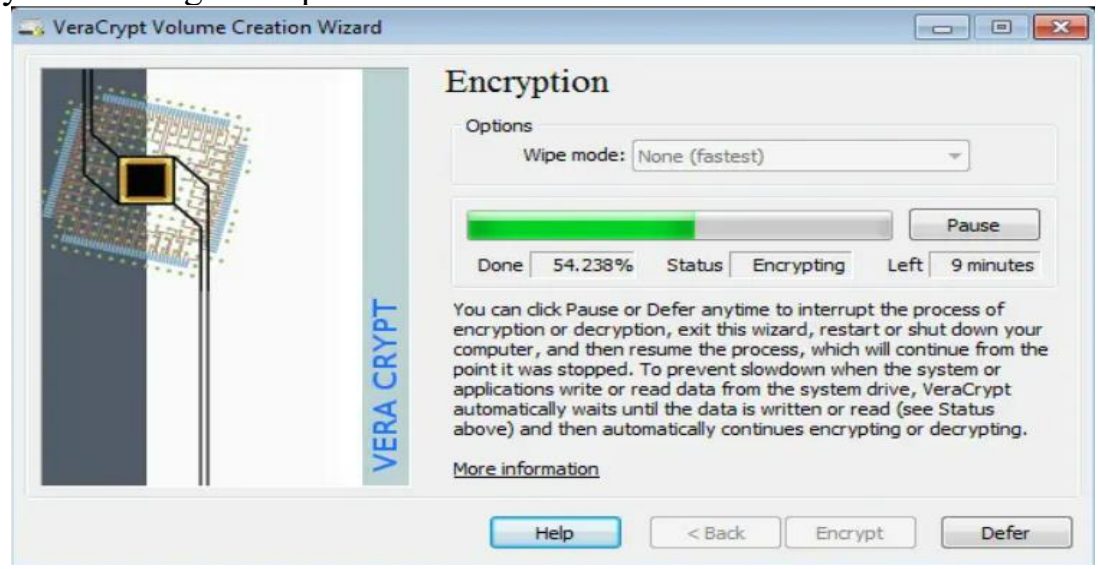
Afzalliklari: Windows bilan integratsiyalashgan, avtomatik tarzda ishga tushadi, foydalanish oson.



2-rasm. Windows operatsion tizimidagi Bitlocker himoya tizimi

VeraCrypt. VeraCrypt — bu ochiq manbali va bepul disk shifrlash dasturi, sobiq TrueCrypt loyihasining davomchisi. Disk bo‘limlarini, butun disklarni va USB qurilmalarni shifrlaydi. Yashirin hajm (hidden volume) va yashirin operatsion tizim yaratish imkoniyati mavjud. AES, Serpent, va Twofish algoritmlarini qo‘llab-quvvatlaydi.

Afzalliklari: xavfsizlik darajasi juda yuqori, ko‘p platformali: Windows, macOS, Linux, foydalanuvchiga to‘liq nazorat beradi.



3-rasm. VeraCrypt dasturi yordamida diskni shifrlash

Uning imkoniyatlari quyidagilar:

- virtual shifrlangan disk yaratadi va uni haqiqiy disk sifatida o‘rnatadi;

- USB yoki qattiq disk kabi butun bo‘lim yoki saqlash qurilmasini shifrlaydi;
- Windows o‘rnatilgan bo‘lim yoki diskni shifrlaydi;
- shifrlash avtomatik, real vaqtda (tezkor) va shaffofdir;
- parallelizatsiya va konveyerlash ma’lumotlarni xuddi disk shifrlanmaganidek bir xil tezlikda o‘qish va yozish imkonini beradi;
- shifrlash zamonaviy protsessorlarda tezlashtirilgan apparat bo'lishi mumkin.
- agar tajovuzkor parolni ochishga majbur qilsa, bu ishonchli rad etishni ta'minlaydi: ya’ni yashirin tovush (steganografiya) va yashirin operatsion tizim.

USB Disk Security. USB Disk Security — bu USB qurilmalar orqali keladigan viruslarga qarshi antivirus himoya vositasi. USB portlarga ulangan qurilmalardagi zararli fayllarni avtomatik aniqlaydi. Offline rejimda ham ishlaydi. Yashirin fayllar va avtomatik ishga tushuvchi (autorun) fayllarni bloklaydi.

