www.idisglobal.ru

Успешное предотвращение кибератак простым для пользователя способом

IDIS КИБЕРБЕЗОПАСНОСТЬ

В современных условиях возросла угроза кибератак на системы видеонаблюдения, что делает сетевую безопасность одной из главных проблем для заказчиков и инсталляторов. Помимо традиционных локальных и аппаратных мер безопасности, целостность, конфиденциальность и доступность данных видеонаблюдения должны быть защищены также во время записи, поиска и передачи данных. Теперь заказчики выбирают вендоров использующих современные технологии и имеющих большой опыт при решении этих задач.

IDIS, крупнейший производитель систем видеонаблюдения в Южной Корее, последовательно и всесторонне рассматривает проблемы кибербезопасности, начиная от НИОКР и до установки конечному заказчику. Имея комплексное решение для обеспечения максимальной защиты конечных пользователей, IDIS непрерывно разрабатывает новые инновационные технологии.
IDIS предлагает комплексный, многоуровневый и многосторонний подход к обеспечению максимальной кибербезопасности для пользователей. Этот подход фокусируется на трех основных уровнях: безопасный доступ к данным, безопасная передача данных и безопасная запись данных.

Безопасный доступ к данным

DirectIP ®

Межсетевой экран на NVR

Двухфакторная аутентификация

Безопасная передача данных

Transport Layer Security (TLS)

FEN Security

Безопасная запись данных

iBank

Chained Fingerprint Edge

Encryption Recording

IDIS® One Solution. One Company.

IDIS КИБЕРБЕЗОПАСНОСТЬ

IDIS DirectIP ®

Сетевая безопасность с помощью мощной системы взаимной аутентификации

IDIS DirectIP при помощи технологии plug-and-play взаимно аутентифицирует все продукты IDIS. Когда IP-камеры IDIS подключены к видеорегистраторам (NVR) IDIS, оба устройства аутентифицируют друг друга на основе сертификата. Это гарантирует, что обе стороны идентифицируют и распознают, с кем они общаются, до установления сеанса связи. Данные аутентификации хранятся и защищаются как на IP-камере, так и на NVR.

Кроме того, DirectIP позволяет избежать ошибок, связанных с человеческим фактором, устраняя необходимость управления несколькими IP-адресами и соответствующими паролями во время внедрения и обслуживания систем видеонаблюдения.

Межсетевой экран на NVR

Встроенный брандмауэр с поддержкой IP-фильтрации и аутентификации на портах

В видеорегистраторах (NVR) IDIS установлен собственный брандмауэр, который от слеживает и контролирует входящий и исходящий сетевой трафик на основе заранее определенного набора правил безопасности, включая проверку подлинности IP, MAC-адреса и портов. Межсетевые экраны в видеорегистраторах IDIS разработаны и заранее настроены для предотвращения несанкционированного доступа.

Двухфакторная аутентификация

Многофакторная аутентификация с использованием учетных записей пользователей и зарегистрированного мобильного приложения

Двухфакторная аутентификация (2FA) является одним из видов многофакторной системы аутентификации. Чтобы получить доступ к видеорегистраторам IDIS , пользователь должен подтвердить свою личность с помощью мобильного приложения IDIS после прохождения обычного процесса входа в систему, введя идентификатор пользователя и пароль. Все видеорегистраторы IDIS надежно защищают учетные записи пользователей с 2FA.

Протокол TLS (transport layer security)

Безопасность передачи данных в сочетании с запатентованной технологией IDIS с TLS

TLS является криптографическим протоколом, обеспечивающим аутентификацию и защиту от несанкционированного доступа, нарушения целостности передаваемых данных в сетях. Интеграция TLS в запатентованные решения IDIS оказывает минимальное влияние на производительность при передаче данных видеонаблюдения. Протокол TLS помогает предотвратить такие вредоносные действия, как прослушивание, изменение и уничтожение данных, когда они передаются между устройствами по сети.

iBank

Защита данных с помощью проприетарной системы IDIS

IDIS iBank - это система баз данных, разработанная и запатентованная IDIS специально для видеозаписи. Система максимально повышает эффективность хранения и обеспечивает быструю обработку данных.

Кроме того, iBank исключает чтение данных при помощи сторонних устройств (например, ПК), что защищает информацию от хищения, подделки и изменения.
iBank используется во всех устройствах записи и хранения IDIS.

Chained Fingerprint

Поддержание целостности данных

IDIS Chained Fingerprint - технология обеспечивающая целостность данных. Подобно технологии блокчейн, все кадры связаны между собой уникальными изменениями - отпечатками. При попытке изменить хотя бы один кадр вся последующая цепочка будет нарушена и видео признано поддельным. Благодаря IDIS Chained Fingerprint предоставленные в суд видеоданные будут являться неоспоримыми.

Edge Encryption Recording

Эффективная и мощная технология записи зашифрованных видеоданных

Технология записи Edge Encryption шифрует видеоданные на IP-камере перед сохранением и отправкой их по сети. Поэтому дополнительные процессы шифрования и дешифрования в системах хранения и передачи данных не требуются. Зашифрованные данные записываются непосредственно на SD-карты и жесткие диски, поэтому эти данные защищены от несанкционированного доступа и изменения, даже если SD-карты или жесткие диски украдены.

For Every Network (FEN) Security

Система безопасного доступа и передачи данных через сети общего доступа

IDIS FEN - система безопасного доступа и передачи данных, разработанная IDIS с использованием технологии P2P. FEN является службой автоматической настройки сети, которая упрощает установку систем видеонаблюдения. FEN позволяет пользователю получить доступ к системе, не требуя при этом глубоких знаний о маршрутизации в IP-сетях.