FLEXXON X-PHY — НОВЫЙ SSD С ИНТЕЛЛЕКТУАЛЬНОЙ ЗАЩИТОЙ

ВЛАДИМИР РЕНТЮК
Rvk.modul@gmail.com
МИХАИЛ РУСКО
rusko@sp-el.ru

Устройства хранения данных, используемые в промышленных компьютерах для критически важных приложений, должны отличаться высокими емкостью памяти, быстродействием и надежностью. При этом таким устройствам необходимо не только выдерживать воздействие неблагоприятных факторов окружающей среды, но и гарантировать безопасность хранения данных. Перечисленными свойствами обладают представленные в этом году компанией Flexxon твердотельные накопители (Solid State Drive, SSD) X-PHY индустриального класса.

ВВЕДЕНИЕ: ЧТО ТАКОЕ ФЛЭШ-ПАМЯТЬ

Устройства хранения информации, или, как мы их называем, память, лежат в основе электронных устройств и систем, которые мы используем каждый день. Практически вся бытовая электроника, средства связи, вычислительные, автомобильные и медицинские устройства требуют определенных типов памяти для хранения программного кода, параметрических данных и текущей информации. По мере развития устройства хранения информации эволюционировали от механических, механоэлектронных, магнитных и оптических до чисто электронных, последней разновидностью которых является флэш-память (англ. flash memory). Выполненные на основе такой памяти SSD стали естественным выбором для индустриальных компьютеров в качестве замены более «нежных» HDD, поскольку механика последних просто изначально не предназначена для работы в жестких условиях среды эксплуатации.

Формально флэш-память была изобретена и представлена в 1984 г. инженером компании Toshiba Фудзио Масуокой (Fujio Masuoka). Название «флэш» также было придумано в Toshiba: оно было выбрано потому, что процесс стирания содержимого памяти был настолько быстрым, что напоминал вспышку фотоаппарата (англ. flash) [1].

Флэш-память — разновидность полупроводниковой технологии электрически перепрограммируемой памяти с длительным хранением информации без внешнего источника энергии. Основной структурой ячеек NAND-флэш является МОП-транзистор с плавающим затвором (Floating Gate Transistor), два варианта исполнения которого представлены на рис. 1 [2].

Для программирования ячейки напряжение подается на управляющий затвор, что притягивает электроны вверх. Создается электрическое поле, позволяющее электронам проникнуть сквозь барьер из оксида к плавающему затвору. Оксид играет роль изолятора, не позволяя электронам двигаться дальше сквозь плавающий затвор. Этот заряд, в случае если это многоуровневая MLC-ячейка (Multi-Level Cell), представляет собой двоичное значение, например 00, 01, 10 или 11. Наличие изоляции также означает, что заряд останется на месте и после отключения питания от SSD, поэтому такая память является энергонезависимой. Для стирания ячейки напряжение подается с другой стороны — на канал. При этом управляющий затвор заземляется, чтобы направить электроны от плавающего затвора через оксид обратно к каналу. Однако этот процесс постепенно повреждает ячейку, поэтому у всех без исключения ячеек NAND-флэш-памяти ограниченный срок службы, который зависит еще и от температуры.

В зависимости от исполнения и подключения МОП-транзисторов различаются два варианта флэш-памяти — NOR и NAND, которые были названы по ассоциации с логическими элементами цифровой логики «ИЛИ-НЕ» (NOR) и «И-НЕ» (NAND). Решение NOR использует классическую двумерную матрицу проводников, в которой на пересечении строк и столбцов установлено по одной ячейке. При этом проводник строк подключается к стоку транзистора, а столбцов — ко вто-

