ТЕХНИЧЕСКИЙ ОБЗОР

# Краткое руководство по листам технических данных Axis

## Нормативные требования, сертификации и протоколы

Ноябрь 2021

AXIS COMMUNICATIONS

# Содержание

# 1 Введение

Axis Communications соблюдает применимые отраслевые стандарты и нормативные требования во всей своей продукции, которую представляет на рынке. Этот документ служит дополнением к листам технических данных Axis и содержит определения и короткие описания упоминаемых в них аббревиатур, нормативных требований, сертификаций и протоколов.

Настоящий документ содержит информацию о разделах листа технических данных, которые выделены и увеличены на приведенной ниже иллюстрации.

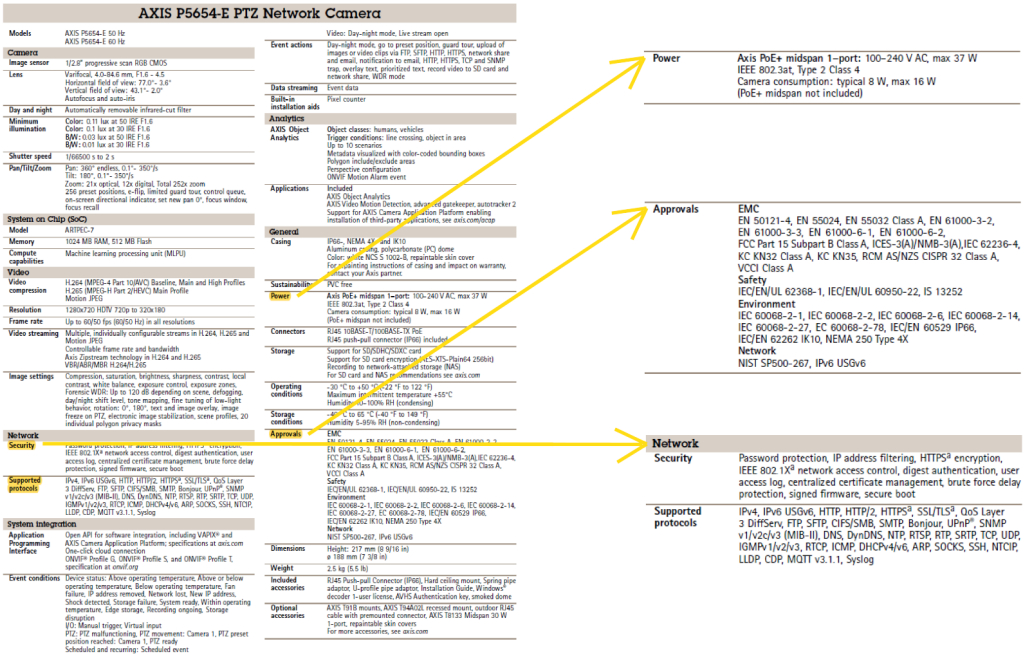


*Figure 1. Разделы листа технических данных Axis, рассматриваемые в настоящем документе.*

# 2 Нормативные требования

Раздел нормативных требований листа технических данных Axis содержит информацию о соответствии различным стандартам. Этот раздел часто делится на подразделы: "ЭМС", "Безопасность", "Среда эксплуатации", "Сеть" и "Другое". Раздел "Другое" может содержать сведения о взрывобезопасности или безопасности при управлении доступом. Если вместе с изделием продается инжектор, также может быть предусмотрен подраздел о соответствии инжектора нормативным требованиям.

## 2.1 ЭМС (электромагнитная совместимость)

Все производители средств сетевого видеонаблюдения обязаны декларировать электромагнитную совместимость своего оборудования для сетевого видеонаблюдения. В некоторых случаях производители могут сертифицировать соответствие самостоятельно, но большинство производителей пользуются услугами аккредитованных испытательных лабораторий,

предоставляющих отчеты об испытаниях с подтверждением соответствия. Соответствие нормативным требованиям по ЭМС делится на две части - помехоэмиссия и помехозащищенность.

*Помехоэмиссия* - это способность оборудования функционировать надлежащим образом, не излучая чрезмерное количество электромагнитной энергии, способной нарушить работу окружающего оборудования.

*Помехоустойчивость* - это способность электронного оборудования выдерживать воздействие электромагнитных помех (излученных и кондуктивных) от других электронных устройств. В странах Европы ЭМС входит в сертификацию CE Mark, которая, в свою очередь, включена в гармонизированное законодательство ЕС.

Перечисленные ниже стандарты устанавливают нормы и методики для испытаний на помехоэмиссию и помехоустойчивость. Поскольку единого испытания, гарантирующего соответствие всем существующим нормативам, не существует, для каждого региона или применения могут действовать разные требования.

