УДК 658.512 (470)

АНАЛИЗ КОНЦЕПЦИИ ПОСТРОЕНИЯ СЕТЕЙ ИНФОРМАЦИОННОГО ОБМЕНА

А.С. Крутолапов, Д.А. Сычев

Предложен анализ методов построения сетей информационного обмена с использованием полевых шин, показаны преимущества распределенных систем управления, показаны основные показатели их работоспособности.

Ключевые слова: *сеть, передача данных, автоматизированная система, диспетчерское управление, сообщение, информация, качество обслуживания.*

Развитие систем автоматизации. В последнее время складывается тенденция к применению компьютеров в автоматизации различных процессов. Такие системы реализуются для управления химическими, технологическими процессами, системами пожарной и охранной сигнализации, управления подачей электроэнергии и системой водоснабжения [1].

Во исполнение Федерального Закона “О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера” от 21 декабря 1994 г. № 68-ФЗ соответствующие органы управления, силы и средства объединяет единая государственная система предупреждения и ликвидации чрезвычайных ситуаций (РСЧС).

В “Положении о единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций”, утверждённом постановлением Правительства Российской Федерации от 30 декабря 2003 г. №794, подчёркнуто, что управление РСЧС осуществляется с использованием средств связи и оповещения (п.21), а её информационное обеспечение − с использованием автоматизированной информационно-управляющей системы (АИУС) РСЧС (п.22).

В начале 90х годов была разработана совершенно новая концепция построения АИУС. Это системы распределенного контроля и управления на основе полевых шин. Объединяя датчики и исполнительные механизмы, используя единый протокол связи по одной последовательной шине данных, такие системы используют интеллектуальные узлы-контроллеры для децентрализованной обработки данных [2 − 7].

Концепция промышленных шин родилась в Европе и развивалась в течение многих лет. В настоящее время в самых разных специализированных прикладных областях используется более 50 промышленных шин. Вместе с тем (по мере их распространения в США) количество широко поддерживаемых шин не превышает половины десятка. Применение технологии промышленных шин знаменует собой совершенно новую эпоху в управлении. Одна из важнейших примет этой эпохи – смещение интеллекта на нижние уровни иерархии систем автоматизации. Растущие масштабы активного применения промышленных шин позволят вынести несложные задачи контроля за рамки централизованной системы управления на уровень конкретного объекта. Распределенные интеллектуальные средства, исполняющие эти задачи, смогут также одновременно собирать информацию реального времени и передавать ее узлам более высокого иерархического уровня.

По мере того, как этот "интеллект" становился всё более распределенным, всё очевиднее проявлялась потребность в общем стандартном средстве связи, как между отдельными интеллектуальными устройствами, так и между ними и остальным миром, что позволило бы упростить визуализацию и управление контролируемым объектом. В результате появилось нескольких стандартов промышленных шин, применяемых в качестве средств связи различных устройств на уровне конкретного объекта.

В результате объем информации на уровне объекта, собираемой в реальном масштабе времени, значительно возрастет. Только для сохранения, анализа и вывода результатов в реальном времени понадобится повысить производительность и расширить функциональные возможности используемых рабочих станций. Благодаря подобному подходу к "рассредоточению" интеллекта, операторы получат возможность контролировать, настраивать и даже менять параметры управления непосредственно с рабочего места.

Основная цель построения распределенных систем автоматизации – упрощение технологий производства и эксплуатации системы автоматизации за счет обеспечения сквозного сетевого доступа: от мощных супервизорных компьютеров и многофункциональных контроллеров до интеллектуальных пассивных элементов (датчики, регуляторы и т. п.). Такая связь должна удовлетворять всем совре-

Крутолапов Александр Сергеевич – заместитель начальника института дополнительного профессионального образования по учебно-методической работе Санкт-Петербургского университета Государственной противопожарной службы МЧС России, кандидат технических наук, доцент, e-mail: krut75@mail.ru;
Сычев Дмитрий Александрович - адъюнкт3 курса очного обучения Санкт-Петербургского университета Государственной противопожарной службы МЧС России, e-mail: 89052304480@mail.ru.

менным требованиям по функциональности, надежности и открытости.

Исследования показали, что переход от централизованного управления к распределенным архитектурам на базе промышленных шин позволяет достичь экономии оборудования до 40 процентов [3, 4].

Прежде были широко распространены такие системы автоматизации, которые были созданы для конкретных узких целей. Это не позволяло наиболее полно использовать оборудование и объединять несколько систем автоматизации в одну. Более того, создание нового типа оборудования приводило к необходимости полной замены старой или создания новой автоматизированной системы.