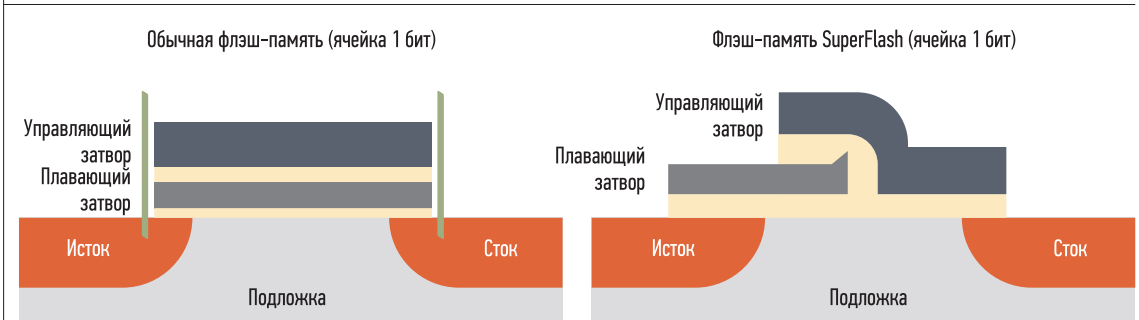

РИС. 1. ▶ Транзисторы с плавающим затвором обычного исполнения и технологии SuperFlash

рому затвору. Исток подключается к общей подложке. Конструкция NAND — это трехмерный массив. В основе та же матрица, что и в NOR, но вместо одного транзистора в каждом пересечении устанавливается столбец из последовательно включенных ячеек. Технология NOR позволяет получить быстрый доступ индивидуально к каждой ячейке, однако площадь ячейки велика. NAND, напротив, имеют малую площадь ячейки, но относительно длительный доступ сразу к большой группе ячеек. Интерфейс ввода-вывода устройства флэш-памяти NAND, в отличие от NOR-флэш, значительно сложнее и меняется не только от устройства к устройству, но и от разработчика к разработчику.

Первые ячейки флэш-памяти были однобитовые, сейчас они эволюционировали в одноуровневые ячейки (single-level cell, SLC) NAND, но производители, работающие на коммерческом рынке, отдают предпочтение многобитовым трехуровневым ячейкам (triple-level cell, TLC) NAND, которые обеспечивают более высокие плотность и емкость микросхем памяти.

Основное различие между SLC и 3D TLC — количество битов, хранящихся в каждой NAND-ячейке. SLC хранит 1 бит данных на одну ячейку NAND, а 3D TLC — 3 бита. Это позволяет SLC быть более отказоустойчивым, чем 3D TLC, не говоря уже о недавно вышедшей на рынок технологии QLC (четыре бита в каждой ячейке), и, соответственно, поддерживать при этом большее количество циклов записи на ячейку. Таким образом, флэш-память технологии SLC может обеспечить более длительный срок службы и является оптимальным выбором для высокопроизводительных приложений с малым объемом хранимой информации. Другие важные различия между SLC и 3D TLC включают время чтения, записи и стирания, циклы P/E и обработку битовых ошибок [3].

Чем больше значений может принимать ячейка, тем больше информации способен хранить накопитель, но и тем выше вероятность некорректного считывания этого значения и тем больше времени требуется на коррекцию ошибок. Это стало источником проблем. Кроме того, из-за конструктивных особенностей каждая ячейка флэш-памяти может выдержать ограниченное число циклов записи. С увеличением количества бит на одну ячейку этот показатель уменьшается, что для индустриальных, а тем более критических приложений может быть просто недопустимо. Однако если для того или иного приложения в приоритете именно емкость диска и, соответственно, плотность записи данных, то предпочтение отдается технологии 3D TLC и проприетарным решениям ее наиболее эффективного использования. Как в поговорке, за каждое удовольствие нужно платить.