### 2.1.1 Стандарты на ИТ-оборудование

Эти стандарты применяются к мультимедийному оборудованию с напряжением питания переменного и постоянного тока не более 600 В. Мультимедийное оборудование определяется как информационно-технологическое оборудование, звуковое оборудование, видеооборудование, оборудование для приема телерадиовещания и оборудование для управления освещением в развлекательной отрасли.

- EN 55032 Class A: стандарт помехоэмиссии (коммерческие, промышленные, офисные зоны), гармонизированный с международными стандартами
- EN 55032 Class B: стандарт помехоэмиссии (жилые зоны), гармонизированный с международными стандартами
- EN 55035: стандарт помехозащищенности, гармонизированный с международными стандартами

### 2.1.2 Гармонизированные стандарты по странам/регионам

- EN 61000-6-1 и EN 61000-6-2: общие стандарты соответствия (Европа)
- FCC Part 15 Subpart B Class A и B: Федеральная комиссия США по связи (FCC) устанавливает правила и нормативы для телекоммуникационных устройств, ориентируясь на помехоэмиссию, а не на помехозащищенность (применяются в США)
- ICES-3 (A и B)/NMB-3 (A и B) (Канада)
- VCCI Class A и B (Япония)
- KS C 9832 Class A и B, KS C 9835, KS C 9547, KS C 9815 (Корея)
- RCM AS/NZS CISPR 32 Class A и B (Австралия/Новая Зеландия)

### 2.1.3 Дополнительные стандарты по областям применения/продуктам

- EN 50121-4, IEC 62236-4: устанавливает требования к характеристикам для сигнализации и связи, которое может создавать помехи для другого оборудования на железных дорогах.
- EN 50130-4: распространяется на компоненты систем тревожной сигнализации, включая системы управления доступом, системы видеонаблюдения, системы пожарной сигнализации, системы

защиты от нападений, системы сигнализации о вторжении, общественные системы тревожной сигнализации.

## 2.2 Безопасность

- Директива о низковольтном оборудовании (2014/35/EU): устанавливает общие требования к безопасности электрического оборудования. Призвана обеспечить безопасность использования продукции без риска травм и материального ущерба.
- IEC/EN/UL 62368-1: требования к сетевым видеокамерам, кодерам, блокам питания, призванные снизить риски возгорания, электротравм и вреда здоровью для лиц, которые могут контактировать с этим оборудованием
- IEC/EN/UL 60950-22: особые требования к безопасности продукции и корпусов, эксплуатируемых вне помещения
- IEC/EN 62471-1: требования к фотобиологической безопасности ламп и систем ламп по уровню облучения, призванные предотвратить повреждение глаз и кожи
- EN/UL/CSA 60065: применяется для электронного оборудования с электропитанием от сети, от блока питания, от батарей или от удаленного источника питания и предназначенного для приема, генерации, записи или воспроизведения звука, видео и связанных с ними сигналов
- IS 13252: индийский стандарт требований к сетевым видеокамерам, кодерам, блокам питания, призванные снизить риски возгорания, электротравм и вреда здоровью для лиц, которые могут контактировать с этим оборудованием

## 2.3 Среда эксплуатации

### 2.3.1 Класс защиты IP

Разработанный IEC (Международная электротехническая комиссия, МЭК) стандарт IEC 60529 устанавливает классы защиты IP (защита от проникновения), обозначаемые кодами из двух цифр. Класс защиты IP характеризует степень защищенности электрического устройства от механического проникновения, проникновения пыли, случайного касания и воды.

*Таблица 2.1 Классы защиты IP - первая цифра после IP: посторонние твердые предметы*

| Уро-вень | Защита от | Воздействия, против которых эффективна защита |
|---|---|---|
| 0 | Защита отсутствует | Защита отсутствует |
| 1 | Твердые предметы размером более 50 мм | Большие поверхности тела, например, тыльная сторона ладони; защита от намеренного проникновения частей тела отсутствует. |
| 2 | Твердые предметы размером более 12,5 мм | Пальцы и другие объекты могут проникать на глубину до 80 мм при условии, что это не сопряжено с риском касания опасных частей. Полное проникновение предметов диаметром более 12,5 мм невозможно. |
| 3 | Твердые предметы размером более 2,5 мм | Полностью исключено проникновение таких объектов, как инструменты и толстые провода. |

*Таблица 2.1. Классы защиты IP - первая цифра после IP: посторонние твердые предметы (Продолжение)*

| | | |
|---|---|---|
| 4 | Твердые предметы размером более 1 мм | Полностью исключено проникновение таких объектов, как провода и винты. |
| 5 | Пылезащита | Полная защита от проникновения пыли не обеспечивается, однако количество проникшей пыли является незначительным и не нарушает надлежащую работу оборудования. |
| 6 | Пыленепроницаемость | Попадание пыли исключено. |

