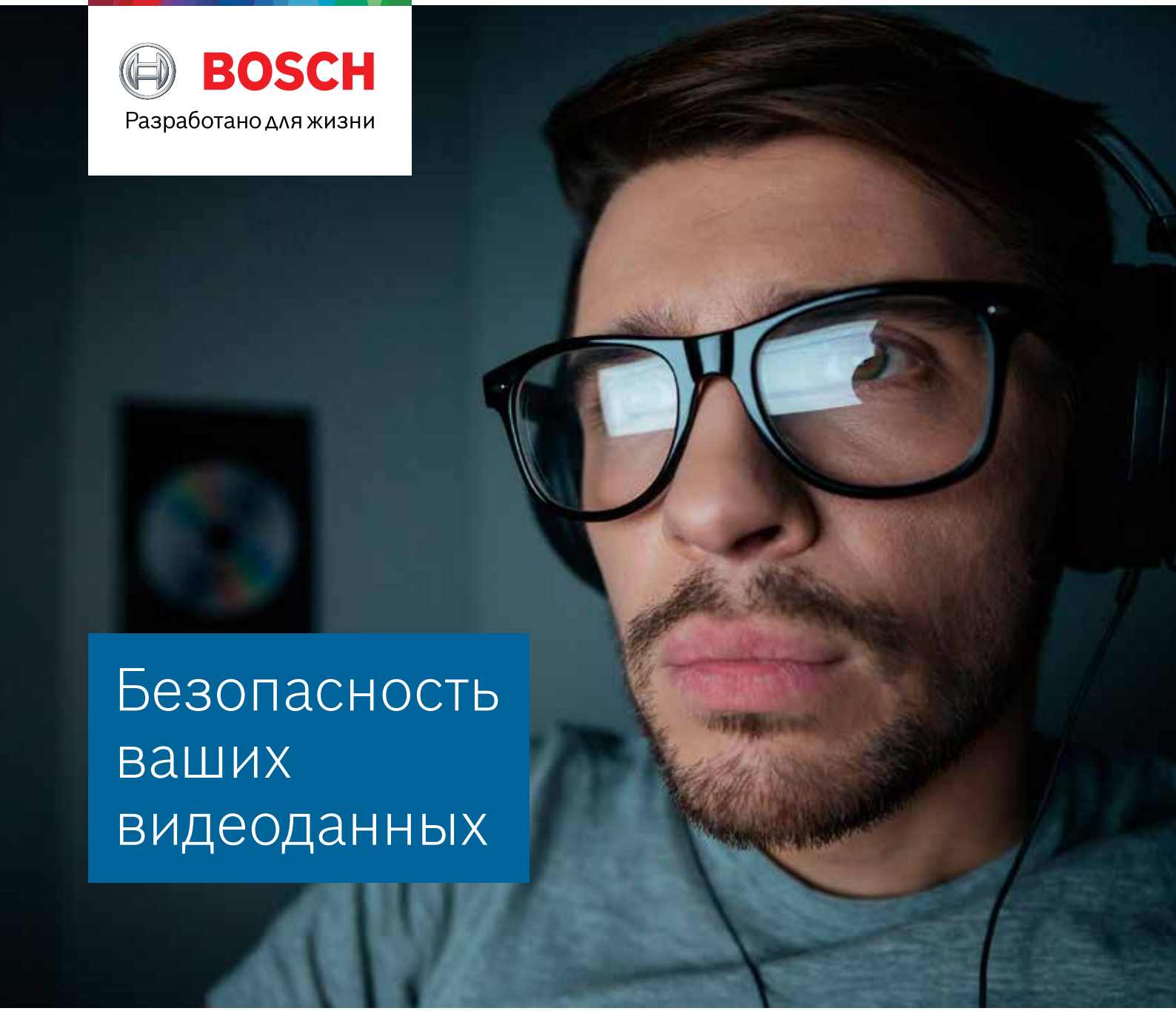
BOSCH

Разработано для жизни



Безопасность ваших видеоданных

Системы, в которых хранятся данные безопасности, становятся все более и более связанными с локальными и глобальными сетями. Все больше камер (удаленные компоненты) отправляет данные на серверы (основные компоненты) через Интернет, в котором действуют злоумышленники и хакеры.

Опасности

Даже одно слабое звено может поставить под угрозу всю систему видеобезопасности. Например, опытные хакеры могут устраивать так называемые атаки посредника и перехватывать данные, передаваемые между камерой и системой управления видео (VMS). Получив доступ, хакеры могут заменить видеопоток, чтобы скрыть противоправные действия, или изменить видеоизображение с камеры в реальном времени, чтобы избирательно убрать из сцены определенные детали или людей.

Защита по всем фронтам

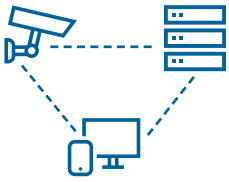
Мы обеспечиваем безопасность высшего класса, используя четырехуровневый подход, учитывающий все компоненты инфраструктуры видеобезопасности. Мы создаем доверие, назначая каждому компоненту в сети ключ проверки подлинности. Мы защищаем данные от хакеров, шифруя их на аппаратном уровне с использованием криптографического ключа, надежно хранящегося в уникальном встроенном доверенном платформенном модуле (TPM). Мы предлагаем удобные способы управления правами доступа пользователей, чтобы доступ к вашим данным был только у уполномоченных людей. Наконец, мы поддерживаем настройку инфраструктуры открытых ключей. Компания Bosch обеспечивает наивысший уровень безопасности.

Так как видеоданные часто очень важны и при этом конфиденциальны, компания Bosch использует систематический подход к обеспечению максимальной защиты данных, учитывающий одновременно физическую безопасность и кибербезопасность. Систематический подход компании Bosch – главная причина, почему нам удается задавать самые высокие стандарты в области комплексной защиты данных.

Компания Bosch защищает все основные элементы инфраструктуры видеобезопасности:

Защита камер

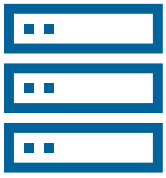
- Поддерживаются защищенные подключения (HTTPS)
- Принудительное использование пароля при начальной настройке
- Выполнение сторонних программ «отключено»
- Обновления микропрограммы только через подписанные производителем файлы
- Криптографические операции, необходимые для проверки подлинности и шифрования, выполняются только в уникальном встроенном доверенном платформенном модуле (TPM)



Защита связи по сети

- «Небезопасные» порты по умолчанию отключены
- Принудительное использование пароля при начальной настройке
- Проверка подлинности в сети с использованием протокола 802.1x
- Поддержка стандарта шифрования AES (с использованием ключей шифрования до 256 бит)

Чтобы узнать подробнее, загрузите:
Руководство по безопасности данных
Техническое примечание по проверке подлинности в сети
VS-EH-ru-06_F01U561105_02



Защита основных устройств

- Криптографические операции, необходимые для проверки подлинности и шифрования, выполняются только в уникальном встроенном доверенном платформенном модуле (TPM)
- Поддержка Microsoft Active Directory для безопасного управления правами доступа пользователей
- Доступ только с дайджест-проверкой подлинности
- Регулярные обновления за счет исправлений для обеспечения безопасности

Поддержка инфраструктур открытых ключей (PKI)

- Уникальные подписанные компанией Bosch и загружаемые на заводе сертификаты на всех камерах
- Уникальный встроенный доверенный платформенный модуль (TPM) для исключительной надежности криптографических операций
- Собственный центр сертификации (Escrypt)
- Поддержка пользовательских сертификатов клиента
- Поддержка сторонних решений PKI