Еще одной важной проблемой для критических приложений является безопасность хранения данных. Имеется в виду не просто безопасность как безошибочность, о чем уже было сказано выше, а безопасность в более широком смысле, включая кибербезопасность. Это необходимо для того, чтобы в случае, если злоумышленник похитил жесткий диск, он не смог бы считать сохраненную в нем информацию. В этом направлении работает целый ряд компаний, использующих как стандартизированные, так и проприетарные технологии и решения, в том числе с использованием искусственного интеллекта (ИИ). Одной из этого ряда является компания Flexxon, которая в апреле 2021 г. официально представила твердотельный накопитель со встроенными функциями безопасности на базе искусственного интеллекта — X-PHY AI Embedded Cyber Secure SSD [4].

О КОМПАНИИ

Flexxon — это ведущий бренд в области разработки, производства и поставок промышленных устройств флэш-памяти и памяти типа NAND из Сингапура. Основной упор компания делает на предоставлении первоклассных решений для хранения данных, обеспечивающих высокий уровень безопасности. Для выполнения этой задачи компания ведет собственные исследования и уже разработала ряд универсальных решений, которые адаптированы к разным секторам рынка: например, обеспечению кибербезопасности критически важных приложений в целом, индустрии, медицинскому и автомобильному оборудованию. Компания определяет свой сегмент рынка как CIMA (Cybersecurity, Industrial, Medical & Automotive).

Flexxon сосредоточена на разработке продуктов и решений, которые могут быть сконфигурированы для поддержки самых разных требований к промышленным средам и направлены на удовлетворение нужд ее клиентов в любой точке земного шара. Для организации надежного, ориентированного и долговечного хранения информации компания поставляет устройства памяти, которые, помимо высокой надежности, требуемой рынком CIMA, обеспечивают и безопасность данных.

Поскольку мы сталкиваемся с постоянно растущим числом краж данных и кибератак, во главу угла становится наличие надежного и эффективного решения для киберзащиты. Поэтому компания создала специальные кибербезопасные решения с использованием технологии флэш-памяти NAND. Стремясь устранить киберугрозы, специалисты компании разработали решение по обеспечению кибербезопасности на основе прошивки. Это первое в мире решение по кибербезопасности на основе ИИ сертифицировано как последний уровень защиты от киберугроз и уже получило награду CSA Group: Product Certification & Standards Development. Благодаря такому решению SSD компании Flexxon обеспечивают целостность и конфиденциальность данных, а также общую кибербезопасность конечных систем. Рассмотрим одно из последних изделий компании, выполненное на основе проприетарной технологии.

ТВЕРДОТЕЛЬНЫЕ НАКОПИТЕЛИ FLEXXON X-PHY, СПОСОБНЫЕ ЗАЩИТИТЬ САМИ СЕБЯ

В апреле 2021 г. компания Flexxon представила под торговой маркой X-PHY первый SSD с защитой на физическом уровне. Новый SSD отличают встроенные решения безопасности, которые выполнены на основе ИИ и, по словам компании, обещают защиту не только от традиционных угроз, таких как вредоносные программы и вирусы, но и от физического вмешательства. Внешний вид нового SSD показан на рис. 2.

Современные контроллеры SSD строятся на нескольких ядрах Arm Cortex R и в основном представляют собой довольно высокопроизводительную систему-на-кристалле

РИС. 2. ▲ Новый твердотельный накопитель Flexxon X-PHY — с защитой на физическом уровне

со множеством вычислительных возможностей. Именно эти возможности, наряду с усовершенствованиями микропрограмм, стали основой платформы новых твердотельных накопителей Flexxon X-PHY.

Платформа базируется на технологии, которую Flexxon называет AI One Core Quantum Engine, и специальной защищенной прошивке. Описание технологии довольно расплывчатое, поэтому пока неясно, является ли ее движок полностью самодостаточной (изолированной) платформой или комбинацией программного обеспечения, оборудования и прошивки [5]. Уровни защиты твердотельного накопителя X-PHY представлены на рис. 3.