*Таблица 2.2 Классы защиты IP - вторая цифра после IP: жидкости*

| **Уро-вень** | **Защита от** | **Воздействия, против которых эффективна защита** |
|---|---|---|
| 0 | Защита отсутствует | Особая защита отсутствует |
| 1 | Капающая вода | Вертикально падающие капли воды не оказывают неблагоприятного воздействия. |
| 2 | Капли воды под наклоном до 15° | Вертикально капающая вода не оказывает неблагоприятного воздействия при любом наклоне корпуса не более чем на 15° от нормального положения. |
| 3 | Распыляемая вода | Мелкие водяные брызги, падающие под углом до 60° относительно вертикали, не оказывают неблагоприятного воздействия. |
| 4 | Разбрызгиваемая вода | Крупные водяные брызги, падающие на корпус под любым углом, не оказывают неблагоприятного воздействия. |
| 5 | Струи воды | Водяные струи из сопла, направленные на корпус под любым углом, не оказывают неблагоприятного воздействия. |
| 6 | Сильные струи воды | Морские волны и мощные струи воды не проникают в корпус в количестве, способном оказать вредное воздействие. |
| 7 | Кратковременное погружение в воду | Исключается проникновение воды в опасных количествах при погружении корпуса в воду на определенное время и при определенном давлении. |
| 8 | Постоянное погружение в воду | Оборудование способно находиться под водой длительное время при соблюдении условий, указанных производителем. Условия должны быть жестче, чем для IPX7 (см. предыдущую категорию). |
| 9 | Вода под высоким давлением и очистка паром высокого давления | Струи воды под очень высоким давлением, падающие на корпус под любым углом, не оказывают неблагоприятного воздействия. |

### 2.3.2 Другие применимые стандарты IEC

- IEC 60068-2: стандарт испытаний электронного оборудования и изделий на способность способности такого оборудования работать при различных условиях окружающей среды, включая экстремально низкие температуры и высокие температуры в сочетании с низкой влажностью. Приведенные ниже процедуры этого стандарта обычно применяются для изделий, находящихся в процессе испытаний при установившейся температуре.

- IEC 60068-2-1: холод
- IEC 60068-2-2: сухое тепло
- IEC 60068-2-6: вибрация (непрерывная)
- IEC 60068-2-14: изменение температуры
- IEC 60068-2-27: удар
- IEC 60068-2-30: влажное тепло (циклическое)
- IEC 60068-2-64: вибрация (широкополосная случайная)
- IEC 60068-2-78: влажное тепло (постоянный режим)

- Стандарт IEC 60825 Class I: призван гарантировать безопасность лазера, используемого в модуле лазерной фокусировки, в любых ситуациях, возникающих при нормальной эксплуатации.

### 2.3.3 Класс защиты NEMA

NEMA (National Electrical Manufacturers Association) - это американская ассоциация, разрабатывающая стандарты для корпусов электрического оборудования. NEMA представила свой стандарт NEMA 250 для использования во всем мире. NEMA также приняла к использованию и опубликовала гармонизированный стандарт IP, ANSI/IEC 60529, через Американский национальный институт стандартов (ANSI).

Стандарт NEMA 250 регламентирует защиту от внешнего проникновения, а также учитывает другие факторы, такие как стойкость к коррозии, рабочие характеристики и детали конструкции. В связи с этим типы NEMA могут перекрывать классы IP, но не наоборот.

Стандарты UL 50 и UL 50E основаны на стандартах NEMA 250. NEMA разрешает самостоятельную сертификацию, в то время как UL предусматривает обязательное прохождение независимого испытания и обследования.

*Таблица 2.3 Классы NEMA для корпусов, используемых в неопасных средах*

| NEMA | Эквивалентный класс защиты IP | Для установки в помещениях | Для наружной установки | Защита от |
|---|---|---|---|---|
| Тип 1 | IP10 | X | | Доступ к опасным частям и проникновение твердых инородных предметов (падающая грязь). Защита от проникновения жидкостей отсутствует. |
| Тип 3 | IP54 | X | X | Доступ к опасным частям и проникновение твердых инородных предметов (падающая грязь и переносимая ветром пыль). Проникновение воды (дождь, мокрый снег, снег). Не получает повреждений от образования льда снаружи на корпусе. |

