

# ЕДИНЫЙ СПЕЦИАЛИЗИРОВАННЫЙ ОБЪЕКТОВЫЙ ПРОТОКОЛ – ПОВЫШЕНИЕ ИНФОРМАТИВНОСТИ ДЛЯ ЦЕНТРАЛИЗОВАННОЙ ОХРАНЫ

*Борисов Сергей Петрович  
Фамильнов Александр Рудольфович  
ФКУ «НИЦ «Охрана» Росгвардии*

**Н**емаловажную роль для проведения необходимых действий и мероприятий службой вневедомственной охраны Росгвардии при осуществлении функции мониторинга охраняемых объектов играет получение оперативной, оптимальной, лаконичной и понятной информации, поступающей от технических средств охраны. Одним из путей повышения эффективности этого процесса является получение в пунктах централизованной охраны (далее – ПЦО) полной информации с охраняемого объекта за счет увеличения информативности сообщений.

Для его реализации требовалось устранить дисбаланс между высокими информационными возможностями оборудования систем централизованной охраны и теми малочисленными сообщениями, которые формируют объектовые средства охраны (извещатели).

Большинство устанавливаемых сегодня извещателей генерируют извещение о тревоге для передачи на устройство оконечное объектовое (далее – УОО) либо прибор приемно-контрольный охраняемых помещений (далее – ПКПО) следующими способами:

- замыканием (размыканием) контактов реле («сухие контакты»);
- увеличением тока потребления извещателей, питающихся по шлейфу.

При этом, такой способ передачи извещений требует для каждого выхода извещателя отдельный шлейф. Поэтому, как правило, извещений передается не более двух. Низкая информативность приводит к неоднозначности определения дальнейших действий группы реагирования.

Для организации гибкой системы охраны, способной полноценно использовать всю номенклатуру имеющихся на рынке охранных извещателей, необходимо применять унифицированный протокол. В этом случае появляется возможность передачи информации как оперативного назначения, так и сервисного. Например, год изготовления прибора, его характеристики, активные настройки и другая информация, необходимая для обслуживания объекта. Это позволит оперативно проводить замену выработав-

ших свой ресурс извещателей и источников вторичного питания (ИВП), а также облегчит диагностику неисправностей и определение причин ложных тревог.

Данные задачи были решены ФКУ «НИЦ «Охрана» Росгвардии в рамках создания Единого специализированного объектового протокола (далее – ЕСОП) систем централизованного наблюдения (СЦН), который обладает следующими преимуществами:

- обеспечивает унификацию интерфейсов объектовых технических средств охраны (далее – ТСО) различных производителей;
- повышает уровень информативности с возможностью точной локализации и определения характера происшествия (проникновение, неисправность, саботаж и др.);
- обеспечивает высокий уровень защиты от подмены или саботажа ТСО, в том числе в период снятия объекта с охраны, благодаря использованию устойчивого к взлому алгоритма шифрования;
- предоставляет возможность получения в ПЦО полной информации о состоянии средств охранной сигнализации, а также сведений о сертификате подлинности, дате изготовления и введения в эксплуатацию, проверке функционирования и наименования ТСО.

ЕСОП является реализацией интерфейса объектового и интерфейса подсистемы передачи информации по ГОСТ Р 56102.1 «Системы централизованного наблюдения. Часть 1. Общие положения» и регламентирует взаимодействие между УОО, с одной стороны, и подключенными к ним отдельными ТСО или охранными подсистемами с другой стороны. Таким образом, ЕСОП обеспечивает передачу необходимой информативности между объектовой подсистемой СЦН и подсистемой передачи информации СЦН. При этом внутренние протоколы подсистем передачи информации СЦН и охранных подсистем, установленных на объектах для функционирования в составе СЦН, построенных на ЕСОП, должны обеспечить только совместимость информативности.