Как уже было сказано, данные по конкретным решениям, использованным в SSD X-PHY, пока скудные. AI One Core Quantum Engine предположительно работает на контроллере SSD, совместимом с NVMe 1.3, и отслеживает весь трафик. Как только его алгоритм обнаруживает угрозу (вирус, вредоносное программное обеспечение, вторжение), он может заблокировать ее, чтобы защитить прошивку и целостность данных. Кроме того, компания заявила, что алгоритм самообучения может обнаруживать отклонения и идентифицировать их как угрозы. Судя по изображению, опубликованному на сайте компании, X-PHY совместим со всеми основными операционными системами (рис. 2).

Аппаратная защита нового SSD включает ряд сенсоров, в том числе температурные датчики, которые дают возможность определять возможные физические вторжения. В случае вторжения пользователю по электронной почте направляется сообщение о проблеме, а накопитель полностью блокируется. В дальнейшем владелец может восстановить доступ к данным, пройдя аутентификацию. Накопители могут быть также настроены на полное автоматическое удаление информации в критических ситуациях. Это исключит возможность попадания секретных данных в чужие руки. Однако (опять обратимся к [5]) не вполне понятно, как устройство может предупредить своего владельца по электронной почте, если кто-то украдет его с выключенного ПК. Способы контролировать активность жесткого диска, когда компьютер выключен, чтобы заблокировать SSD, если он будет удален, есть. Тем не менее не существует способа отправить уведомление о физическом вторжении, если ОС не работает (если, конечно, SSD не оснащен тем или иным беспроводным модемом). Компания Flexxon подчеркивает, что твердотельный накопитель X-PHY не заменяет традиционные меры безопасности, и называет его «последней линией обороны» (рис. 4). До публикации более детального описания нам остается принять это как данность — как в старом анекдоте про Василия Ивановича («У нас джентльменам верят на слово!»).

Новый SSD с интеллектуальной защитой будет поддерживать технологию LDPC ECC (Low Density Parity Check Code), в которой применяется код коррекции ошибок с контролем четности с низкой плотностью, а также динамическое и статическое