*Таблица 2.3. Классы NEMA для корпусов, используемых в неопасных средах (Продолжение)*

| | | | | |
|---|---|---|---|---|
| Тип 3R | IP14 | X | X | Доступ к опасным частям и проникновение твердых инородных предметов (падающая грязь). Проникновение воды (дождь, мокрый снег, снег). Не получает повреждений от образования льда снаружи на корпусе. |
| Тип 3S | IP54 | X | X | Доступ к опасным частям и проникновение твердых инородных предметов (падающая грязь и переносимая ветром пыль). Проникновение воды (дождь, мокрый снег, снег). Внешние механизмы сохраняют работоспособность при обледенении. |
| Тип 4 | IP56 | X | X | Доступ к опасным частям и проникновение твердых инородных предметов (падающая грязь и переносимая ветром пыль). Проникновение воды (дождь, мокрый снег, снег, брызги воды, вода из шланга). Не получает повреждений от образования льда снаружи на корпусе. |
| NEMA 4X | IP56 | X | X | Доступ к опасным частям и проникновение твердых инородных предметов (падающая грязь и переносимая ветром пыль). Проникновение воды (дождь, мокрый снег, снег, брызги воды, вода из шланга). Обеспечивает дополнительную защиту от коррозии. Не получает повреждений от образования льда снаружи на корпусе. |
| Тип 6 | IP67 | X | X | Доступ к опасным частям и проникновение твердых инородных предметов (падающая грязь). Проникновение воды (струя воды из шланга и попадание воды при эпизодическом временном погружении на ограниченную глубину). Не получает повреждений от образования льда снаружи на корпусе. |
| Тип 6P | IP67 | X | X | Доступ к опасным частям и проникновение твердых инородных предметов (падающая грязь). Проникновение воды (струя воды из шланга и попадание воды при длительном погружении на ограниченную глубину). Обеспечивает дополнительную защиту от коррозии. Не получает повреждений от образования льда снаружи на корпусе. |
| Тип 12 | IP52 | X | | Без выбивных отверстий. Доступ к опасным частям и проникновение твердых инородных предметов (падающая грязь и летающая пыль, волокна и частицы). Проникновение воды (капли сверху и легкие брызги). |
| Тип 12K | IP52 | X | | С выбивными отверстиями. Доступ к опасным частям и проникновение твердых инородных предметов (падающая грязь и летающая пыль, волокна и частицы). Проникновение воды (капли сверху и легкие брызги). |
| Тип 13 | IP54 | X | | Доступ к опасным частям и проникновение твердых инородных предметов (падающая грязь и летающая пыль, ворс, волокна и частицы). Проникновение воды (капли сверху и легкие брызги). Распыленная вода, брызги воды и протекание масла и коррозионно неактивных антифризов. |

NEMA TS 2 – это руководство по проектированию сигнального оборудования для управления дорожным движением.

### 2.3.4 Класс защиты IK

Классы IK определены в международном стандарте IEC/EN 62262, который устанавливает степени защиты от внешних механических воздействий. Этот стандарт, первоначально утвержденный в 1994 году как европейский стандарт EN 50102, позднее, в 2002 г., был принят в качестве международного.

Многие производители идут по пути испытания наиболее уязвимых частей изделия, чтобы гарантировать стойкость изделия на протяжении всего срока службы.

| Уровень | IK01 | IK02 | IK03 | IK04 | IK05 | IK06 | IK07 | IK08 | IK09 | IK10 | IK10+* |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Энергия удара (Дж) | 0,14 | 0,2 | 0,35 | 0,5 | 0,7 | 1 | 2 | 5 | 10 | 20 | 50* |
| Масса (кг) | <0,2 | <0,2 | 0,2 | 0,2 | 0,2 | 0,5 | 0,5 | 1,7 | 5 | 5 | |
| Высота падения (мм) | 56 | 80 | 140 | 200 | 280 | 400 | 400 | 300 | 200 | 400 | |

*Удар до 50 Дж. Производитель должен указать энергию, массу и высоту падения ударного элемента.

## 2.4 Другие нормативные требования

### 2.4.1 Взрывобезопасность

- IEC/EN/UL/SANS/CSA 60079-0: общие требования к конструкции, испытанию и маркировке взрывобезопасного оборудования и взрывобезопасных комплектующих, предназначенных для использования во взрывоопасной атмосфере.
- IEC/EN/UL/SANS/CSA 60079-1: специальные требования к конструкции и испытанию электрического оборудования с взрывонепроницаемой оболочкой типа d, предназначенного для эксплуатации в атмосфере взрывоопасного газа.

### 2.4.2 Нормативные требования для инжекторов

В случаях, когда в комплект поставки изделия входит инжектор, в этом разделе листа технических данных приводятся сведения о соответствии инжектора нормативным требованиям. Пояснения см. в предыдущих разделах настоящего документа.

