С.В. Агеев, М.В. Носов
(ВНИИ ГОЧС МЧС России, Академия гражданской защиты МЧС России;
e-mail: asvaser@yandex.ru)

МЕТОДИЧЕСКИ ОСНОВЫ ТРЕБОВАНИЙ К СИСТЕМАМ ОПОВЕЩЕНИЯ О ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

Авторы предлагают методические основы определения оперативно-технических требований к системам оповещения о чрезвычайных ситуациях.

Ключевые слова: система оповещения, гражданская защита, своевременность, достоверность, надёжность, живучесть, помехоустойчивость, безопасность, техническое обслуживание.

S.V. Ageev, M.V.Nosov

METHODICAL BASES OF REQUIREMENTS TO SYSTEMS TO ALERT ABOUT EMERGENCIES SITUATIONS

The authors suggest methodical basis for determining the operational and technical requirements to systems to alert about emergencies situations.

Key words: alert system, civil protection, timeliness, portability, reliability, durability, noise immunity, security, maintenance.

1. Введение

Для своевременного оповещения органов управления ***Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС)*** и населения об угрозе возникновения ЧС в мирное и военное время применяются ***системы оповещения (СО)***, которые прошли определенный путь развития: от местных систем оповещения до систем централизованного оповещения государственно-административных образований РФ и потенциально-опасных объектов.

В настоящее время наступил новый этап развития СО, который обусловлен:

- необходимостью замены морально и физически устаревших аналоговых систем оповещения на цифровые;
- возрастающей интенсивностью техногенных и природных ЧС;
- изменениями в государственно-административном делении РФ;
- необходимостью создания на всех ***потенциально опасных объектах (ПОО)*** локальных систем оповещения и другими факторами.

В связи с этим возникает необходимость уточнения существующих оперативно-технических требований к СО с учётом их предстоящей модернизации на основе цифровых ***технических средств оповещения (ТСО)*** и информирования населения.

Оперативно-технические требования (ОТТ) к системам оповещения используются на всех этапах жизненного цикла: проектирования и создания, ввода в эксплуатацию, постановки на постоянную эксплуатацию.

В соответствии с ГОСТом 34.602-89, ОТТ к СО целесообразно подразделить на следующие категории:

- по показателям назначения систем оповещения;
- к эффективности и безопасности функционирования;
- по техническому обслуживанию и метрологическому обеспечению;
- по стандартизации и унификации ТСО и программного обеспечения;
- финансово-экономические требования.

2. Требования по показателям назначения

2.1. Задачи системы оповещения населения

Система оповещения населения (СОН) является составной частью соответствующих систем управления ***гражданской обороны (ГО)*** и РСЧС, строится по радиально-узловому принципу в соответствии с административно-территориальным делением РФ и представляет собой иерархическую структуру, включающую пять уровней оповещения: федеральный, межрегиональный, региональный (территориальный), местный и объектовый.

Оперативные дежурные службы любого звена оповещения должны иметь возможность оповещать объекты (организации) и население находящиеся в зоне ответственности этих дежурных служб. В случае выхода из строя СО промежуточного или нижнего уровня, дежурная служба более высокого уровня должна иметь возможность оповещения абонентов более низкого уровня.

Системы оповещения всех уровней должны обеспечивать как централизованное так и децентрализованное оповещение, а также ретрансляцию информации, полученной от вышестоящего уровня оповещения, на нижестоящий. Для сокращения сроков прохождения информации по уровням оповещения применяется автоматизация процессов оповещения путём применения специальной аппаратуры.

В каждом уровне оповещения должно быть предусмотрено сопряжение СО с информационными системами организаций и учреждений, которые являются источниками информации об угрозе или факте возникновения ЧС.

Источниками данных для принятия решения на задействование СО при возникновении ЧС мирного и военного времени являются учреждения и организации, дислоцированные на данной территории и осуществляющие постоянный контроль за состоянием окружающей среды, водных акваторий и воздушной обстановкой.

Кроме того, системы оповещения в период повседневной деятельности должны осуществлять дистанционную подготовку населения по РСЧС, а при угрозе и возникновении ЧС (режимы повышенной опасности и ЧС) – своевременное оповещение и информирование населения.

2.2. Требования по боевой готовности

Системы оповещения должны находиться в постоянной готовности к немедленному задействованию по предназначению при получении сигналов по ГО и РСЧС.

2.3. Своевременность оповещения и информирования населения

Это требование определим как время $t_ф$, фактически затрачиваемое на доведение информации по ЧС до населения, не превышающее допустимого времени "подхода" поражающих факторов ЧС до населённого пункта $t_д$, начиная с момента времени $t_о$ обнаружения ЧС, то есть $t_ф \le t_д$, рис. 2.1.