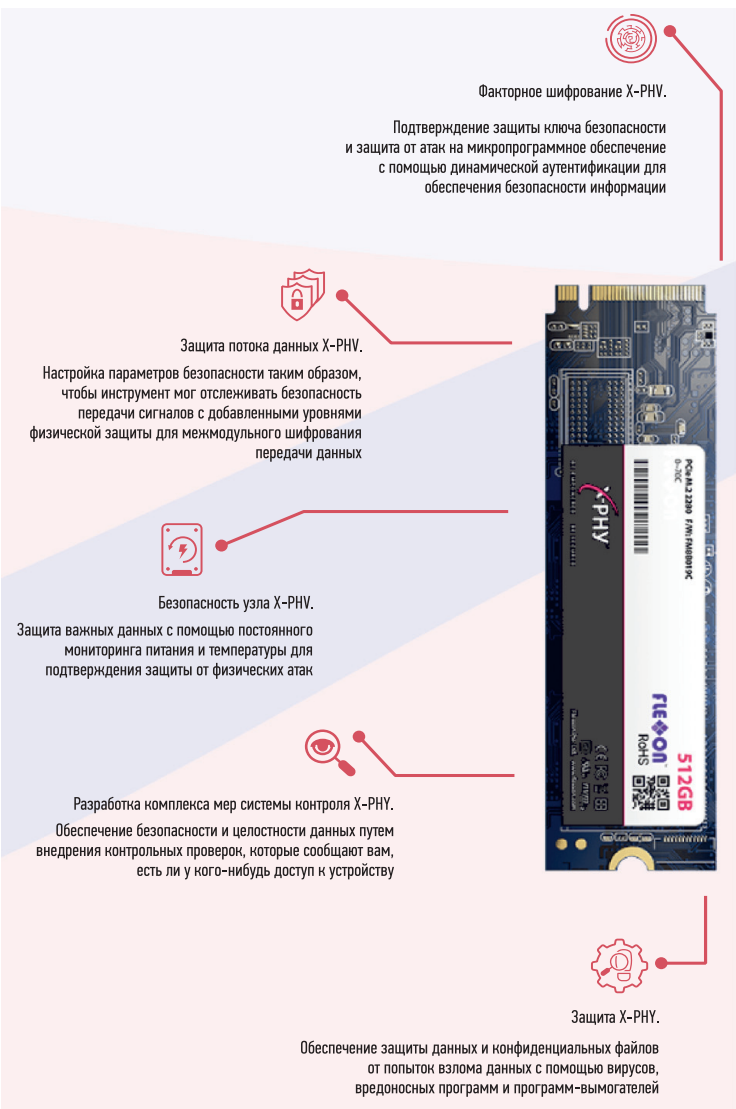

РИС. 3. ▶ Уровни защиты твердотельного накопителя X-PHY

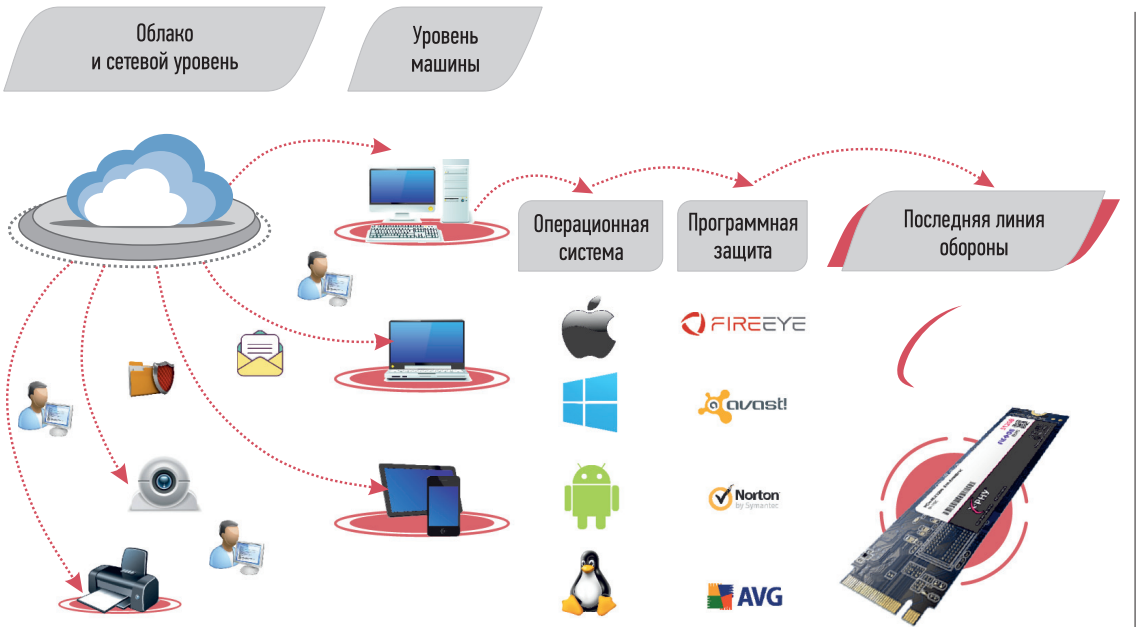

РИС. 4. Твердотельный накопитель X-PHY — «последняя линия обороны»

выравнивание износа (англ. wear leveling — технология перемещения часто изменяемых данных по выделенному адресному пространству флэш-памяти) [6].

Выравнивание — очень полезная опция, так как на любом компьютере существуют файлы, которые остаются неизменными в течение длительного времени, например системные файлы и определенные приложения. Поскольку флэш-ячейки NAND хоть и медленно, но деградируют с каждым циклом программирование/стирание (P/E cycle), ячейки, которые содержат неизменяемые данные, используются в меньшей степени, что приводит к неравномерной деградации ячеек и в итоге к сокращению срока службы устройств. Выравнивание износа для реализации полного потенциала SSD обеспечивает регулярный перенос таких постоянных данных между блоками, что в некоторой степени нивелирует проблемы надежности технологии 3D TLC, на основе которой, согласно [5], выполнен новый накопитель, хотя компания на это прямо не указывает. Это наверняка так, поскольку у компании есть микросхемы флэш-памяти технологии SLC с максимальной емкостью всего 4 Гбайт.