Данная ситуация дала толчок к появлению микропроцессорных систем автоматизированного управления с использованием fieldbus-сетей, или сетей на основе полевых шин, объединяющих интеллектуальные контроллеры, датчики и исполнительные механизмы.

Fieldbus-сети сегодня используются, в основном, как коммуникационные системы для обмена информацией между системой автоматизации и распределенными устройствами. При этом считается, что устройства распределены в поле (от английского field), что и определило термин fieldbus (полевая шина, или промышленная сеть). Тысячи успешных внедрений обеспечивают внушительное впечатление, а кроме того fieldbus технология позволяет сократить до 40% затрат на прокладку кабелей, накладных расходов и расходов на техническое обслуживание по сравнению с обычными технологиями. Только два провода необходимо для передачи трафика (входных и выходных данных, параметров, диагностических данных и т.д.).

Полевые шины – это, во-первых, некий физический способ объединения устройств (например, интерфейс RS-485 или оптоволокно) и, во-вторых, программно-логический протокол их взаимодействия. Причем “весовой коэффициент” программно-логических протоколов по отношению к физической среде, в общем понимании такого термина, как fieldbus, составляет не менее 95% [4].

Системы АИУС на основе полевых шин характеризуются уходом от концепции иерархического построения управляющих сетей к полной или частичной децентрализации управления более мощными средствами и механизмами, заложенными в их основу, строгой стандартизацией на уровне центральных межгосударственных организаций, богатыми возможностями совместного использования систем, работающих согласно различным протоколам [8].

Пользователи постепенно отходят от практики применения собственных систем и централизованных систем управления и начинают обращать внимание на системы с распределенным интеллектом. В результате фирменные и централизованные архитектуры понемногу сдают свои позиции на рынке, в то время как открытые распределенные системы начинают его завоевывать. Одна из причин этого кроется в том, что прокладка кабелей и развертывание системы с использованием промышленных шин обходится значительно дешевле. Системы с централизованным управлением обычно требуют, чтобы каждый датчик или группа датчиков подключалась к центральному контроллеру отдельным (и довольно дорогим) высококачественным кабелем. Напротив, в системе на основе полевых шин рядом с каждым кластером датчиков располагается один интеллектуальный узел, преобразующий сигналы датчиков в цифровую последовательность и передающий их в этом виде в систему управления и мониторинга.

По оценкам западноевропейских аналитиков, информационно-управленческие сети на основе полевых шин занимают на данный момент ведущее положение в сфере автоматизации и управления, начиная от крупных производств и заканчивая домашним хозяйством. Им безоговорочно отводится будущее автоматизации. Их идеологической основой является децентрализация управления или распределение функций управления по сети. Это означает, что задача управления распределяется между компонентами сети управления (микропроцессорными устройствами), каждому из которых отводится определенное задание и которые общаются по определенному протоколу. Следует также отметить, что устройства некоторых fieldbus-систем отличает довольно высокий уровень "интеллекта", реализованный аппаратно, что сводит к минимуму усилия, необходимые для конфигурации, инсталляции и сопровождения сети [36].

Системы управления на основе полевых шин являются распределенными в пространстве, т. е. обработка информации производится в географически удаленных местах. Компонент, который в состоянии обрабатывать данные, принято называть интеллектуальным. Обмен данными между интеллектуальными компонентами производится посредством шин и сетей [8].

Несмотря на то, что fieldbus-технологии появились уже более десяти лет назад, абсолютно доминирующими в управлении технологическими процессами они еще не стали. Основная причина этого – отсутствие единого международного стандарта на протокол промышленной сети, который мог бы гарантировать полную взаимозаменяемость и совместимость изделий различных производителей.

В 1984 г. Международная электротехническая комиссия (МЭК, IEC) начала разработку единого универсального стандарта промышленной сети. Европейское сообщество потребителей и производителей fieldbus-систем пошло по пути создания единого европейского стандарта. По ряду критериев была определена группа “претендентов”, и 15 марта 1996 г. в Брюсселе были подведены итоги проведенного накануне голосования по одобрению проекта EN50170 в качестве европейского стандарта промышленной сети (European Fieldbus Standard). EN50170 включил в себя (без изменений) три на-

циональных стандарта в области промышленных сетей: PROFIBUS (Германия), FIP (Франция) и P-NET (Дания). Эти решения подтверждены соответствующими национальными стандартами.

CAN, LON, PROFIBUS, Interbus-S, FIP, EIB, DeviceNET, SDS, ASI, HART, ControlNet и еще несколько десятков протоколов – это сегодняшняя ситуация на рынке промышленных сетей. Они имеют свои особенности и области применения, а единый международный стандарт промышленной сети отсутствует.