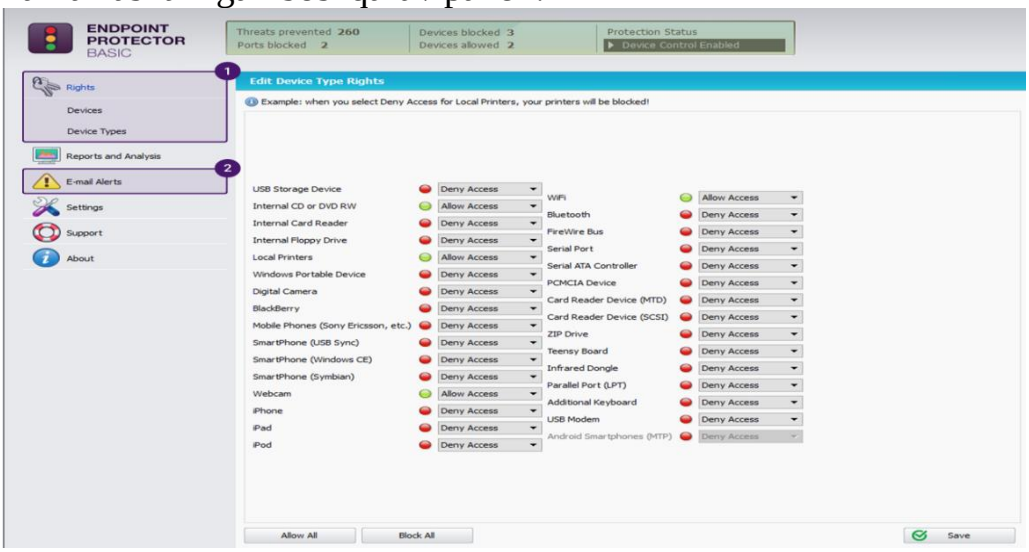
Afzalliklari: Tez va yengil, interfeysi oddiy, USB portni bloklash imkoniyati bor.

4-rasm. USB disk Security dasturining interfeysi

USB disk security dasturi o‘rnatilgandan so‘ng, dastur o‘zini dasturiy ta’minotning avtomatik ishga tushirish ro‘yxatiga qo‘shadi, shunda u har safar Windows qurilmangizni yuklaganingizda yuklanadi. Shuningdek, siz Windows Task Scheduler dasturiga USB Disk xavfsizligini qo‘shishingiz mumkin, shunda dastur kun davomida muntazam ravishda ishlaydi.

Endpoint Protector. Endpoint Protector — bu korxona darajasidagi ma’lumotlar xavfsizligi yechimi bo‘lib, Data Loss Prevention (DLP) va USB nazoratini ta’minlaydi. USB portlar va boshqa tashqi qurilmalarning ishlashini nazorat qiladi. Maxfiy ma’lumotlarni oqib ketishidan himoya qiladi. Ko‘plab operatsion tizimlar bilan mos (Windows, macOS, Linux).

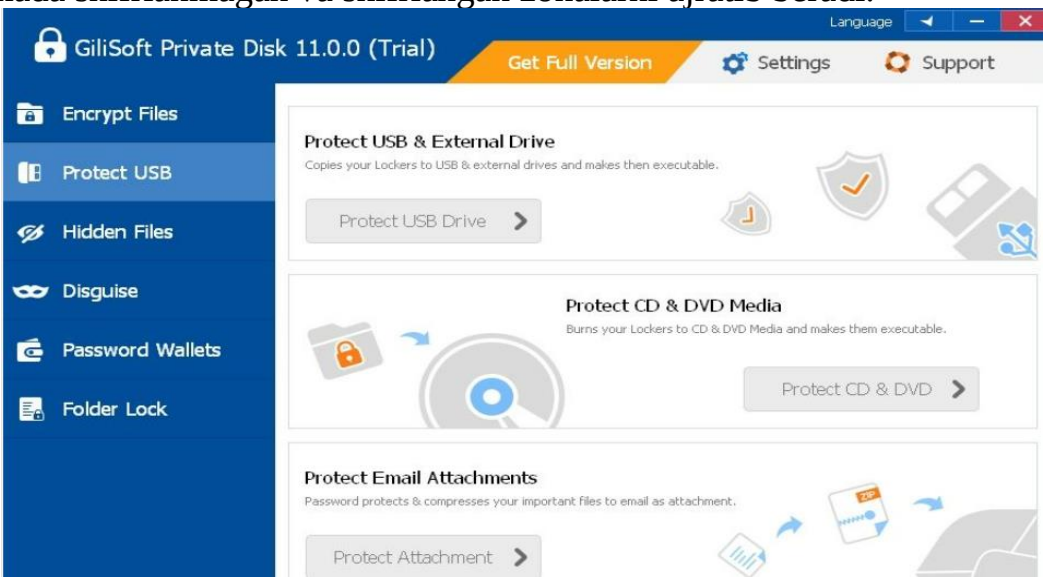
Afzalliklari: Korxona darajasida kuchli nazorat, real vaqtda monitoring va hisobotlar, markazlashtirilgan boshqaruv paneli.



5-rasm. Endpoint detector dasturining ishchi oynasi

GiliSoft USB Encryption. GiliSoft USB Encryption — bu USB fleshka qurilmalarini va tashqi drayvlarni kriptografik shifrlashga mo‘ljallangan dastur hisobalandi. USB fleshka ichida shifrlangan zonani yaratadi. Parol bilan himoyalash funksiyasi mavjud. FAT, FAT32 va NTFS fayl tizimlarini qo‘llab-quvvatlaydi.