SSD X-PHY компании Flexxon выполнен в формате M.2 2280 и U.2, а для подключения к нему предусмотрен интерфейс PCIe 3.0 × 4 с NVMe 1.3. В серию, согласно данным, приведенным в [7], вошли модели вместимостью 512 Гбайт и 1 Тбайт. Как сообщают в самой компании Flexxon, рассматриваемый твердотельный накопитель сейчас проходит испытания у соответствующих «государственных учреждений, медицинских и промышленных клиентов». Компания рассчитывает на то, что проблем не будет и этот SSD будет доступен уже в четвертом квартале 2021 г. или, в крайнем случае, в начале 2022 г. Кроме того, компания готовит и уже анонсировала мини-ПК GuardForce и сервер Fortress, где в качестве системных накопителей используются X-PHY SSD. Установка X-PHY SSD на материнской плате показана на рис. 5. Стоит отметить, что на сайте компании Flexxon [8] накопитель назван решением для ноутбука, что явно не соответствует действительности.

ПЕРВЫЕ ШАГИ В ПРОДВИЖЕНИИ ПЛАТФОРМЫ X-PHY CYBER SECURE

Уже сегодня с целью продвижения платформы X-PHY Cyber Secure компания Flexxon сотрудничает с известным мировым изготовителем ноутбуков Lenovo. Они планируют создать первую в мире линейку персональных компьютеров со встроенной аппаратной защитой для обеспечения кибербезопасности на базе искусственного интеллекта [7].

Такое решение сможет эффективно отражать сложные современные кибератаки, защищая пользователей от известных и неизвестных угроз посредством круглосуточного мониторинга и обнаружения. Партнерство с Lenovo станет важным шагом компании Flexxon в миссии по расширению прав и возможностей «цифровых» граждан с большей киберзащитой.

Уже в сентябре 2021 г. будут выпущены три серии ноутбуков, отвечающие различным предпочтениям пользователей, а именно X-PHY Ace, X-PHY CyberPad и X-PHY Zepto. Один из вариантов таких ноутбуков представлен на рис. 6. Эти ноутбуки будут сочетать высококачественные, проверенные временем оборудование и интерфейс компании Lenovo и технологии обеспечения кибербезопасности в режиме реального времени от компании Flexxon, эффективно устраняя ограничения традиционной

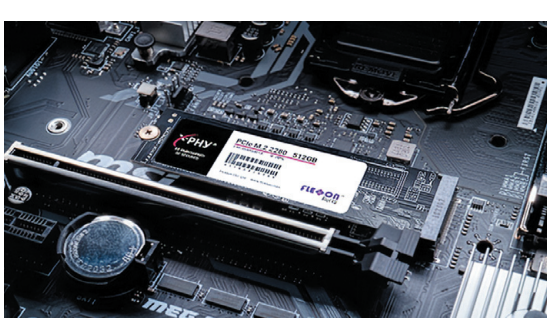

РИС. 5. Установка X-PHY SSD на материнской плате

РИС. 6. ▲ Разработанные совместно компаниями Flexxon и Lenovo серии ноутбуков со встроенной аппаратной защитой для кибербезопасности на базе ИИ

разрозненной архитектуры защиты программного обеспечения за счет повышения безопасности микропрограмм твердотельного накопителя.

Ноутбуки X-PHY AI Cybersecurity — пример структуры безопасности Zero Trust, необходимого требования к инфраструктуре кибербезопасности в сегодняшнем сложном ландшафте киберпреступности. Основанная на принципе «Никогда не доверяй, всегда проверяй», эта структура выходит за рамки традиционной защиты периметра и переходит в систему, в которой запросы доступа к критически важным данным постоянно отслеживаются, должным образом анализируются с помощью ИИ и только затем проверяются. Это предотвратит любые попытки фишинга, программ-вымогателей, кражи данных и других форм кибератак.