Это приводит к тому, что каждая технология развивается самостоятельно в условиях неизбежной конкуренции. Вполне естественно, что со временем определится ведущая, например, пятерка технологий, на которой будет сосредоточено основное внимание пользователей и бизнес независимых производителей. Таким центром кристаллизации де-факто можно считать сегодня европейский стандарт EN50170. Со стороны Европейского комитета по стандартизации CENELEC поступили предложения по расширению EN50170 за счет промышленных сетей Foundation Fieldbus и ControlNet. Если такое предложение будет принято, тогда EN50170 реально превратится в международный стандарт, каждая отдельная часть которого будет определять отдельную технологию полевых шин.

Иерархия сетей информационного обмена. Промышленная шина – это коммуникационная сеть, объединяющая несколько промышленных систем и функционирующая практически так же, как и локальная сеть в учреждении. Однако для поддержания режима реального времени промышленная шина должна быть детерминированной – качество, отсутствующее в локальных офисных сетях. Именно поэтому ни Ethernet, ни другие аналогичные сети не применяются в чисто промышленных системах. Отвечая требованиям различных прикладных сфер, промышленные шины обладают соответствующими характеристиками: детерминированностью; поддержкой больших расстояний между узлами; защита от электромагнитных наводок; упрочненной механической конструкцией.

Многие промышленные шины опираются на стандарт двухпроводного интерфейса RS-485, обеспечивающего взаимосвязь нескольких устройств на расстояниях до нескольких сотен метров. В промышленных условиях оперативность и предсказуемость времени передачи информации − характеристики более важные, чем способность передавать большие объемы данных. Скорости передачи по промышленным шинам колеблются от 50 Кбит/с до 4 Мбит/с (с одним замечательным исключением − шина PROFIBUS имеет пропускную способность до 12 Мбит/с).

В распределенных промышленных системах объединяются сетевые узлы самых разных типов, с самыми разными скоростями, расстояниями передачи информации и типами данных. Например:

– вентиль может постоянно сообщать о своем состоянии (закрыт/открыт) единственным битом;

– датчик температуры может передавать соответствующий параметр каждые 5 минут;

– датчик быстродействующей системы регулирования должен сообщать о произошедшем отказе в течение нескольких микросекунд;

– для обновления изображения на дисплее оператора в большой системе управления может понадобиться передача нескольких мегабайт информации.

По функциям и областям применения различают следующие системы шин и сетей:

1. SAN (Small Area Networks) − малые сети. К ним принадлежат:

– системная шина, которая непосредственно объединяет компоненты компьютера друг с другом. Если в распределенной системе отдельные интеллектуальные компоненты общаются друг с другом посредством системной шины, то при высокой скорости передачи расстояние между ними относительно невелико (в Multibus II, например, от 2 до 3 метров);

– периферийная шина, которая представляет собой параллельное или последовательное соединение компьютерных систем, которые подключаются к устройствам ввода/вывода. В качестве примера можно назвать SCSI-Bus (Small Computer System Interface: ANSI).

2. LAN (Local Area Network) – последовательная система коммуникации между компонентами компьютера, которая принадлежит, как правило, одному владельцу (например, сеть Ethernet).

3. MAN (Metropolitan Area Network) − передающая среда для расстояний от 25 до 200 км.

4. WAN (Wide Area Network) – общественная передающая среда, которая предлагает удаленное соединение компьютеров свыше 100 км. Самые известные WAN базируются на протоколе X.25.

5. GAN (Global Area Network) − глобальные компьютерные сети с применением спутников связи.

Представляется возможным разместить сети на основе полевых шин между LAN и MAN сетями. С учетом этого FAN (Fieldbus Area Network) – полевые шины, которые связывают друг с другом комплексные компоненты управления [5].

Промышленные сети на основе полевых шин занимают низкий уровень в иерархии сетей, образуя так называемый уровень поля.

Преимущества распределенных систем управления. Проанализировав источники [8, 9 − 12], можно определить основные преимущества распределенных систем управления на основе полевых шин по отношению к централизованным:

Во-первых, стоимость проводников и расходы на их прокладку значительно ниже, так как требуется проложить всего одну линию связи, а в отдельных случаях можно обойтись уже существующей (Рис. 1).

Кроме того, сокращается количество необходимого оборудования (Рис. 2). А также, благодаря совместимости устройств изготовителей друг с дру-

гом, резко увеличивается возможность выбора поставщиков оборудования, что позволяет выбрать приемлемый по цене вариант системы.