### 2.4.3 Безопасность в управлении доступом

- UL 294: определяет требования к конструкции, характеристикам и эксплуатации систем управления доступом.

# 3 Сертификации

Корпус камеры, устанавливаемой в потенциально взрывоопасной среде, должен отвечать особым стандартам безопасности. Он должен защищать окружающую среду от потенциальных источников воспламенения в камере и другом оборудовании.

Европейская продукция должна соответствовать директиве ATEX; соответствующий международный стандарт носит название IECEx. В Северной Америке в основном используются классы и подразделения NFPA70 (Национальный свод законов и стандартов США по электротехнике, NEC) и CSA C22.1 (Канадский свод законов и стандартов по электротехнике, CEC) в дополнение к системе зон, описанной в ATEX и IECEx.

*Таблица 3.1 Уровни взрывобезопасности*

| Класс / подраздел | Атмосфера | Определение | Зона (IECEx и ATEX) |
|---|---|---|---|
| Класс I / подраздел 1 | Газ | Зона, где взрывчатая смесь присутствует постоянно или в течение длительных периодов времени. | Зона 0 |
| Класс I / подраздел 1 | Газ | Зона, где взрывчатая смесь с большой вероятностью появляется в нормальном процессе работы. | Зона 1 |
| Класс I / подраздел 2 | Газ | Зона, где появление взрывчатой смеси при нормальной работе маловероятно, а в случае такого появления оно является кратковременным. | Зона 2 |
| Класс II / подраздел 1 | Пыль | Зона, где взрывчатая смесь присутствует постоянно или в течение длительных периодов времени. | Зона 20 |
| Класс II / подраздел 1 | Пыль | Зона, где взрывчатая смесь с большой вероятностью появляется в нормальном процессе работы. | Зона 21 |
| Класс II / подраздел 2 | Пыль | Зона, где появление взрывчатой смеси при нормальной работе маловероятно, а в случае такого появления оно является кратковременным. | Зона 22 |

# 4 Питание

## 4.1 Классы Power over Ethernet (PoE)

Классы PoE обеспечивают эффективное распределение электропитания, устанавливая значения мощности, которая требуется для питаемого устройства (PD).

*Таблица 4.1 Классы PoE*

| Класс | Тип | Гарантированное значение мощности на питающем устройстве | Максимальная мощность, потребляемая питаемым устройством |
|---|---|---|---|
| 0 | Тип 1, 802.3af | 15,4 Вт | 0,44 Вт — 12,95 Вт |

*Таблица 4.1. Классы PoE (Продолжение)*

| | | | |
|---|---|---|---|
| 1 | Тип 1, 802.3af | 40,0 Вт | 0,44 Вт — 3,84 Вт |
| 2 | Тип 1, 802.3af | 7,0 Вт | 3,84 Вт — 6,49 Вт |
| 3 | Тип 1, 802.3af | 15,4 Вт | 6,49 Вт — 12,95 Вт |
| 4 | Тип 2, 802.3at* | 30 Вт | 12,95 Вт — 25,5 Вт |
| 6 | Тип 3, 802.3bt | 60 Вт | 51 Вт |
| 8 | Тип 3, 802.3bt | 100 Вт | 71,3 Вт |

*Этот тип также называется PoE+.

# 5 Сеть

## 5.1 Защита и контроль безопасности

Существуют различные способы противодействия угрозам в отношении составляющих системы. Некоторые угрозы представляют риски для оборудования, в то время как другие представляют риски для сетей или данных в процессе передачи или хранения. Вот некоторые меры безопасности, которые могут быть приняты для защиты оборудования и сетей:

- Учетные данные (пользователь/пароль) защищают от несанкционированного доступа к видео и настройкам оборудования. Использование учетных записей с различными уровнями полномочий позволяет регулировать доступ к различным ресурсам.
- Фильтрация по IP (межсетевой экран) сокращает уязвимость устройства в локальной сети и тем самым защищает его от доступа неуполномоченных клиентов. Это снижает риски в случае рассекречивания пароля устройства, а также в случае обнаружения новых критических уязвимостей.
- IEEE 802.1x: защита сети от неуполномоченных клиентов. Спецификация 802.1x направлена на защиту сетевой инфраструктуры с помощью управляемых коммутаторов и RADIUS-сервера. Клиент 802.1x в устройстве обеспечивает аутентификацию устройства в сети.
- HTTPS (HyperText Transfer Protocol Secure): защищает данные (видео) от прослушивания в сети. Использование подписанных сертификатов в HTTPS дает видеоклиенту возможность проверить, что он подключен к легитимной камере, а не к вредоносному компьютеру, имитирующему камеру.
- Подписанное встроенное ПО создается поставщиком программного обеспечения, который подписывает образ встроенного ПО с помощью своего закрытого ключа. Если к встроенному ПО присоединена такая подпись, устройство проверяет встроенное ПО перед его приемом и установкой. Если устройство обнаруживает нарушение целостности встроенного ПО, оно отклоняет обновление прошивки. Встроенное ПО Axis шифруется с помощью принятого в отрасли способа шифрования с открытым ключом на основе алгоритма RSA.
- Безопасная загрузка представляет собой процесс загрузки, состоящий из неразрывной цепочки криптографически проверенного программного обеспечения, берущей начало в с неизменяемой памяти (загрузочное ПЗУ). Технология безопасной загрузки основана на применении подписанного встроенного ПО; она гарантирует, что устройство будет загружаться только с авторизованным встроенным ПО. Безопасная загрузка гарантирует отсутствие на устройстве Axis вредоносных программ после его сброса до заводских установок.

