# ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К УЗЛАМ ДОСТУПА СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ ПЕРИМЕТРА ТРАНСПОРТНОГО ПРЕДПРИЯТИЯ

***Озеров Евгений Игоревич***
*ведущий инженер-проектировщик слаботочных систем, автор Low-voltage Blog (eozerov.ru)*

Защита транспортных объектов от различного рода угроз – прежде всего террористических – непростая задача. Такого рода объекты имеют свою ярко выраженную специфику. Например, они занимают большую площадь и, как правило, имеют распределенную структуру.

Одной из задач, стоящих перед службами безопасности транспортных объектов, является мониторинг периметра и контрольно-пропускных пунктов (КПП). Для решения данной задачи могут использоваться технические средства: системы охраны периметра, телевизионного и тепловизионного наблюдения, досмотровое оборудование, системы контроля и управления доступом на КПП и др. Но не будем забывать и о «кровеносной» системе для всех перечисленных технических средств охраны периметра транспортных объектов – системе передачи данных. Именно система передачи данных связывает все распределенные на объекте технические средства в единое целое, доставляет информацию и команды до операторов службы безопасности, позволяет контролировать работоспособность отдельных узлов систем.

Сегодня поговорим об основной «единице» системы передачи данных – узле доступа или, по-другому, о шкафе системы передачи данных технических средств охраны (шкаф СПД ТСО).

Узел доступа представляет из себя всепогодный антивандальный шкаф, предназначенный для установки непосредственно на периметре защищаемого объекта. Основной «начинкой» является телекоммуникационное оборудование – как правило промышленный коммутатор уровня доступа по классификации Cisco Systems (технология Ethernet). Кроме того, узел доступа может быть укомплектован оборудованием защиты питающих линий и линий связи от скачков напряжения, грозовых разрядов и т.п.; оборудованием, поддерживающим требуемые климатические параметры внутри шкафа и др. оборудованием, о чем подробней поговорим чуть позже.

## СДЕЛАТЬ САМИМ ИЛИ КУПИТЬ ГОТОВЫЙ? ПЛЮСЫ И МИНУСЫ ДВУХ ПОДХОДОВ

Это один из первых вопросов, встающих перед интегратором, получившим подряд на оборудование транспортного предприятия системой передачи данных на периметре. Если ответить очень кратко, то чем крупнее объект, тем предпочтительнее «заложить» в проект готовый узел доступа. Рассмотрим плюсы и минусы обоих подходов.

### 1. РАЗРАБАТЫВАЕМ И СОБИРАЕМ УЗЕЛ ДОСТУПА САМОСТОЯТЕЛЬНО

**Достоинства:**

*Наиболее гибкий подход.* Вы самостоятельно выбираете номенклатуру используемого оборудования, арматуры и материалов, состав узла доступа, его основные тактико-технические характеристики.

*Отсутствие избыточности.* Так как, по сути, каждый шкаф разрабатывается и собирается индивидуально, вы включаете в его состав лишь необходимые элементы.

**Недостатки:**

*Сложность разработки.* В состав проектной и рабочей документации на систему передачи данных необходимо будет включить конструкторскую документацию на типовые узлы доступа. Это требует наличия соответствующей компетенции у проектировщика.

*Сложность грамотного и сбалансированного подбора «начинки» шкафа.* Дело в том, что общая надежность проектируемого узла доступа не может превышать надежность самого «слабого» элемента, входящего в его состав. Приведу пример. Вы можете включить в состав узла доступа промышленный коммутатор Industrial Ethernet с наработкой на отказ (MTBF)

в 250 000 часов и температурным диапазоном от –40 до +85° С, но если к нему подключен Input/Output (I/O) Ethernet модуль с наработкой на отказ (MTBF) в 20 000 часов и температурным диапазоном от –30 до 50° С, то коэффициент готовности узла доступа для функции диспетчеризации и необходимый для работы климатический режим внутри шкафа будет определяться именно IO Ethernet модулем – 20 000 MTBF и от –30 до +50° С. Значит деньги на промышленный коммутатор потрачены избыточные. Необходимо либо выбрать коммутатор «попроще», либо IO Ethernet модуль «покруче».