## ПРОГРАММНО-АППАРАТНАЯ ЧАСТЬ УОО

Основными функциями УОО, при использовании ЕСОП, являются управление техническими средствами охраны и модулями объектовой подсистемы, объединенными на программно-аппаратном уровне в единую объектовую сеть, прием от них информации, ее обработка и передача на ПЦН. Информационная емкость – количество устройств объектовой сети (УОС) в основной объектовой сети для УОО, передающих извещения по цифровым каналам связи, должна быть не более 254. Устройствами, входящими в объектовую сеть, могут являться:

- объектовые приборы – УОО, ППКО и ППКОП;
- извещатели (охранные, тревожные, пожарные, технологические);
- расширители сети – для подключения устройств, объединенных в сеть нижнего уровня (подсеть), недоступных для прямых запросов с УОО;
- преобразователи интерфейсов – для подключения устройств, имеющих отличные от ЕСОП физические и логические протоколы обмена;
- источники вторичного электропитания;
- считыватели, клавиатуры и шифроустройств;
- дисплеи, световые и звуковые оповещатели.

Извещения, принимаемые УОО от УОС и передаваемые на ПЦН, сгруппированы в 9 классов в зависимости от их характера, физической сущности и предназначения. Классы извещений представлены в порядке убывания их приоритета передачи информации на ПЦН:

1. «ТРЕВОГА» – тревожные события;
2. «ВНИМАНИЕ» – сообщения о возможной, неподтвержденной тревоге;
3. «САБОТАЖ» – сообщения о действиях по выводу системы из строя;
4. «НЕИСПРАВНОСТЬ» – сообщения о неисправностях;
5. «ВЗЯТИЕ/СНЯТИЕ» – сообщения о взятии/снятии зон и разделов под охрану/с охраны;
6. «УПРАВЛЕНИЕ» – сообщения об активных действиях пользователей;
7. «ПИТАНИЕ» – извещения о состоянии источников питания;
8. «СВЯЗЬ» – сообщения о состоянии каналов связи;
9. «ИНФОРМАЦИЯ» – информационно-диагностические сообщения.

И для каждого класса извещений существует от 15 до 20 видов извещений. Так, например, в классе «ТРЕВОГА» могут формироваться следующие извещения: «Тревога ШС», «Короткое замыкание ШС», «Обрыв ШС», «Выход за пределы контролируемого параметра», «Превышение контролируемого параметра», «Снижение контролируемого параметра», «Тревога

ручная», «Принуждение», «Тихая тревога», «Внешняя тревога», «Внутренняя тревога», «Тревога входа», «Тревога, проникновение», «Тревога, перемещение», «Пожар», «Тревога, высокая температура», «Тревога, низкая температура», «Дым», «Пламя», «Тревога, газ», «Тревога, затопление».

При этом общая информативность УОО с учетом всех классов составляет более 90 видов извещений, что на порядок больше информативности широко используемых в настоящее время устройств.

Типы зон объектовой сети должны в общем случае соответствовать типам подключаемых к сети устройств и могут иметь различные наименования: охранные; пожарные; технологические; измерительные; управления; исполнительные; информационные; оповещательные; питания.

## ФУНКЦИИ УОО В АВТОМАТИЧЕСКОМ РЕЖИМЕ

УОО должно обеспечивать в автоматическом режиме выполнение следующих функций:

- автоматически либо в ручном режиме по командам электромонтера, в зависимости от качества и длины линии связи, устанавливать скорость приема/передачи данных с УОС из следующего ряда: 115200 бит/с, 57600 бит/с, 38400 бит/с, 19200 бит/с и 9600 бит/с;
- оценивать качество связи в объектовой сети посредством подсчета количества сбоев за определенное время или количества циклов опроса УОС;
- поиск, идентификацию и регистрацию нового подключенного УОС;
- назначение УОС порядковых внутрисетевых адресов, которые будут использоваться в дальнейшем при организации циклического опроса;
- процедуру обмена ключами шифрования с УОС;
- понижать/повышать скорость передачи данных при наличии сбоев, ухудшении/улучшении качества связи в объектовой сети как для всех, так и для каждого УОС в отдельности. Параметры критериев, по которым происходит изменение скорости, должны быть настраиваемыми (сбоем следует считать необходимость в любой повторной передаче данных);
- устанавливать взаимно однозначное соответствие введенных по командам с ПЦН/с клавиатуры номеров зон УОС их сетевым адресам и сохранять эту информацию в виде табличных форм либо другим способом в энергонезависимой памяти;
- по командам с автоматизированного рабочего места дежурного пульта управления (АРМ ДПУ) либо командам электромонтера выполнять объе-