Afzalliklari: O‘rnatish va ishlatish juda oson, foydalanuvchi interfeysi qulay, USB qurilmada shifrlanmagan va shifrlangan zonalarni ajratib beradi.



6-rasm. GiliSoft USB Encryption dasturining ishchi oynasi

Ushbu dasturdan foydalanishda agar foydalanuvchi xohlasa, olinadigan vositaning butun xotirasini yoki shunchaki kerakli maydonni shifrlash imkoniyati mavjud, ya’ni oddiy ma’lumotlarni ham, diskdagi begona ko‘zlardan shifrlanishi kerak bo‘lgan ma’lumotlarni ham saqlashimiz mumkin. Bo‘limga kirishni ochish uchun diskda saqlanadigan "Agent" dasturini ishga tushirish va parolni kiriting kerak xolos.

Demak, yuqorida keltirilgan USB qurilmalarining xavfsizligini ta;minlash uchun ishlatiladigan dasturiy vositalarning tahlillari amalga oshirdik va bundan quyidagi xulosalarni aytish mumkin:

BitLocker – Windows foydalanuvchilari uchun qulay va tizimga integratsiyalashgan shifrlash yechimi mavjud bo‘lgan dasturiy vosita;

VeraCrypt – yuqori darajadagi xavfsizlikka ega, professional foydalanuvchilar uchun mos bo‘lgan bepul dasturiy vosita;

USB Disk Security – bu USB qurilmalardagi mavjud bo‘lgan zararli dasturlar va viruslarni aniqlaydigan va ulardan himoya qilishga ixtisoslashgan dasturiy vosita;

Endpoint Protector – korxona va tashkilotlar uchun ma’lumotlar xavfsizligi va kompleks nazorat tizimini amalga oshirishni ta’minlovchi dasturiy vosita;

GiliSoft USB Encryption – oddiy foydalanuvchilar uchun tezkor USB shifrlash dasturiy vositasi.

1-jadval

USB qurilmalar xavfsizligini ta’minlaydigan dasturiy vositalar tahlili

Dastur nomi	**Xavfsizlik darajasi**	**Foydalanish qulayligi**	**Tezligi**	**Moslashuvchanlik**	**Narx**
BitLocker	Yuqori	O‘rtacha	Yuqori	Windowsga mos	Bepul
VeraCrypt	Juda yuqori	Murakkab	O‘rtacha	Keng	Bepul
USB Disk Security	O‘rta	Yuqori	Yuqori	Cheklangan	Pullik
Endpoint Protector	Yuqori	Yuqori	O‘rtacha	Keng	Pullik
GiliSoft USB Encryption	Yuqori	O‘rtacha	Yuqori	Windowsga mos	Pullik

Yuqoridagi tahlilga ko‘ra, quyidagicha xulosalarga kelish mumkin, ya’ni, VeraCrypt USB flash disklarni shifrlash dasturi xavfsizlik darajasi eng yuqori bo‘lgan dastur hisoblanadi, ammo undan foydalanish nisbatan murakkab. BitLocker esa foydalanuvchi uchun qulay va tez ishlaydi.

Tahlillar natijasiga ko‘ra USB qurilmalaridan foydalanish va ularning xavfsizligini oshirish bo‘yicha quyidagi takliflarga amal qilish tavsiya etiladi:

- korxona va tashkilotlarda USB qurilmalardan foydalanish bo‘yicha siyosatni ishlab chiqish;
- foydalanuvchilarni axborot xavfsizligi bo‘yicha muntazam o‘qitish va ogohlantirish;
- faqat ishonchli va sertifikatlangan USB qurilmalardan foydalanish;
- USB portlarga cheklovlar o‘rnatish yoki monitoringlash vositalarini joriy qilish;
- ma’lumotlarni doimiy ravishda zaxira nusxasini olish va USB qurilmalarini shifrlash tizimlaridan muntazam foydalanish.

Yuqoridagi choralar amalga oshirilganda, USB qurilmalari orqali axborot xavfsizligiga tahdidlar sezilarli darajada kamayadi va axborot resurslarining himoyasi ta’minlanadi.

Foydalanilgan adabiyotlar ro‘yxati

G‘aniyev S. K., Karimov M. M., Tashev K. A. Axborot xavfsizligi. Talabalar uchun darslik. Toshkent, 2016.

Eshonqulov Sh.U., Qarshiboyev N.A “Axborot xavfsizligi” o‘quv qo‘llanma, Jizzax-2022.

Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. Изд. 4-е-М: Ленанд, 2015.

S.K. G‘aniyev, T.A. Qo‘chqorov Axborot xavfsizligining maxsus vositalari. Ma’ruzalar matni. TATU 2013.

Stamp, Mark. Information security: principles and practice / Mark Stamp/ -2nd ed. ISBN 978-0-4-470-62639-9(hardback)/ QA76.9.A25S69, USA, 2011.

Hacking exposed. Web Applications 3. Joel Scambray, Vincent Liu, Caleb Sima. 2010 y.

https://hetmanrecovery.com/ru/recovery_news/backup-and-recovery-in-windows-10.htm.