*Сложность «закупки» компонентов.* Как уже упоминалось в самом начале статьи, транспортные объекты, как правило, достаточно «протяженные». А значит, количество узлов доступа может исчисляться десятками (по моему опыту – не менее 5 на километр). И тут начинаются проблемы при закупке компонентов разработанного узла доступа. Банально могут подвести сроки поставки, а на складе вашего поставщика отсутствовать требуемое количество номенклатуры части изделий, входящих в состав шкафа. Придется производственно-техническому отделу пересогласовывать с проектным отделом альтернативу на отсутствующие позиции. Кроме того, при этом может возникнуть «пересортица». Не говоря уже о сложности администрирования и документирования данных процедур.

*Сложность самостоятельной «сборки» узлов доступа.* По сути, вам будет необходимо либо наличие достаточного количества квалифицированного персонала, специально оборудованных помещений под сборку. Либо наличие партнеров, готовых взять данную задачу «на аутсорс» и располагающих для этого необходимыми ресурсами.

*Сложность контроля качества.* Понятно, что узел доступа мало просто собрать по конструкторской документации. Надо еще протестировать работоспособность всех функций и проконтролировать качество сборки. Это отдельная, трудоемкая, требующая наличия оборудования и очень квалифицированного персонала задача.

*Логистика.* При самостоятельной разработке и сборке узла доступа вам придется решить еще и непростую задачу логистики. Что проще? Собрать шкаф «дома» и везти на объект «вместе с воздухом» либо организовать сборку из комплектующих на самом объекте. Вам придется хорошенько подумать над данным вопросом.

## 2. ПОКУПАЕМ УЗЕЛ ДОСТУПА КАК ГОТОВОЕ ИЗДЕЛИЕ

**Достоинства:**

*Экономия ресурсов на проектирование.* Можно «не заморачиваться» начинкой узла доступа – для проектировщика это просто функциональный блок с набором параметров (количество портов Ethernet, UpLink портов, максимальная дистанция передачи данных, тип установленного в шкафе кросса и т.п.). Таким образом, квалификация проектировщика может быть ниже без ущерба качеству проекта. Также снижается время на проектирование.

*Разделение ответственности.* Вы делегируете ответственность за качество разработки, сборки и тестирования узла доступа производителю. При данном подходе – это его зона ответственности.

*Упрощение вопросов логистики.* Вы можете договориться с производителем о доставке нужного количества узлов доступа непосредственно на объект, сняв с себя эту головную боль.

**Недостатки:**

*Ограниченный выбор.* На российском рынке не так много производителей готовых узлов доступа. И, как правило, они предлагают устанавливать только свое сетевое оборудование. Привыкли работать с другим? Ничего не поделаешь…

*Меньшая гибкость решения.* Хотели «запихнуть» в тот же шкаф еще и IO-модули для сбора «сухих контактов» от ППКП-системы охраны периметра? И туда же устанавливать контроллеры СКУД для управления шлагбаумами, турникетами и калитками КПП? Увы, если это не предусмотрено конкретной моделью узла доступа – вы вряд ли сможете это сделать. Впрочем, можно попробовать договориться с производителем о внесении соответствующих изменений в конструктив, если ваш заказ достаточно интересен – шансы на это не такие уж маленькие.

## ОСНОВНЫЕ ЭЛЕМЕНТЫ УЗЛА ДОСТУПА. СОСТАВ ОБОРУДОВАНИЯ

Какое оборудование и арматура может входить в состав типового узла доступа системы передачи данных?