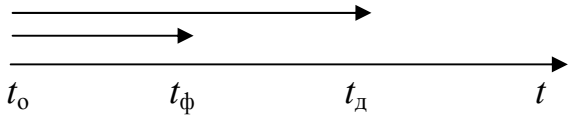

Рис. 2.1. К определению своевременности оповещения

Фактическое время $t_ф = t_з + t_н$, где

$t_з$ – время задержки задействования СО и их оконечных средств по доведению информации до населения;

$t_н$ – время, непосредственно затрачиваемое на информирование населения.

Время задержки $t_з$ определим как $t_з = t_1 + t_2 + t_3$, где t_1 – время, затрачиваемое на получение информации о факте возникновения ЧС (это время может быть сокращено за счёт автоматизации процесса доведения информации о факте возникновения ЧС от датчиков контроля опасного состояния до системы оповещения);

t_2 – время, необходимое для оценки обстановки и принятия решения на задействование системы оповещения;

t_3 – время прохождения сигналов по направлениям оповещения.

Для действующих СО при автоматическом способе передачи время прохождения сигналов на территориальном уровне оповещения составляет 12 *с* с вероятностью прохождения сигнала $p \ge 0{,}95$, а на местном уровне – 8 *с* при $p \ge 0{,}95$.

Допустимое время на анализ и ретрансляцию сигналов оповещения не должно превышать 60 *с* на территориальном и местном уровнях оповещения.

Очевидно, для цифровых СО приведенные характеристики прохождения сигналов по направлениям оповещения существенно улучшатся. При этом можно принять $t_3 \le 10$ *с* для регионального уровня оповещения и $t_3 \le 5$ *с* для местного уровня оповещения с вероятностью прохождения сигнала $p \ge 0{,}99$.

Примем допущение о том, что в цифровых СО время задержки сигналов оповещения не увеличится и поэтому для цифровых СО можно принять $t_3 \le 30$ *с*.

Определим продолжительность времени $t_н$ непосредственного доведения информации по ГЗ до населения. Оно включает время действия сирен $t_с$, которое составляет 165 *с* и время $t_р$ передачи речевой информации для населения, которое должно составлять не более 5 *мин.*

Будем считать, что современные телекоммуникационные технологии обеспечивают доведение речевой информации по ГЗ до населения за время $t_р$ = (2-3) *мин.* Очевидно, можно ограничить время действия сирен до 135 *с*.

Допустим, что $t_с$ = 165 *с*, а $t_р$ = 150 *с*. Тогда $t_н$ = 165 + 150 = 315 *с* = = 5,25 *мин*. Это означает, что для цифровых СО можно принять $t_н$ = 5 *мин*.

С учётом этого фактическое время, затрачиваемое на оповещение и информирование населения по ГЗ, будет равно $t_ф = t_з + t_н = 0{,}5 + 5 = 5{,}5$ *мин*.

Рассмотренные временные предпосылки для определения фактически затрачиваемого времени на оповещение и информирование населения по ГЗ позволяют принять $t_ф$ = 5 *мин*.

Таким образом, если $t_ф$ = 5 *мин*. $\leq t_д$, то факт оповещения и информирования населения по ГЗ следует считать своевременным.

2.4 Достоверность передачи-приёма сигналов и информации оповещения

Под достоверностью будем понимать степень соответствия принятых сигналов оповещения и речевых сообщений переданным. Достоверность характеризует способность системы оповещения обеспечить воспроизведение переданных сообщений оперативными дежурными ***центров оповещения и информирования (ЦОИ)*** с заданной точностью. Возможные несоответствия между переданным и принятым сообщением могут быть вследствие ошибок операторов при вводе информации, воздействия помех в канале связи и др. Главными источниками искажения переданных сообщений являются каналы связи, так как они для СО характеризуются большой протяженностью, изменяющимися условиями прохождения сигнала и воздействиями помех на канал связи.

Требования к достоверности в общем случае зависят от характера передаваемых сообщений и их важности.

Достоверность приёма цифровых сигналов оповещения оценим коэффициентом ошибок на один бит и коэффициентом необнаружения ошибки на знак сообщения. Если $N_{но}$ – число знаков, принятых с необнаруженной ошибкой, а $N_{общ}$ – общее количество переданных знаков в заданном интервале времени, то коэффициент необнаружения ошибок $K_{но} = \dfrac{N_{но}}{N_{общ}}$.

Требования к достоверности приёма данных сформулированы в ГОСТах 17422-79, 17657-79, 24375-80, 24734-81. В соответствии с указанными ГОСТами, системы передачи данных при использовании незащищенных каналов связи должны обеспечивать градации достоверности передачи информации, приведённые в табл. 2.1.

Таблица 2.1

Максимальное значение коэффициента ошибок на бит в незащищённом канале	**Коэффициент необнаружения ошибки для градации достоверности**		
	1	2	3
10^{-2}-10^{-3}	10^{-5}	10^{-6}-10^{-7}	10^{-8}-10^{-9}
10^{-4}	10^{-6}	10^{-7}-10^{-8}	10^{-9}-10^{-10}

С учётом данных табл. 2.1, важности информации, передаваемой в системах оповещения и допущениях о том, что ошибки операторов должны быть сведены к нулю, требования к достоверности принимаемых сигналов оповещения должны соответствовать:

1. На местном и объектовом уровнях оповещения:

- коэффициент ошибок на бит – не более 10^{-4};
- коэффициент необнаруженной ошибки – не более 10^{-8}.