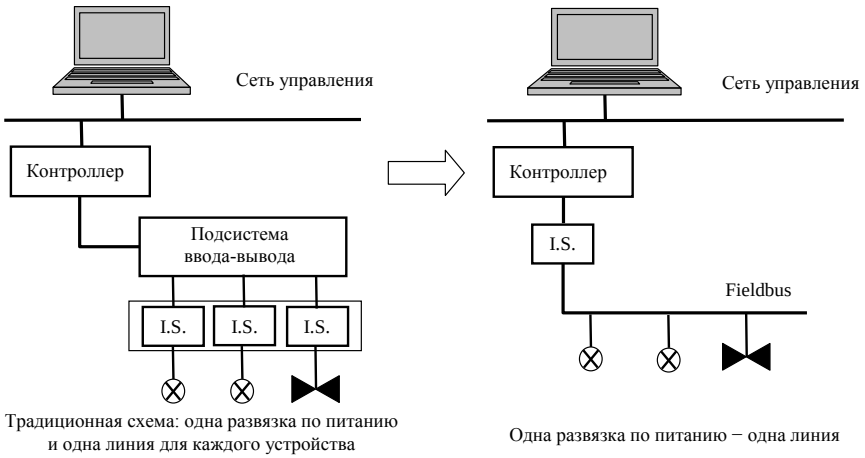


Рис. 1. Сокращение количества проводников [10]

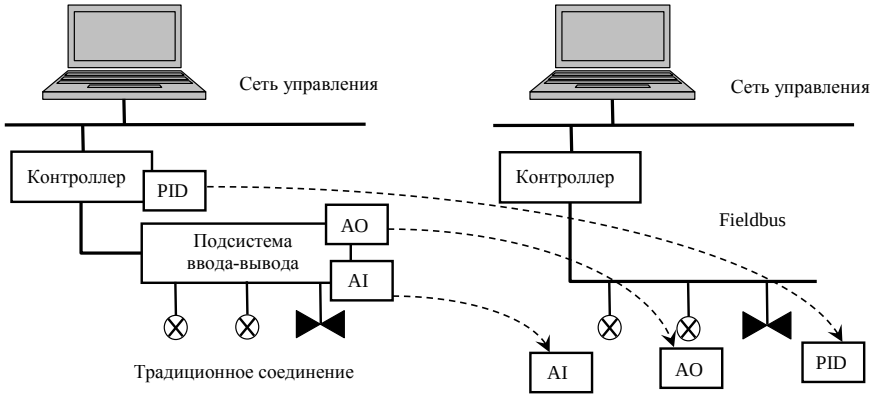


Рис. 2. Сокращение количества программного обеспечения [10]

Во-вторых, распределенная система предлагает повышенную помехоустойчивость, так как большое количество компонентов может продолжать работать, если выйдет из строя одна из частей. Функции одного устройства может взять на себя другое. Централизованная же система прекращает работать, если не функционирует центральное устройство.

В-третьих, гибкость системы, способность к интеграции. Прежде были распространены системы управления, которые создавались для конкретных узких целей, что ограничивало возможности использования оборудования и не позволяло объединять несколько систем автоматизации в одну. Более того, создание нового типа оборудования приводило к необходимости полной замены старой или создания новой автоматизированной системы. С приходом систем полевых шин положение резко изменилось. Использование стандартизированных протоколов связи обеспечивает совместимость устройств различных фирм-производителей друг с другом.

В-четвертых, при проектировании централизованной системы разработчику необходимо ориентироваться на централизованное и комплексное применение алгоритмов. Децентрализованная система реализует во многих случаях простые алгоритмы и приемлемые по цене конфигурации системы, а решение задач возлагается на периферию. В большинстве случаев фирмы-производители предлагают уже готовые решения для каждого конкретного типа узлов. Снижается нагрузка на помещения контроля и управления. Количество оборудования, устанавливаемого в них, сокращается.

В-пятых, возможность передачи по одной линии большого количества переменных позволяет получать больше информации за определенный интервал времени (Рис. 3).