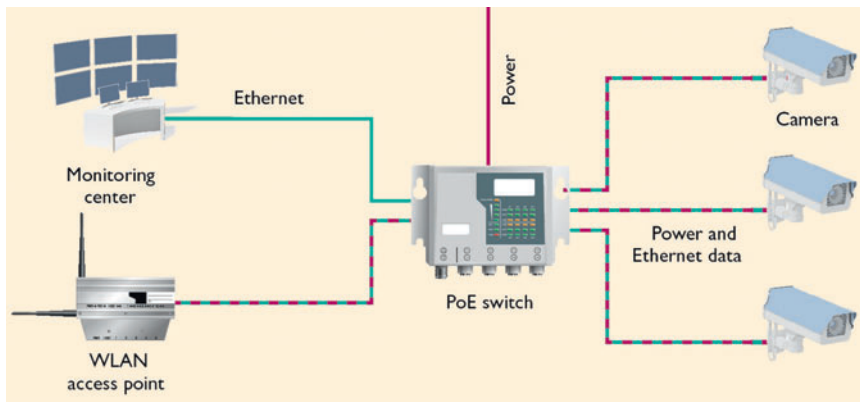
1. **Шкаф монтажный** (термошкаф).
2. **Различная арматура шкафа** – кабельные вводы (гермовводы) и фитинги либо герметичные разъемы для непосредственного подключения питающих и телекоммуникационных кабелей; элементы крепления шкафа (на опору, на стену, напольное основание); монтажная плата для крепления оборудования внутри шкафа; кронштейн крепления 19" оборудования; Din-рейка; короб перфорированный для прокладки кабелей внутри шкафа; кабель-канал гибкий для перехода на дверь; запирающее устройство; козырек или навес от дождя; внутренний светильник и др.
3. **Климатическое оборудование шкафа** – термостат внутрищитовой; обогреватель внутрищитовой; вентилятор.
4. **Силовое оборудование шкафа** – выключатели автоматические; силовые клеммы; шина заземления; блоки питания; система бесперебойного питания; PoE-инжекторы; электрическая розетка для обслуживания и др.
5. **Грозозащита** линий электропитания, оборудования и линий связи и передачи данных.
6. **Оборудование передачи данных** – оптический кросс; промышленный коммутатор с установленными SFP-модулями; патчкорды и шнуры оптические соединительные и др.
7. **Оборудование для мониторинга состояния узла доступа** – концевой выключатель для контроля открытия шкафа; Ethernet-I/O модуль для подключения «сухих контактов» от датчиков, блока питания, термостата и др.

## ТРЕБОВАНИЯ К МОНТАЖНОМУ ШКАФУ И АРМАТУРЕ ШКАФА

На что обратить внимание:

- степень защиты оболочки (Ingress Protection Rating) – не ниже IP55;
- степень защиты корпуса от внешних механических воздействий (IEC 62262:2002) – желательно IK10;
- наличие термоизоляции корпуса шкафа;
- габариты шкафа (типоразмер);
- вес;
- наличие креплений шкафа на опору, стену, напольное основание;
- наличие кабельных вводов (гермовводов) и фитингов либо герметичных разъемов для непосредственного

**Схема подключения**



**Пример начинки шкафа**

подключения питающих и телекоммуникационных кабелей;
- организацию внешних и внутренних подключений – наличие разъемов, клемм, модулей типа Keystone, а также кабельных органайзеров, гибких переходов на дверцу (при наличии на ней оборудования) и т.п. (Электроника – наука о контактах. И они должны быть выполнены надежно.);
- наличие аксессуаров (козырьки, замки и т.п.).

Обращаю ваше внимание на необходимость применять только герметичные уличные антивандальные шкафы, очень желательно с термоизоляцией корпуса (IP55 IK10 – необходимый минимум!). Естественно, что ввод кабелей также не должен понижать степень защиты IP всего шкафа. Необходимо использовать герметичные вводные устройства для всех видов кабелей, как силовых, так и слаботочных и оптических.

Важно не экономить на удобстве организации кабельных соединений внутри шкафа и удобстве внешних подключений. В конечном итоге это отразится на эксплуатации и ремонтопригодности узла доступа. Идеальный вариант для внешних подключений – использование герметичных разъемов, смонтированных непосредственно на корпус шкафа. Это позволит минимизировать ошибки подключения при пусконаладке и практически исключит необходимость «лезть» в сам шкаф, что очень хорошо для обслуживания. Узел доступа в таком случае – по-настоящему законченное изделие, «черный ящик». Подвели кабели, оконцевали их соответствующими вилками, подключили к соответствующим розеткам – и все! Далее – удаленная настройка.