2. В других уровнях оповещения:

- коэффициент ошибок на бит – не более 10^{-4};
- коэффициент необнаружения ошибки – не более 10^{-10}.

Достоверность передаваемой информации в цифровых системах оповещения должна обеспечиваться за счёт применения современных методов кодирования, аппаратуры восстановления искаженных знаков и мажоритарных способов передачи-приёма сигналов оповещения.

Достоверность приёма речевой информации оценивается слоговой (S) и словесной (W) разборчивостью. Количественно слоговая разборчивость речи оценивается отношением числа правильно принятых слогов $N_{пп}$ к их общему принятому числу $N_о$ в процентах:

$$S = \frac{N_{пп}}{N_о} \cdot 100\ \%.$$

Аналогично определяется и словесная разборчивость. Требования к разборчивости речи сформулированы в ГОСТе В 20775-75, в соответствии с которым разборчивость речевых сообщений в цифровых системах оповещения должна соответствовать второму классу качества и быть не хуже 90 % слоговой и 97 % словесной разборчивости.

2.5. Требования к мобильным ЦОИ

С целью обеспечения устойчивости функционирования и эффективности применения СО в дополнение к стационарным ЦОИ должны создаваться и мобильные ЦОИ.

Сформулируем следующие основные требования к мобильным ЦОИ:

- время развёртывания $t_р \le 20$ *мин*;
- средняя скорость перемещения $s \ge 60$ *км/ч*;
- время коммутации (кроссировки) $t_к \le$ (5-19) *с*.

Мобильный ЦОИ должен решать те же задачи, что и стационарный ЦОИ.

2.6. Требования по задачам управления СО

В СО должно быть предусмотрено три способа управления оповещением и информированием населения по ГЗ: автоматический, автоматизированный и ручной. Каждым из указанных способов должны решаться следующие основные задачи:

- сбор, документирование и отображение состояния оповещения и информирования населения;

- сбор, документирование и отображение информации о прохождении сигналов оповещения;

- отображение возможных сбоев по направлениям оповещения;

- отображение взаимодействия по вертикальным и горизонтальным уровням (направлениям) оповещения.

Степень автоматизации процесса оповещения и информирования должна быть доведена до 100 %.

2.7. Структурно-технические требования

Организационно-техническое построение СО должно соответствовать государственно-административному делению Российской Федерации и географическому размещению ПОО. При этом должно быть обеспечено организационное, техническое и программное сопряжение разнотипных ***технических средств оповещения (ТСО)***, находящихся в составе СО.

Способы и технические параметры сопряжения определяются на этапе проектирования СО.

Способы обмена информацией между ЦОИ должны быть автоматическими, автоматизированными, ручными и в диалоговом режиме по прямым телефонным каналам. Характеристики взаимосвязей по направлениям оповещения должны соответствовать параметрам, указанным в эксплуатационно-технической документации на ТСО.

Способы и средства связи для информационного обмена между ЦОИ должны быть цифровыми (аналогово-цифровыми).

Скорость передачи сигналов оповещения по цифровым каналам и трактам связи должна составлять порядка 2048 *кбит*/*с*.

3. Требования по эффективности и безопасности функционирования

3.1. Требования по надёжности

Надёжность – способность системы выполнять поставленные задачи, сохраняя эксплуатационные показатели в пределах, соответствующих заданным режимам и условиям использования, технического обслуживания, восстановления и ремонта. В качестве показателей надёжности СО будем использовать: среднюю наработку на отказ, среднее время восстановления, коэффициент готовности и коэффициент технической (эксплуатационной) готовности к практическому применению, а также средний срок службы до списания и гарантийный срок эксплуатации.

Надёжность СО определяется состоянием технических средств оповещения, каналов (линии) связи и программного обеспечения.

Например, уровень надёжности телекоммуникационных средств Общероссийской комплексной системы информирования и оповещения населения (ОКСИОН) характеризуется средней наработкой на отказ не менее $T_о = 10$ *тыс. ч* и средним временем восстановления не более $T_в = 12$ *ч*. При этом коэффициент готовности $K_г = T_о/(T_о + T_в) = 0{,}9988$.

За критерий отказа примем нарушение связности в направлении оповещения на время не более 10 *с*.

Вместе с тем современная элементная база, технологический и конструкторско-производственный уровень позволяют создавать технические средства ОКСИОН с показателями надёжности, превышающими принятые значения.

Кроме указанных показателей надёжности разработчики ОКСИОН установили гарантийный срок эксплуатации телекоммуникационных средств оповещения, равный одному году, а средний срок их службы до списания – 15 лет [2].