Другой ноутбук, X-PHY User Application Tool, надежен, безопасен и прост в использовании. Для навигации по его приборной панели и настройкам не требуется предварительных знаний о кибербезопасности, а его удобный интерфейс с динамической двухфакторной аутентификацией позволяет пользователям легко разблокировать свой компьютер после любой блокировки из-за обнаружения угрозы. После активации интерфейса только аутентифицированные пользователи могут разблокировать свои компьютеры с динамической безопасностью аутентификации через Bluetooth посредством установленного на смартфоне приложения X-PHY App (рис. 7). Приложение совместимо с операционными системами iOS и Android. С его помощью можно не только удаленно разблокировать компьютер, но и просмотреть «живые» уведомления и даже журналы прошлых событий.

Кроме того, попытки обойти защиту в существующих моделях SSD, такие как физическое удаление, атаки по побочным каналам с использованием скачков напряжения или внезапных колебаний температуры, заставят X-PHY Cyber Secure SSD немедленно заблокировать систему для защиты данных пользователя.

Благодаря сочетанию производительности и безопасности от Flexxon и новым ноутбукам Lenovo компании смогут прийти к кибербезопасности будущего, которая позволит пользователям работать с большей уверенностью в любое время и в любом месте. Партнерство этих компаний обещает еще много интересных совместных технологических инноваций. Поскольку Flexxon имеет большой послужной список в разработке эффективных, действенных и экономичных систем хранения и кибербезопасности, компания надеется работать вместе с Lenovo над созданием устойчивых решений, обеспечивающих защиту от постоянно развивающихся киберугроз. Больше информации доступно на специализированном сайте [8].

С полным перечнем продукции компании Flexxon можно ознакомиться на сайте компании [9] и в обзоре, опубликованном в [10]. Всю необходимую информацию по продуктам компании можно также получить у ее авторизованного дистрибьютора в Российской Федерации — компании SPEL Ltd. [11]. ⬢

ООО «СПЭЛ»
www.sp-el.ru
E-mail: sales@sp-el.ru
Тел./факс: +7 (812) 401-44-12

РИС. 7. ▼ Сообщение о несанкционированном действии на разработанном Flexxon и Lenovo ноутбуке

ЛИТЕРАТУРА

1. История развития флэш-памяти. https://habr.com/ru/company/kingston_technology/blog/391367/
2. Рентюк В. Память NOR-флэш малой емкости еще долго будет востребована во встроенных приложениях // Компоненты и технологии. 2021. № 8.
3. iSLC — Claiming the Middle Ground of the High-end Industrial SSD Market. www.innodisk.com/epaper/eDM/US_Whitepaper_Download_iSLC.html
4. Flexxon officially unveils the X-PHY AI Embedded Cyber Secure SSD. www.flexxon.com/flexxon-officially-launched-xphy-ssd/
5. Shilov A. Flexxon Launches X-Phy SSD with Embedded AI-Based Security Features. www.tomshardware.com/news/flexxon-ai-ssd-security-platform
6. Бенджамин Дж. Технология iRetention для хранения данных в средах с высокой температурой // Control Engineering Россия. 2018. № 5.
7. Flexxon INKS Partnership With Lenovo For First-ever Line Of Laptops With AI-Embedded Cybersecurity Hardware Defences. www.flexxon.com/flexxon-inks-partnership-with-lenovo/
8. Introducing World's First AI Cybersecurity Laptops. https://x-phy.com/laptop/?currency=USD
9. www.flexxon.com
10. Верхулевский К. Высоконадежные SSD-устройства компании Flexxon // Компоненты и технологии. 2019. № 10.
11. www.sp-el.ru