**Установка шкафа**

## ТРЕБОВАНИЯ К КЛИМАТИЧЕСКОМУ ОБОРУДОВАНИЮ УЗЛА ДОСТУПА

На что обратить внимание:
- диапазон рабочих температур;
- мощность обогревателя, напряжение питания для обогрева;
- наличие вентилятора;
- наличие функции аварийного отключения аппаратуры термостатом;
- диапазон регулирования температуры включения/отключения обогрева;
- диапазон регулирования температуры аварийного отключения/включения аппаратуры.

В конечном счете, требования зависят от климатических условий и особенностей самого объекта.

## ТРЕБОВАНИЯ К СИЛОВОМУ ОБОРУДОВАНИЮ УЗЛА ДОСТУПА

На что обратить внимание:
- соблюдение требований ПУЭ;
- линии питания должны быть защищены от перегрева (токи к.з. и т.п.) автоматическим выключателем;
- сам монтажный шкаф и внутреннее оборудование должны быть заземлены в соответствии с рекомендациями производителей;
- для блока питания: тип исполнения (желательно, чтобы он был промышленным); мощность; выходные параметры напряжения и тока; диапазон входных рабочих напряжений; диапазон рабочих температур;
- для системы бесперебойного питания с АКБ: емкость батарей Ач; диапазон рабочих температур;
- для PoE-инжекторов: выходные параметры напряжения и тока; диапазон входных рабочих напряжений; диапазон рабочих температур; поддержка стандартов IEEE 802.3af (PoE), 802.3at (PoE+), IEEE 802.3 (Ethernet), IEEE 802.3u (Fast Ethernet), IEEE 802.3ab (Gigabit Ethernet);
- наличие электрической розетки для удобства обслуживания.

Небольшое замечание: внимательно смотрите на классы потребления мощности питаемых устройств по PoE. В некоторых случаях целесообразно заложить в проект отдельные уличные блоки питания для подключения периферийного оборудования непосредственно рядом с этим оборудованием – например, камер телевизионного, тепловизионного наблюдения и ИК прожекторов. А не пытаться запитать все от коммутатора (PoE switches), расположенного в узле доступа.

## ТРЕБОВАНИЯ К ГРОЗОЗАЩИТЕ УЗЛА ДОСТУПА

На что обратить внимание:
- внутреннее оборудование узла доступа должно быть защищено от перенапряжений, возникающих во внешних линиях электропитания и линиях передачи данных, в том числе во время близких грозовых разрядов;
- класс устройства защиты от импульсных перенапряжений (УЗИП);
- диапазон рабочих температур.

Не стоит пренебрегать грозозащитой узла доступа. Отсутствие грозозащиты ставит под большое сомнение общую надежность системы передачи данных, а значит, и всего комплекса мер по защите транспортного объекта. Важно, чтобы грозозащита была комплексной, а наличие перенапряжений на внешних кабелях не приводило к выходу из строя элементов узла доступа.

## ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ ПЕРЕДАЧИ ДАННЫХ

На что обратить внимание:
- тип коммутатора: управляемый или не управляемый (уровень сетевого управления не оговариваем – понятно, что для узла доступа на периметре достаточно коммутации второго уровня модели OSI – L2);
- количество RJ45 портов Fast и Gigabit Ethernet;
- количество RJ45 портов с поддержкой управляемого PoE (по стандарту IEEE 802.3af) и PoE+ (по стандарту IEEE 802.3at); максимальная поддерживаемая мощность на каждый порт и общая мощность PoE на коммутатор в поддерживаемом температурном диапазоне;
- количество Fiber Ports Fast и Gigabit Ethernet;
- поддерживаемые SFP модули: для одномодового (тип ITU-T G.652, ITU-T G.653 и ITU-T G.655) или многомодового волокна; тип оптического коннектора (LC, SC, FC, ST); типы полировки коннектора (PC, UPC, SPC, APC);
- поддержка multicast трафика (IGMP snooping и GMRP);
- поддержка VLAN (IEEE 802.1Q, GVRP);