Для сравнения заметим, что разработчики комплекса технических средств оповещения типа П-166Ц приводят следующие значения показателей надёжности:

- средняя наработка на отказ $T_о > 10$ *тыс. ч*;
- среднее время восстановления $T_в \approx 2$ *ч*;
- среднее время ***технического обслуживания (ТО)*** $T_{то} \approx 2$ *ч*;
- гарантийный срок эксплуатации $T_г = 12$ месяцев;
- назначенный срок службы (ресурс) до списания (продления ресурса) $T_р = 12$ лет.

Для указанных значений единичных показателей надёжности коэффициент технической готовности П-166Ц будет равен:

$$K_{тг} = \frac{T_о}{T_о + T_в + T_{то}} = 0{,}9996.$$

Общеизвестно, что тенденция повышения надёжности технических систем (средств), в том числе и технических средств оповещения, сопровождается сокращением среднего времени технического обслуживания и увеличением гарантийных сроков эксплуатации и срока службы до списания. Поэтому, с учётом этого положения и приведённых количественных показателей надёжности ОКСИОН и П-166Ц, для создаваемой СО нового поколения в качестве задания на проектирование ТСО можно рекомендовать следующие значения показателей надёжности:

- средняя наработка на отказ $\overline{T}_о > 10$ *тыс. ч*;
- среднее время восстановления $\overline{T}_в = 1\text{-}1{,}5$ *ч*;
- среднее время ТО $\overline{T}_{то} \le 2$ *ч*
- гарантийный срок службы $T_г = 2\text{-}3$ года;
- назначенный срок службы $T_р = 15\text{-}20$ лет.

При этих исходных данных коэффициент технической готовности ТСО буде равен $K_{тг} \ge 0{,}9998$. Известно, что техническая готовность кабельных линий связи протяжённостью 2,5 *км* в соответствии с рекомендацией G 602 МККТТ (МЭС – Международный союз электросвязи), должна быть не менее 0,996. Очевидно, связность СО в определенном направлении оповещения не превысит технической готовности кабельной линии связи. Поэтому для повышения связности между центрами оповещения СО необходимо применять не только кабельные, но и радиорелейные линии связи, а также радио и спутниковую связь (рис. 3.1).

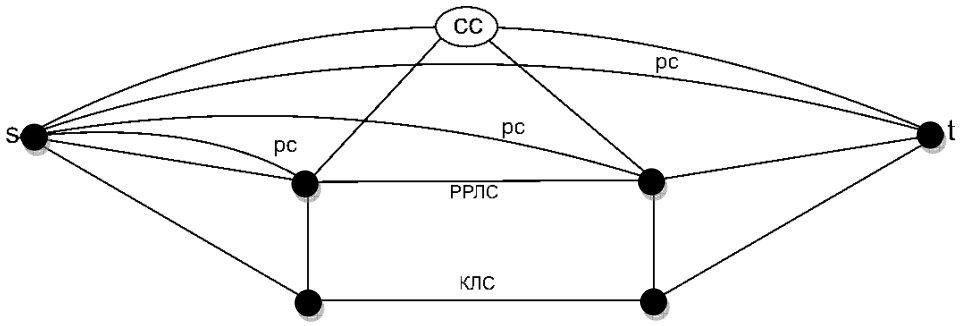

Рис. 3.1. Комплексное применение родов связи:
●– обозначение центров оповещения; S- центр истока информации; *t* – центр стока информации; КЛС – кабельная линия связи; РРЛС – радиорелейная линия связи; РС – радиосвязь; СС – спутниковая связь

Для повышения надёжности связи ЦОИ в СО может быть также использован дублированный кабельный канал связи, техническая готовность которого оценивается величиной $K_{тг} \geq 0{,}99998$, что соответствует требуемой надёжности ТСО.

Оценка структурной надёжности СО

Системы оповещения представляют собой структурно сложные территориально-распределенные системы, построенные по радиально-узловому иерархическому принципу в соответствии с государственно-административным делением РФ.

Вышестоящие уровни оповещения имеют приоритет, по отношению к нижестоящим. Поэтому при анализе структурного построения приоритетность СО выражается в виде значимости ЦОИ верхних уровней, по отношению к нижним.

Под значимостью ЦОИ будем понимать число направлений оповещения, инцидентных рассматриваемому ЦОИ, то есть входящих и исходящих.

Допустим, что минимальное число направлений оповещения, идущее от регионального ЦОИ (ОЦОИ) до местных (МЦОИ), равно 10. Тогда инцидентность РЦОИ равна 10, а каждого местного ЦОИ –1 и, следовательно, значимость РЦОИ, относительно МЦОИ, равна 10:1.

Аналогичную значимость можно, по всей видимости, принять для межрегиональных и федерального ЦОИ.

Определённая таким образом значимость ЦОИ, применительно к заданию требований к их надёжности по принятому показателю (например, коэффициенту готовности), означает, что надёжность вышестоящего ЦОИ должна быть на один порядок выше надёжности нижестоящих ЦОИ. Допустим, что $K_г$ местного ЦОИ $K_г$(МЦОИ) = 0,999, тогда $K_г$ регионального $K_г$(РЦОИ) = 0,9999, межрегионального (МРЦОИ) – $K_г$(МРЦОИ) = 0,99999, федерального (ФЦОИ) – $K_г$(ФЦОИ) = 0,999999.