- TPM (доверенный платформенный модуль) — это компонент, предоставляющий набор криптографических функций для защиты информации от несанкционированного доступа. Закрытый ключ хранится в TPM и не покидает его пределов. Все криптографические операции, требующие использования закрытого ключа, передаются в для обработки в TPM. Благодаря этому секретная часть сертификата остается защищенной даже в случае взлома.
- Axis Edge Vault — это защищенный криптографический вычислительный модуль (модуль или защищенный элемент), в который записывается и в котором надежно и постоянно хранится идентификатор устройства Axis.

Другие ресурсы по кибербезопасности можно найти на сайте *www.axis.com/cybersecurity*

## 5.2 Поддерживаемые протоколы

Для безопасной передачи данных между подключенными к сети устройствами применяется множество протоколов.

### 5.2.1 Референсные модели протоколов

Понять взаимодействие различных протоколов между собой удобнее всего используя сетевую модель OSI. Также существует референсная модель TCP/IP.

#### 5.2.1.1 Референсная модель OSI

Модель, описывающая обмен данными между открытыми системами. Для предоставления услуг каждый уровень модели использует услуги лежащего сразу под ним уровня. Каждый уровень при предоставлении услуг должен соответствовать определенным правилам (протоколам).

**Уровень 7 – прикладной уровень**

Предоставляет приложениям различные функции - доступ к Web, файлам, электронной почте и т.п.

Реальные приложения, например, браузеры или клиенты электронной почты, действуют поверх этого уровня и не описываются моделью OSI.

**Уровень 6 – уровень представления (данных)**

Обеспечивает возможность чтения данных прикладным уровнем системы, другой системой или тем же приложением в более поздний момент времени. Преобразует зависимые от системы форматы данных, например, ASCII, в независимый формат, обеспечивающий синтаксически корректный обмен данными между разными системами.

**Уровень 5 – сеансовый уровень (сеанс - устойчивое соединение между равноправными узлами)**

Предоставляет ориентированные на приложения услуги и отвечает за взаимодействие процессов между системами. Взаимодействие процессов начинается с установления сеанса, который служит основой для виртуального соединения между двумя системами.

**Уровень 4 – транспортный уровень (транспорт данных между оконечными узлами, протокол, ориентированный на соединение)**

Предоставляет услуги надежной передачи данных (за счет управления потоками и контроля ошибок) уровню 5 и вышележащим уровням.

**Уровень 3 – сетевой уровень (пакетная передача данных, адресация, фрагментация пакетов)**

Обеспечивает фактическую передачу данных, маршрутизируя и направляя пакеты данных между системами. Создает и администрирует таблицы маршрутизации и предоставляет средства для обмена данными через границы сетей. На этом уровне данным присваиваются адреса назначения и происхождения, которые используются для целенаправленной маршрутизации.

**Уровень 2 – Канальный уровень (кадры)**

Обеспечивает передачу данных и управляет доступом к среде передачи, объединяя данные в блоки, называемые кадрами. Уровень 2 делится на два подуровня; верхний из них соответствует логическому управлению соединениями (LLC), а нижний - доступом к среде передачи (MAC). LLC облегчает обмен данными, в то время как MAC управляет доступом к среде передачи.

**Уровень 1 – физический (битовый)**

Предоставляет услуги, поддерживающие передачу данных в виде потока бит через среду передачи, например, проводную или беспроводную сеть.

#### 5.2.1.2 Референсная модель TCP/IP

Референсная модель TCP/IP - это еще одна модель, позволяющая понять взаимодействие протоколов и процесс обмена данными. Референсная модель TCP/IP делится на четыре уровня, соответствие которых уровням модели OSI показано ниже.