динение зон в произвольном порядке в логические группы – разделы (общее количество разделов основной сети не должно превышать 126, каждая зона объектовой сети должна входить в один раздел и не более);

- перед сдачей УОО под охрану по команде пользователя производить проверку состояния устройств объектовой сети и выводить на индикаторы либо дисплей информацию о готовности/неготовности объекта;
- осуществлять приоритетную, по отношению к другим событиям, передачу на ПЦН извещений о тревоге/пожаре;
- выполнять шифрование двумя ключами: 32-битным сеансовым и 128-битным постоянным всех внутрисетевых команд и запросов к устройствам;
- выполнять шифрование передаваемых сообщений, полученных от устройств объектовой сети на ПЦН, динамически изменяемыми ключами шифрования.

## ИНТЕРФЕЙС

УОО должно обеспечивать поддержку физического, транспортного и прикладного уровня ЕСОП.

Для поддержки объектового протокола на аппаратном уровне УОО должны иметь в своем составе микросхемы – приемо-передатчики и разъемы, необходимые для организации адресного шлейфа сигнализации типа «Кольцо» на основе спецификации интерфейса RS 485 (EIA 485).

В УОО должен быть реализован механизм программно-аппаратного определения короткого замыкания и обрыва линий связи объектовой сети с выдачей на АРМ ДПУ и устройства индикации соответствующих извещений.

## ВЫЧИСЛИТЕЛЬНЫЕ РЕСУРСЫ

УОО должны обладать необходимыми вычислительными ресурсами и объемом оперативной памяти, обеспечивающими выполнение всех функций по управлению объектовой сетью, обмен информацией с УОС и ПЦН. Кроме того, они должны быть оснащены модулем энергонезависимой памяти, предназначенным для хранения следующей информации:

- извещений, принятых от устройств объектовой сети после нарушении всех каналов связи с ПЦН (далее – архив событий);
- идентификаторов устройств и их адресов;
- конфигурационной информации о составе объектовой сети;
- сетевых параметров, необходимых для связи с ПЦН;
- закрытого ключа шифрования.

Емкость архива событий должна позволять хранение в энергонезависимой памяти не менее 3 извещений для каж-

дого устройства сети. При переполнении буферов архива извещения в нем заменяются на вновь полученные в зависимости от их приоритетности.

### УПРАВЛЕНИЕ И ОТОБРАЖЕНИЕ ИНФОРМАЦИИ

Для конфигурирования объектовой сети, ввода параметров устройств, а также команд управления ими, УОО должны иметь устройства управления. В качестве устройства управления предлагается использовать встроенную либо внешнюю, подключаемую по протоколу ESOП либо иным стандартным интерфейсам (RS 232, RS 485, CAN, Wi-Fi и т. д.) клавиатуру, мобильные телефоны и планшетные компьютеры и прочие устройства.

Управление процессами взятия/снятия под охрану/с охраны зон/разделов УОО может осуществляться с клавиатуры при помощи ключей Touch Memoгу, защищенных от копирования типа DS1961 либо DS1963, Proximity-карт, а также различных вещественных идентификаторов, в том числе и биометрических.

УОО должно обеспечивать визуальное отображение состояний подключенных УОС посредством выносных устройств индикации, которые могут входить в состав объектовой сети, кроме того, они могут иметь исполнения со встроенным графическим или Touch Screen дисплеем. Наличие визуального отображения состояний подключенных УОС позволит упростить процедуры конфигурирования устройств в объектовой сети, проведение собственником контроля исправности сигнализации перед сдачей под охрану.

По командам пользователя, набранным с клавиатуры либо командам оператора с АРМ ДПУ УОО должно запрашивать

устройства объектовой сети об их текущем состоянии, а также получать полную информацию (расширенный запрос) об устройствах, выводить ее на дисплей либо передавать на ПЦН.

Доступ к функциям по управлению взятием/снятием УОС и конфигурированию самого устройства и объектовой сети предусмотрен посредством использования паролей (секретных кодов), введенных на этапе ввода его в эксплуатацию. Должны быть предусмотрены и условные уровни доступа: электромонтер; инженер ПЦО; пользователь.