Оценим надёжность направления оповещения, которая определяется надёжностью вышестоящего ЦОИ (ВЦОИ), ***кабельной линии связи (КЛС)***, сети радиосвязи, а также надёжностью нижестоящих ЦОИ (НЦОИ) или оконечных ТСО (ОТСО) (рис. 3.2).

Рис. 3.2. К определению надёжности направления оповещения

Допустим, что $К_г$ кабельной линии связи $К_г$(КЛС) = 0,996, а ***канала радиосвязи (РС)*** оценивается величиной $К_г$(РС) = 0,99.

Пусть для передачи сигналов оповещения используется только КЛС. При этом $К_г$ направления оповещения не превысит значения $К_г$(КЛС) = 0,996.

Для повышения $К_г$ направления оповещения можно применить дублирование КЛС радиосвязью. Примем вариант, когда сигналы оповещения передаются одновременно по КЛС и радиосвязи. Тогда $К_г$ принятой ***дублированной системы (ДС)*** передачи сигналов оповещения будет равна $К_г$(ДС) = 1 – (1 – $К_г$(КЛС)(1 – $К_г$(РС)) = 0,99996, а $К_г$ ***направлений оповещения (НО)*** примет следующие значения:

- для местных направлений оповещения (МНО)

$К_г$(МНО) = $К_г$(МЦО) $К_г$(ДС) $К_г$(ОТСО) = 0,999 · 0,99996 · 0,9998 ≈ 0,999;

- для региональных направлений оповещения (РНО)

$К_г$(РНО) = $К_г$(МЦО) $К_г$(ДС) $К_г$(ОТСО) = 0,999 · 0,99996 · 0,9998 ≈ 0,999;

- для межрегиональных направлений оповещения (МРНО)

$К_г$(МРНО) = $К_г$(МЦО) $К_г$(ДС) $К_г$(ОТСО) = 0,999 · 0,99996 · 0,9998 ≈ 0,999;

- для федеральных направлений оповещения (ФНО)

$К_г$(ФНО) = $К_г$(ФЦОИ) $К_г$(ДС) $К_г$(МОЦОИ) = 0,999999·0,99996·0,99999 = = 0,99995.

Надёжность программного обеспечения не должна снижать уровень надёжности ***системы оповещения населения (СОН)***. Поэтому надёжность программного обеспечения по выбранному показателю (например, средняя наработка на один сбой в рабочей программе) должна быть на порядок выше надёжности СОН.

Кроме того, достижение высокой связности между ЦОИ СО зависит от их устойчивого сопряжения по техническим параметрам и рабочим программам.

3.2. Требования по живучести

Под живучестью СО будем понимать её свойство сохранять и восстанавливать в заданное время работоспособность при воздействии ***поражающих факторов (ПФ)*** чрезвычайных ситуаций.

Живучесть СО определяется элементной стойкостью к ПФ ЧС, структурной избыточностью и восстанавливаемостью. Элементная стойкость характеризуется способностью отдельных элементов СО (например, направления оповещения) сохранять работоспособное состояние при воздействии ПФ ЧС.

Частными характеристиками элементной стойкости являются: радиационная, электромагнитная стойкость, термостойкость, водостойкость и д.р. Стойкость – адресная характеристика, так как всегда увязывается с физической природой конкретного поражающего фактора.

Например, ЦОИ размещаются в сооружениях повышенной ответственности и сохраняют нормальное функционирование при воздействии некоторых ПФ ЧС (ураганы, аварийное отключение электропитания и др.). Поэтому вероятность повреждения ЦОИ очень низка.

Структурная избыточность СО обеспечивается, например, за счёт комплексного использования проводной, радиорелейной, спутниковой, транкинговой и сотовой связи, а также систем чрезвычайной и мобильной связи и оповещения.

СО определим как её способность к устранению повреждений за время, не превышающее заданного.

Поражающие факторы в мирное время будет порождать: пожары, ураганы, наводнения, землетрясения, взрывы, злоумышленные повреждения, аварийное прекращение подачи электроэнергии, попадание в систему оповещения компьютерных вирусов, саботаж и другие опасные события и явления.

Заметим, что перечисленные события и явления не являются характерными для всех регионов России. Поэтому при оценке живучести региональных СО необходимо рассматривать только те опасные события и явления, которые характерны для данного региона.

Опасные события и явления являются редкими и вследствие их воздействия образуется поток повреждений (разрушений), который предлагается характеризовать распределением Пуассона и формулой:

$$P_m(t) = \frac{(\lambda t)^m}{m!} \mathrm{e}^{-\lambda t}, \qquad (3.1)$$

где $P_m(t)$ – вероятность появления ровно m повреждений (разрушений) за время наблюдения t;

λ – интенсивность появления поражающего фактора:

$$\lambda = \frac{1}{\overline{T_{\text{п}}}};$$

$\overline{T_{\text{п}}}$ – период повторения поражающего фактора;

λt – среднее число повреждений за текущее время t.