*Таблица 5.1 Сравнение референсных моделей*

| Модель OSI | Модель TCP/IP |
|---|---|
| Уровень 7 – прикладной уровень | Уровень 4 – прикладной уровень |
| Уровень 6 - уровень представления | |
| Уровень 5 – сеансовый уровень | |
| Уровень 4 - транспортный уровень | Уровень 3 - транспортный уровень |
| Уровень 3 - сетевой уровень | Уровень 2 - межсетевой уровень |
| Уровень 2 – канальный уровень | Уровень 1 - уровень сетевого интерфейса |
| Уровень 1 - физический | |

### 5.2.2 Протоколы прикладного уровня

- **CIFS/SMB** (Common Internet File System/Server Message Block) – применяется в основном для предоставления совместного доступа к файлам, принтерам и последовательным портам и различных взаимодействий между узлами в сети.
- **DDNS** (Dynamic Domain Name System) – отслеживает связь имен доменов с меняющимися адресами IPv4
- **DHCPv4/v6** (Dynamic Host Configuration Protocol) – автоматическое назначение IP-адресов и управление ими
- **DNS/DNSv6** (Система доменных имен): преобразует имена доменов в связанные с ними IP-адреса.
- **FTP** (File Transfer Protocol) – используется в первую очередь для передачи файлов с сервера на клиент (скачивание) или с клиента на сервер (загрузка). Также может использоваться для создания и выбора каталогов и для переименования и удаления каталогов и файлов.

- **HTTP** (Hypertext Transfer Protocol) – используется в первую очередь для загрузки текста и изображений с Web-сайтов в Web-браузер. Сетевые системы видеонаблюдения содержат HTTP-сервер, предоставляющий доступ к системе через браузер для загрузки конфигурации и просмотра видеоизображения в реальном времени.
- **HTTP/2**: существенно пересмотренная версия протокола HTTP, определенная в RFC 7540 и выпущенная в феврале 2015 г.
- **HTTPS** (HTTP Secure) – адаптация протокола HTTP для защищенного обмена данными по компьютерной сети; широко используется в Интернете. В HTTPS протокол связи шифруется с использованием технологии TLS.
- **MQTT** (Message Queuing Telemetry Transport) — стандартный протокол обмена сообщениями для Интернета вещей (IoT). Разработан с целью упростить интеграцию IoT и используется в самых разных отраслях для подключения удаленных устройств с небольшим объемом кода и минимальными требованиями к пропускной способности сети.
- **NTP** (Network Time Protocol) – служит для синхронизации времени между клиентским или серверным компьютером и другим сервером.
- **RTP** (Real-Time Transport Protocol) – обеспечивает передачу данных в реальном времени между конечными точками системы.
- **RTCP** (Real-Time Control Protocol) – служит для обмена статистическими данными и управляющей информацией для RTP-сеанса. Вместе с RTP обеспечивает доставку и пакетирование мультимедийных данных, но сам не передает никаких мультимедийных данных.
- **RTSP** (Real-Time Streaming Protocol) – предоставляет расширенные возможности управления передачей мультимедийной информации в реальном времени.
- **SFTP** (Secure File Transfer Protocol) – предоставляет возможности доступа к файлам, передачи файлов и управления файлами поверх любого надежного потока данных.
- **SIP** (Session Initiation Protocol) – коммуникационный протокол для сигнализации и управления сеансами мультимедийной связи.
- **SIPS** (Session Initiation Protocol Secure): версия SIP с шифрованием.
- **SMTP** (Simple Mail Transfer Protocol) – стандартный протокол передачи сообщений электронной почты через Интернет. Сетевые камеры поддерживают SMTP для передачи уведомлений по электронной почте.
- **SNMPv1/v2/v3** (Simple Network Management Protocol): – протокол, применяемый для дистанционного мониторинга и управления подключенным к сети оборудованием - коммутаторами, маршрутизаторами, сетевыми камерами и др. Поддержка SNMP позволяет управлять сетевыми камерами при помощи инструментов с открытым кодом.
- **SOCKS**: обеспечивает обмен сетевыми пакетами между клиентами и серверами через удаленный сетевой прокси.
- **SRTP** (Secure Real-Time Transport Protocol): обеспечивает обмен зашифрованными данными в реальном времени между сетевыми конечными точками; защищенный вариант RTP.
- **SSH** (Secure Shell): позволяет защищенным образом управлять доступом к сетевым устройствам и отлаживать такой доступ через незащищенную сеть.

- **TLSv1.2/v1.3** (Transport Layer Security): – обеспечивает согласование надежного частного соединения между клиентом и сервером.