Инженеру ПЦН и электромонтеру рекомендуется предоставление сервисных функций.

Пользователю рекомендуется предоставлять права взятия/снятия разделов и зон объектовой сети и всего объекта в целом под охрану/с охраны, изменение своего пароля, запрос состояния УОС, разрешенных ему для взятия под охрану. УОО должно блокировать постановку под охрану по команде пользователя при неготовности соответствующих разделов/зон объектовой сети или отсутствии связи с ПЦН.

Опционально в УОО предусмотрен режим автономной охраны, в настройках устройства может присутствовать опция, разрешающая постановку под охрану при отсутствии связи с ПЦН.

### КОНФИГУРИРОВАНИЕ И СЕРВИСНЫЕ ФУНКЦИИ

По командам с клавиатуры либо ПЦН в память УОО можно заносить следующие параметры:

- коды пользователя;
- код инженера;
- коды принуждения;
- номера зон устройств сети;
- номера разделов сети;

- адрес основного и резервного сервера ПЦН;
  - строки с наименованием точек доступа для режима GPRS;
  - сетевой статический IP-адрес УОО;
  - маску сети;
  - IP-адрес шлюза;
  - значения временных задержек на вход;
  - значения временных задержек на выход;
  - настройки режимов работы управляющих выходов (реле).
- Отдельно стоит выделить доступные сервисные функции для инженера ПЦО и электромонтера:
- регистрация и удаление устройств объектовой сети;
  - просмотр состояния устройств;
  - установка полномочий пользователей по взятию/снятию зон и разделов;
  - сброс параметров устройств на заводские установки;
  - просмотр и очистка архива событий;
  - загрузка обновления программного обеспечения УОО.

### ЗАКЛЮЧЕНИЕ

*В документе «Единые требования к системам передачи извещений и объектовым техническим средствам охраны, предназначенным для применения в подразделениях вневедомственной охраны полиции», утвержденном ГУВВ от 25.03.2016 установлено, что вновь разрабатываемые объектовые технические средства должны обеспечивать возможность информационного обмена по ESOП, а вновь разрабатываемые СПИ должны обеспечивать возможность информационного обмена с объектовыми техническими средствами по ESOП и передавать всю необходимую информацию на ПЦН ПЦО подразделения вневедомственной охраны.*

## ИЗМЕНЕНИЯ В ТЕХНИЧЕСКИЙ РЕГЛАМЕНТ РФ ПО ПОЖАРНОЙ БЕЗОПАСНОСТИ

30 июля 2017 года вступил в силу и был опубликован федеральный закон № 244-ФЗ от 29.07.2017 «О внесении изменений в Федеральный закон «Технический регламент о требованиях пожарной безопасности». Федеральным законом предусмотрено:

- Утверждение требования о проведении идентификации объектов защиты по пожарной и взрывопожарной опасности.
  - Принятие возможности проведения идентификации органом по сертификации, в обязательном порядке аккредитованным в соответствии с законодательством РФ об аккредитации в национальной системе аккредитации.
  - Выделение объектов культурного наследия религиозного значения в новый класс функциональной пожарной опасности – Ф3.7.
  - Исключение положения о запрете уменьшения противопожарных расстояний между жилыми, общественными зданиями, спортивными и детскими площадками при условии сооружения противопожарных преград.
- Технический регламент дополнен статьей 6.1 «Идентифика-

ция объектов защиты», согласно которой идентификация производственного объекта, здания и сооружения производится путем установления их соответствия таким признакам:

- 1) класс функциональной пожарной опасности;
- 2) класс конструктивной пожарной опасности, степень огнестойкости;
- 3) категория наружных установок по пожарной опасности, категория зданий, сооружений и помещений по пожарной и взрывопожарной опасности.

Обращаем внимание, что документ вступил в силу не в полном объеме. Только с 31 июля 2018 года начнет действовать положение о том, что в отношении объектов культурного наследия религиозного назначения требования пожарной безопасности устанавливаются соответствующим нормативным документом. 24 июля 2017 года был опубликован технический регламент Евразийского экономического союза «О требованиях к средствам обеспечения пожарной безопасности и пожаротушения». Документ вступает в силу 1 января 2020 года.