При $m = 0$ получим выражение вероятности того, что за время t повреждений не произойдёт, то есть

$$P_0(t) = e^{-\lambda t}.$$

Из определения живучести следует, что СОН работоспособна, если она в случае повреждения восстанавливается за допустимое время, предусмотренное условиями её функционирования.

Функцию распределения случайной величины времени восстановления повреждения $T_{\text{в}}$ можно описать экспоненциальным законом:

$$F(t) = P(T_{\text{в}} < t) = 1 - \mathrm{e}^{-\mu t}, \qquad (3.2)$$

где μ – интенсивность восстановления повреждённого элемента СО в единицу времени:

$$\mu = \frac{1}{T_{\text{в}}}.$$

Для принятых распределений (3.1) и (3.2) при $t \to \infty$ справедливо выражение

$$K_{ж} = \frac{\mu}{\lambda + \mu} = \frac{\overline{T_{п}}}{\overline{T_{п}} + \overline{T_{в}}}, \qquad (3.3)$$

которое является показателем живучести элемента и характеризует вероятность нахождения элемента СО (например, направления оповещения) в работоспособном состоянии.

На величину показателя (3.3) существенное влияние оказывает значение времени $T_{в}$. При $T_{в} \to 0$, $K_{ж} \to 1$.

В соответствии с [5] допускается, что $T_{в}$ = (24-48) *ч*. Вместе с тем показатель (3.3) также зависит от времени $\overline{T_{п}}$: с увеличением этого времени величина показателя (3.3) также увеличивается.

Для обоснования требований к величине показателя (3.3) произведём его вычисление для следующих исходных данных: $\overline{T_{в}}$ = 24 *ч*, $\overline{T_{п}}$ = 1, 2, 4, 6, 8, 10 годы.

Расчёты выполним для следующих условий:

- поражающий фактор ЧС приводит к повреждению хотя бы одного направления оповещения;
- полученное повреждение обнаруживается немедленно;
- появлением нового повреждения в период устранения предыдущего можно пренебречь, так как $\overline{T_{в}} << \overline{T_{п}}$.

Результаты расчётов приведены в табл. 3.1.

Таблица 3.1

$T_{п}$, год	1	2	4	6	8	10
$K_{ж}$	0,997	0,9986	0,9993	0,9995	0,9996	0,9997

Заметим, что живучесть СО может быть увеличена на основе комплексного использования имеющихся родов и систем связи, а также применения радиально-кольцевой окольцованной схемы при организационно техническом построении СОН.

3.3. Требования по помехозащищенности

Под помехозащищенностью СО будем понимать их способность обеспечивать передачу сигналов оповещения в условиях воздействия радиопомех.

В [11] показано, что для СО можно допустить сбои связи в условиях непреднамеренных помех не более 10 *с* с вероятностью связности $P_{с} \geq 0{,}98$.

Приведённые характеристики помехозащищенности СО можно улучшить, если применить шумоподобные сигналы, которые могут увеличить помехозащищенность СО как от преднамеренных, так и непреднамеренных помех.

Реальные предпосылки для такого подхода к повышению помехозащищенности СОН, в связи с переходом на цифровую и оптоволоконную технику связи, имеются.

Основной характеристикой систем широкополосной связи является база сигнала B, под которой понимается произведение ширины спектра сигнала Δf_c на его длительность T:

$$B = \Delta f_c \cdot T. \quad (3.4)$$

Для фазоманипулированного сигнала $B = 1$, так как для такого сигнала справедливо равенство: $T = 1 / \Delta f_c$.

При этом высокая помехозащищенность СО достигается за счёт того, что отношение "сигнал-помеха" относительно узкополосных сигналов увеличивается пропорционально базе сигнала [15]:

$$\gamma = \frac{P_c}{P_п} B, \quad (3.5)$$

где P_c – мощность сигнала;

$P_п$ – мощность помехи;

$B \geq 1$ – значение базы сигнала.

Таким образом, принятые значения характеристик помехозащищенности СО будем считать приемлемыми.

3.4. Требования по безопасности

Под безопасностью будем понимать способность обеспечивать сохранение втайне от противника содержания передаваемых сигналов оповещения и противостоять вводу ложной информации.

Безопасная СО в процессе её функционирования не должна переходить в опасное состояние.

Основными инициирующими условиями перехода СО в опасное состояние могут быть: несанкционированный запуск, а также низкая криптостойкость и имитостойкость передаваемых сигналов оповещения.

Несанкционированный запуск может быть предотвращен выполнением некоторых организационных мер. Это, например, ограничение должностных лиц, допущенных к эксплуатации СОН, применение эффективных способов паролирования, позволяющих идентифицировать принадлежность должностных лиц по признаку "свой-чужой", передача сигналов оповещения по мажоритарным системам связи, получение подтверждения о приёме сигнала оповещения и др.