- поддержка QoS (IEEE 802.1p/1Q) и TOS (DiffServ);
- поддержка IPv6 (IPv6 Logo Committee certified);
- поддержка DHCP (что впрочем спорно, но лучше когда есть выбор);
- поддержка Ethernet/IP, PROFINET и Modbus/TCP протоколов для управление устройствами и мониторинга;
- поддержка SNMP (v1, v2c, v3) для различных уровней управления сетью;
- поддержка разных топологий сети (кольцо; звезда; двойное кольцо; два кольца, соединенных в двух точках, – Dual-homing, Ring coupling);
- время восстановления после единичного обрыва (время сходимости) для кольца/цепочки из 250 коммутаторов;
- поддерживаемые протоколы «аппаратного ускорения» сходимости (Ethernet ring protocols);
- значение MTBF (Mean Time Between Failures) – средней наработки на отказ (обычно не менее 200 000 часов);
- рабочее напряжение, ток, потребляемая мощность коммутатора;
- диапазон рабочих температур;
- тип монтажа (на Din-рейку, в 19" стойку/корзину);
- соответствие требованиям стандартов (в том числе отраслевых и международных) – таким как NEMA TS2, EN 50155, EN 50121;
- наличие сертификатов (в том числе отраслевых и международных) – таких как сертификат по общей безопасности UL 60950, CE, по промышленной безопасности UL 508 и т.п.;
- срок гарантии.

Узел доступа – это прежде всего коммутатор. Все остальное вторично, хотя и также очень важно. К выбору коммутатора нужно подойти максимально ответственно. Коммутатор должен быть промышленного исполнения. Желательно управляемый (L2 для «маркировки» VLAN-ов и разделения трафика от разных систем), надежный (MTBF не менее 200 000 часов).

Кроме того, хочу обратить ваше внимание на достаточно важный момент, который можно упустить из виду. А именно – на подержку Ethernet ring protocols коммутатором. Очень желательно использовать Ethernet ring protocols при построении отказоустойчивой архитектуры системы передачи данных на периметре транспортных объектов. Есть два важных момента. Во-первых, не стоит использовать в этом качестве стандартные протоколы RSTP и IGMP – они не оптимизированы для использования с критическими узлами таких важных на периметре систем, как телевизионное и тепловизионное наблюдение. Пока стандартный протокол среагирует на возникновение точки отказа, передача видеопотока может быть остановлена на срок до двух минут, что в данном случае не приемлемо. И второй момент. Сравнивая проприетарные Ethernet ring protocols разных производителей по параметру «время сходимости» после единичного обрыва/отказа коммутатора в кольце/цепочке, всегда задавайте вендорам вопрос, для какого количества коммутаторов оно указано. Если производитель гарантирует время сходимости в несколько десятков миллисекунд для цепочки или кольца из 250 коммутаторов – то все в порядке, это современное и рабочее решение.

## ТРЕБОВАНИЯ К МОНИТОРИНГУ СОСТОЯНИЯ УЗЛА ДОСТУПА

На что обратить внимание:

- мониторинг доступа к «начинке» шкафа при обслуживании – контролируем состояние концевого выключателя;
- мониторинг температуры внутри шкафа – контролируем переключения термостата либо отдельный датчик температуры;
- мониторинг электропитания узла доступа – как минимум, о наличии вводного напряжения сети, напряжения на выходе блока питания БП или ИБП, напряжения на аккумуляторной батареи (для ИБП) и о переходе на питание от аккумуляторов;
- мониторинг работы коммутатора (SNMP) и других сетевых устройств.

Смысл мониторинга – понимать, что происходит с узлом доступа для принятия необходимых мер по устранению возникающих неисправностей и обеспечению живучести системы передачи данных на периметре транспортного объекта.

## ЗАКЛЮЧЕНИЕ

*Конечно, в рамках статьи невозможно обсудить все возможные нюансы выбора узла доступа системы передачи данных на периметре. Это достаточно сложная и объемная тема, требующая обязательного изучения в процессе проектирования системы передачи данных на периметре. Тем не менее, я надеюсь, что данный материал послужит для вас полезным «чек-листом» в данной теме и даст некоторые ориентиры, какие вопросы стоит проработать техническим специалистам интегратора. Главное – внимание к деталям!*