

Integral – Оборудование для защиты информации.

USB флэш-накопители и SSD диски с аппаратным шифрованием данных.

Защита информации, хранящейся на SSD и USB флэш-накопителях является одной из важнейших задач для ИТ- подразделений всех государственных органов и коммерческих предприятий. Integral производит ряд SSD и USB флэш-накопителей с AES 256-битным аппаратным шифрованием хранимой на них информации, которые являются простым в использовании и экономически эффективным решением, обеспечивающим безопасность ваших данных.

Все наши устройства Crypto модельного ряда сертифицированы на соответствие стандартам FIPS 140-2 / 197. Они не требуют установки какого-либо дополнительного программного обеспечения и не оставляют никаких следов в операционной системе. Все данные при записи на накопитель зашифровываются автоматически и защищаются паролем. Если накопитель потерян или украден и делаются попытки подобрать пароль, данные, хранящиеся на накопителе автоматически уничтожаются.

Crypto накопители пользуются доверием и применяются правительствами, государственными учреждениями всего мира, глобальными корпорациями а так же средним и малым бизнесом.



Обязательное 256-bit аппаратное шифрование данных



Совместима с Endpoint Protection системами



Простые в использовании



Производительнее и надежнее систем программного шифрования

USB FLASH DRIVE “CRYPTO” TOTAL LOCK С СЕРТИФИКАЦИЕЙ ПО FIPS 197

MFR PART NO	ITEM NAME
INFD2GCRYPTO197	2GB CRYPTO AES FIPS 197
INFD4GCRYPTO197	4GB CRYPTO AES FIPS 197
INFD8GCRYPTO197	8GB CRYPTO AES FIPS 197
INFD16GCRYPTO197	16GB CRYPTO AES FIPS 197
INFD32GCRYPTO197	32GB CRYPTO AES FIPS 197



USB FLASH DRIVE “CRYPTO” TOTAL LOCK С СЕРТИФИКАЦИЕЙ ПО FIPS 140-2

MFR PART NO	ITEM NAME
INFD2GCRYPTO140-2	2GB CRYPTO AES FIPS 140-2
INFD4GCRYPTO140-2	4GB CRYPTO AES FIPS 140-2
INFD8GCRYPTO140-2	8GB CRYPTO AES FIPS 140-2
INFD16GCRYPTO140-2	16GB CRYPTO AES FIPS 140-2
INFD32GCRYPTO140-2	32GB CRYPTO AES FIPS 140-2



Crypto SSD (2.5" SATA III) и Crypto mSATA SSD накопители.

Integral Crypto твердотельные накопители – это комплексное решение защиты, которое сочетает в себе защищенность AES 256-битного аппаратного шифрования со скоростью и надежностью SSD твердотельных накопителей. Crypto SSD накопители используют систему аутентификации, которая не зависит от BIOS компьютерной системы (Встроенная аппаратная аутентификация). Простое в использовании устройство для обязательного шифрования всех без исключения записываемых данных.

Использованием твердотельных Crypto накопителей экономически очень выгодно (значительно уменьшается TCO):

- Никаких дополнительных расходов после покупки. Отсутствует лицензионная плата, подписки или контракты, требующие периодическую оплату, как в случае с программным обеспечением.
- Отсутствие дополнительных текущих расходы на поддержку
- Повышение производительности – аппаратная шифрование происходит быстрее, чем шифрования посредством программного обеспечения, и твердотельные накопители быстрее по сравнению с традиционными жесткими дисками
- Пониженное энергопотребление.

SATA -III SSD НАКОПИТЕЛИ С 256-БИТ AES ШИФРОВАНИЕМ, СЕРТИФИЦИРОВАННЫЕ ПО FIPS 197

MFR PART NO	ITEM NAME
INSSD64GS625M7CR197	64GB SSD 2.5" SATA III 7mm
INSSD128GS625M7CR197	128GB SSD 2.5" SATA III 7mm
INSSD256GS625M7CR197	256GB SSD 2.5" SATA III 7mm
INSSD512GS625M7CR197	512GB SSD 2.5" SATA III 7mm



mSATA SSD НАКОПИТЕЛИ С 256-БИТ AES ШИФРОВАНИЕМ, СЕРТИФИЦИРОВАННЫЕ ПО FIPS 197

MFR PART NO	ITEM NAME
INSSD64GMSA6MCR197	64GB mSATA 6Gbps SATA III
INSSD128GMSA6MCR197	128GB mSATA 6Gbps SATA III
INSSD256GMSA6MCR197	256GB mSATA 6Gbps SATA III



Почему стоит отдать предпочтение устройствам с аппаратным шифрованием по сравнению с программными шифрованием?

Основное различие между аппаратным шифрованием и шифрованием при помощи программного обеспечения является то, что при аппаратном шифровании, шифрование и дешифрование осуществляется специализированным процессором (который является частью устройства аппаратного шифрования Integral). При использовании программного обеспечения, для шифрования и дешифрования данных используются ресурсы устройства, на котором установлено программное обеспечение. Это делает аппаратное шифрование гораздо более быстрым.

Другим значительным преимуществом аппаратного шифрования является то, что криптографический ключ хранится в отдельном защищенном и недоступном для чтения отделе памяти, что делает аппаратное шифрование гораздо более безопасным, чем шифрование при помощи программного обеспечения.