Заметим, что переход на цифровые технологии связи способствует увеличению криптостойкости и имитостойкости передаваемых сигналов оповещения.

Действительно, цифровая техника связи упрощает техническую возможность увеличения элементности шифрующего кода и вследствие этого повышается криптостойкость и имитостойкость сигналов оповещения.

Кроме того, в цифровой широкополосной системе связи увеличивается безопасность передачи шумоподобного сигнала оповещения (его криптостойкость и имитостойкость) вследствие уменьшения его спектральной плотности и увеличения базы сигнала. Действительно, отношение спектральной плотности

сигнала $N_с$ к спектральной плотности шумов $N_ш$ в B раз меньше, чем у узкополосных сигналов [15]:

$$G_с = \frac{N_с}{N_ш} = \frac{2P_с}{N_ш \Delta f_с} = \frac{2P_с T}{N_ш B}. \quad (3.6)$$

Следовательно, выделить полезный сигнал из шума можно только при известной шифрующей последовательности, энтропия которой может быть достаточно высокой.

Таким образом, использование широкополосной связи и шумоподобных сигналов оповещения одновременно обеспечивает высокую помехозащищенность и безопасность СОН.

Из рассмотренных положений следует, что при переходе на цифровые способы передачи-приёма сигналов оповещения можно обеспечить достаточно высокую безопасность СОН.

В МЭК 61511-1-2003 определены 4 уровня полноты безопасности систем по частоте опасных отказов в час, которые представлены в табл. 3.2.

Таблица 3.2

Уровни полноты безопасности по частоте опасных отказов

Уровень полноты безопасности	Предельная частота опасных отказов в час
4	$\geq 10^{-9}$ до $< 10^{-8}$
3	$\geq 10^{-8}$ до $< 10^{-7}$
2	$\geq 10^{-7}$ до $< 10^{-6}$
1	$\geq 10^{-6}$ до $< 10^{-5}$

Очевидно, наиболее приемлемым уровнем полноты безопасности для СО является 4 уровень, которому соответствует предельная частота опасных отказов в час $\lambda_п \geq 10^{-9}$ до $\lambda_н < 10^{-8}$. Эти значения предельной частоты опасности отказов в час могут быть приняты в качестве требований к безопасности СОН.

4. Требования по техническому обслуживанию и метрологическому обеспечению

4.1. Требования по техническому обслуживанию

Требования к устойчивости и безопасности функционирования СО реализуются на этапах её проектирования и создания, оцениваются при проведении опытных испытаний и обеспечиваются в процессе эксплуатации. При этом в зависимости от принятой модели эксплуатации и её эффективности устойчивость функционирования может быть снижена или увеличена. Под эксплуатацией СО будем понимать организацию и проведение технического обслуживания, ремонта и контроля технического состояния в соответствии с принятой моделью эксплуатации.

Поскольку цифровая нового поколения СО является высоконадёжной системой, то, как показано в [12], для такой системы наиболее эффективной моделью эксплуатации является модель эксплуатации по состоянию с контролем уровня надёжности. Применение данной модели позволяет повысить техническую готовность СО к применению и снизить стоимость эксплуатации.

При использовании такой модели эксплуатации контроль уровня надёжности СО (например, по интенсивности отказов) проводится один раз в год. Одновременно с этим проводится комплексный контроль технического состояния СОН, включающий контроль некоторых параметров, а также сезонное техническое обслуживание ТСО, эксплуатирующихся в естественных атмосферных условиях.

В качестве требования по техническому обслуживанию цифровых СО можно рекомендовать модель эксплуатации по состоянию с контролем уровня надёжности.

4.2. Требования по численности и квалификации обслуживающего персонала

Численность обслуживающего персонала должна соответствовать нормам времени в человеко-часах на все виды ***эксплуатационно-технического обслуживания (ЭТО)*** для различных типов ТСО на один год эксплуатации. Эти нормы определяет разработчик ТСО для принятой модели эксплуатации и указывает в соответствующей эксплуатационно-технической документации.

С учётом выше сформулированных положений будем считать, что нормы времени в человеко-часах (чел./*ч*) на один год эксплуатации отдельно взятого типа ТСО и есть исходное требование к определению численности обслуживающего персонала.

Очевидно, чем большее число ТСО будет находиться в схеме организационно-технического построения СОН, тем потребуется большее число обслуживающего персонала и выше стоимость ЭТО.

Исходя из такого подхода к определению численности обслуживающего персонала, заказчик сможет сформулировать требования по численности обслуживающего персонала и стоимости ЭТО в техническом задании на проектирование СО.

Заметим, что наиболее высокие нормы времени в чел./час. на ЭТО ТСО соответствуют модели эксплуатации по выработке ресурса, а самые низкие – модели эксплуатации по состоянию с контролем уровня надёжности.