### 5.2.3 Протоколы транспортного уровня

- **TCP** (Transmission Control Protocol) – ориентированный на соединения, надежный, сохраняющий порядок протокол потоков данных. Самый распространенный протокол передачи данных.
- **UDP** (User Datagram Protocol) – служба передачи данных без установления соединения; отдает приоритет своевременности доставки данных перед надежностью.
- **ICMP** (Internet Control Message Protocol) – служит для передачи сообщений об ошибках и управляющей информации, указывающей, что затребованная услуга, хост или маршрутизатор недоступны.

### 5.2.4 Протоколы сетевого уровня

- **IGMPIGMPv1/v2/v3** (Internet Group Management Protocol) – используется хостами и соседними маршрутизаторами в сетях IPv4 для установления членства в группах многоадресного вещания; позволяет эффективнее использовать ресурсы при поддержке соответствующих приложений.
- **IPv4/IPv6** (Internet Protocol): протокол, обеспечивающий назначение индивидуальных публичных адресов, необходимых для обмена данными между Интернет-устройствами. IPv4 – исходная версия IP, использующая 32-разрядные адреса. IPv6 – современная версия IP, использующая 128-разрядные адреса, записываемые в виде восьми групп по четыре шестнадцатеричные цифры.
- **USGv6**: определенный правительством США профиль технических стандартов для IPv6 по защите данных, призванный обеспечить совместимость при закупке сетевого оборудования с поддержкой IPv6.

### 5.2.5 Протоколы канального уровня

- **ARP** (Address Resolution Protocol) – используется для определения MAC-адреса хоста назначения.
- **CDP** (Cisco Discovery Protocol): проприетарный протокол Cisco, используемый в качестве альтернативы LLDP для получения информации о подключенных аппаратных устройствах.
- **IEEE 802.3 (i, u, ab)**: стандарты Ethernet, определяющие передачу данных по кабелю типа "витая пара" со скоростью 10 Мбит/с (10Base-T), 100 Мбит/с (100Base-TX) и 1 Гбит/с (1000Base-T).
- **LLDP** (Link Layer Discovery Protocol) – используется для оповещения об идентификационных данных и возможностях устройства, а также других устройств, подключенных к этой же сети.

### 5.2.6 Протоколы обнаружения

- **mDNS (Bonjour)** – может использоваться для обнаружения сетевого видеооборудования компьютерами Mac, а также в качестве протокола обнаружения новых устройств в любой сети.
- **UPnP** (Universal Plug and Play) – используя этот протокол, операционные системы Microsoft могут автоматически обнаруживать ресурсы (например, оборудование Axis) в сети.
- **Zeroconf** – автоматическое выделение сетевым устройствам свободных IP-адресов в диапазоне от 169.254.1.0 до 169.254.254.255.

### 5.2.7 Quality of Service

В IP-сети необходимо контролировать совместное использование сетевых ресурсов для соблюдения требований к каждой услуге.

- **QoS** (Quality of Service - качество обслуживания) – способность устанавливать приоритеты сетевого трафика таким образом, чтобы особо важные потоки доставлялись раньше потоков с меньшим приоритетом. Повышает надежность сети, регулируя долю пропускной способности, которую может использовать конкретное приложение, и предоставляя возможность регулировать конкуренцию между приложениями за пропускной способностью.
- **DiffServ** – подход, при котором сеть предоставляет услуги с учетом данных QoS, указанных в каждом пакете.

### 5.2.8 Методы передачи данных

Существует три разных метода передачи данных по компьютерной сети.

- **Одноадресная передача** – наиболее распространенный метод, отправитель и получатель взаимодействуют по принципу "точка-точка". Пакеты данных направляются только одному получателю, никакие другие клиенты эту информацию не получают.
- **Многоадресная передача** – передача данных от одного отправителя множеству получателей в сети. Уменьшает сетевой трафик за счет передачи одного потока информации множеству получателей.
- **Широковещательная передача** – отправитель отправляет одну и ту же информацию всем другим серверам в сети; все хосты в сети принимают сообщение и каким-то образом обрабатывают его.

T10169734/RU/M1.10/2111

# О компании Axis Communications

Компания Axis вносит весомый вклад в формирование более разумного и безопасного мира, разрабатывая и внедряя сетевые решения, которые не только способствуют повышению безопасности, но и открывают новые пути ведения бизнеса. Занимая в отрасли ведущие позиции, компания Axis поставляет продукцию и оказывает услуги в сфере сетевого охранного видеонаблюдения и аналитики, контроля доступа, сетевых домофонов и звукового сопровождения. Свыше 3800 специалистов компании Axis трудятся более чем в 50 странах мира, вместе с нашими партнерами разрабатывая и внедряя решения стоящих перед нашими клиентами задач. Компания Axis была основана в 1984 году. Штаб-квартира компании находится в городе Лунд, Швеция.

Более подробную информацию о компании Axis можно найти на нашем веб-сайте *axis.com*.