К эксплуатационно-техническому обслуживанию ТСО допускаются специалисты:

- имеющие среднетехническое или высшее образование;
- прошедшие специальную подготовку на предприятии разработчика (изготовителя) технических средств оповещения или в учебно-методических центрах МЧС России;
- сдавшие зачёт по знанию основных положений по эксплуатационно-техническому обслуживанию систем оповещения и правил техники безопасности, указанных в инструкциях по эксплуатации технических средств оповещения;
- прошедшие инструктаж по технике безопасности и медицинское освидетельствование на предмет годности к работе по техническому обслуживанию ТСО и в целом СОН.

4.3. Требования по метрологическому обеспечению

На этапе проектирования ТСО или СО должна быть разработана система метрологического обеспечения, основными задачами которой в соответствии с ГОСТ 1.25-80 являются:

- обеспечение единства, требуемой точности измерений и достоверности контроля оперативно-технических характеристик и параметров СО для оценки их технического состояния и поддержания в постоянной готовности к применению;

- обоснования оптимального состава измеряемых и контролируемых параметров, достоверности контроля параметров, а также необходимой точности измерений.

Для решения этих задач точность контрольно-измерительной аппаратуры должна быть выше требуемой точности измерения контролируемых параметров, указанных в эксплуатационно-технической документации. Кроме того контрольно-измерительная аппаратура должна регулярно подвергаться метрологической экспертизе.

5. Требования по стандартизации и унификации ТСО и программного обеспечения

С целью повышения эффективности функционирования цифровой СО нового поколения и сокращения расходов на эксплуатацию необходимо добиться такого положения, чтобы СО разных уровней оповещения были совместимы по техническим и функциональным параметрам, независимо от производителя их структурных элементов. Тогда заказчик может отдать предпочтение тому разработчику (производителю), который предложит организационно-техническое построение СО с более высокими качественными показателями, приемлемой их стоимостью и более низкими расходами на эксплуатацию.

Заметим, что современные цифровые технологии существенно упрощают создание совместимых по техническим и функциональным параметрам СО. Очевидно, для реализации этого положения заказывающим организациям необходимо обосновать технические условия по совместимости ТСО.

Работа по унификации и стандартизации типовых ТСО позволит создавать СО по модульному принципу, обеспечивающему сокращение расходов на создание и эксплуатацию СО и повышение эффективности их применения.

Одним из важных условий эффективного функционирования СО является выполнение требования по унификации программного обеспечения, которая может быть достигнута на основе использования унифицированной операционной системы и системы управления базами данных.

6. Финансово-экономические требования

К финансово-экономическим требованиям относятся:

- стоимость модернизации (создания) СО;
- стоимость одного года эксплуатации СО.

Стоимость модернизации (создания) СО определяется многими факторами, основными из которых являются: стоимость проектирования; стоимость ТСО, входящих в состав схемы организационно-технического построения СОН; расходы на монтаж СО и проведение опытной эксплуатации.

Годовая стоимость эксплуатации определяется затратами времени в человеко-часах на техническое обслуживание и ремонт одного типового ТСО в течение одного года эксплуатации и стоимостью одного человеко-часа работ. Тогда в целом стоимость эксплуатации СО определяется числом типовых ТСО, входящих в состав СО. Кроме того, в годовую стоимость эксплуатации включается стоимость израсходованных запасных частей на восстановление отказавших ТСО. Затраты на эксплуатацию также зависят от принятой модели эксплуатации. Для высоконадёжных ТСО наименее затратной моделью эксплуатации являются модель эксплуатации по состоянию с контролем уровня надёжности.

Финансово-экономические требования должны быть определены заказчиком на этапе обоснования необходимости модернизации действующей СО и указаны в концепции и программе её модернизации. В последующем эти требования также должны отражаться в техническом задании на проектирование модернизации (создания) СОН.

Литература

1. ***Концепция*** создания Общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей. М.: МЧС России, 2005.
2. ***Методические*** рекомендации по реконструкции территориальных систем оповещения гражданской обороны Российской Федерации. М.: МЧС России, 2001.
3. ***Методические*** рекомендации по созданию в районах размещения потенциально-опасных объектов локальных систем оповещения. М.: МЧС России, 2003.
4. ***Методические*** рекомендации по обеспечению функционирования системы оповещения гражданской обороны. М.: МЧС России, 1998.
5. ***Носов М.В.*** Региональные подсистемы общероссийской комплексной системы информирования и оповещения населения. Академия гражданской защиты МЧС России, 2010.
6. ***Носов М.В.*** Методологические аспекты развития систем оповещения населения. М.: Электросвязь, №4, 2004.
7. ***Носов М.В.*** Обоснование эффективности эксплуатации систем оповещения гражданской защиты. М.: Технологии гражданской безопасности, № 2, 2010.
8. ***Носов М.В.*** Организационно-технический состав систем оповещения гражданской обороны. Академия гражданской защиты МЧС России, 2005.
9. ***Носов М.В.*** Оповещение населения о чрезвычайных ситуациях. М.: ОБЖ, № 3, 2004.
10. ***Авиационные*** радиосвязные устройства. ВВИА им. проф. Н.Е. Жуковского, 1985.