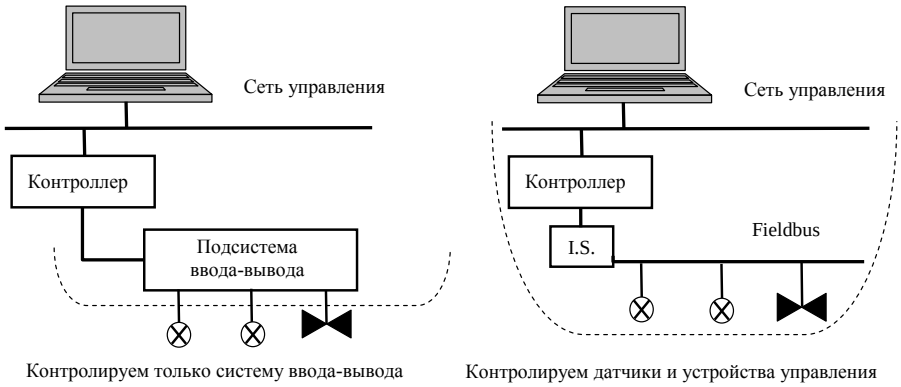


Рис. 3. Передача данных по одной линии [10]

В-шестых, преимущества полностью цифровой связи обеспечивают поступление большего количества доступной информации не только о состоянии объекта управления, но и о состоянии самой системы (например, датчиков в агрессивной среде) (Рис. 4).

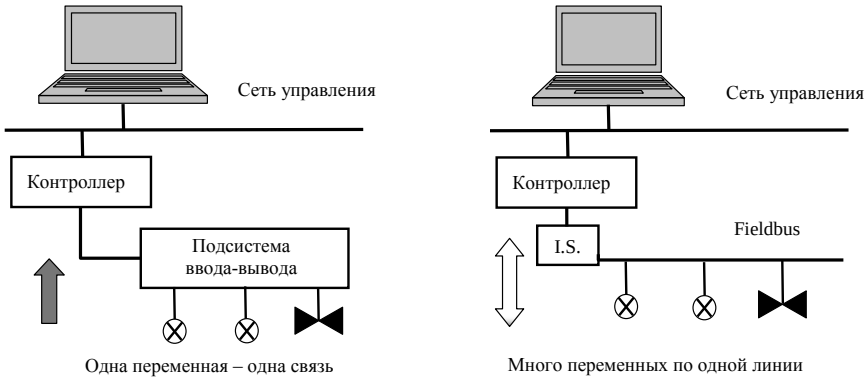


Рис. 4. Расширенное видение процесса управления

В-седьмых, децентрализованная система управления представляет собой параллельную систему, в которой основная обработка информации происходит на местах, а верхние ее уровни получают только данные о качественных состояниях объекта управления.

В-восьмых, этапы установки, сопровождения и диагностики системы занимают гораздо меньше времени ввиду большей гибкости системы и наличия развитых средств ее отладки и диагностики. Узлы полевой шины обладают возможностями интеллекта, реализованного аппаратно, что сводит к минимуму усилия, необходимые для конфигурации, установки и сопровождения сети [13].

Вместе с тем следует назвать и проблемы, которые возникают при объединении в сеть: электронные компоненты устанавливаются вблизи технологических процессов, где встречается достаточно много помех [8]. Более того, интеллектуальные компоненты должны обеспечиваться энергией, что снижает уровень безопасности. Эти трудности преодолевают с помощью введения стандартов на взрывозащищенное и искробезопасное оборудование, которые устанавливают строго определенный предел уровня помех и потребляемой мощности устройств [9].

Основные требования к сетям информационного обмена. Автоматизация информационно-управленческих процессов – задача сложная, и необходимо учитывать следующие требования:

1. Автоматизация должна выполняться в условиях реального времени, т.е. замеры параметров и выдача управляющих сигналов должны выполняться своевременно, при поступлении сигнала. Своевременно должна осуществляться и выдача данных пользователю.

2. Реализация конкретной системы должна быть ориентирована на выполнение строго определенной задачи, следовательно, необходимо применять технические средства, соответствующие стандарту области применения системы.

3. Система должна быть гибкой и легко модернизируемой, поэтому в ней должно использоваться децентрализованное управление. Этим обеспечивается возможность добавления элементов в уже существующую систему. При построении АИУС к ним предъявляются следующие требования, которые необходимо учитывать на этапе их проектирования и реализации: работа в режиме реального

времени; применение стандартных интерфейсов передачи данных; децентрализованное управление.

Характер этих требований различен для конкретных информационно-управленческих процессов, но все они имеют общие особенности, которые обуславливаются их природой. Это связано с тем, что для реализации АИУС необходимо использовать строго определенную технологию, которая бы обеспечивала выполнение этих требований.

Работа в режиме реального времени. Одним из требований при реализации развернутых АИУС является измерение параметров в условиях реального времени. При построении системы этот фактор определяет скорость реакции исполнительного механизма сразу после поступления информации с датчика.

Любая система на основе данных, поступающих от датчиков, вырабатывает определенные команды для исполнительных механизмов. При этом необходимо, чтобы время, прошедшее с момента измерения, до начала работы исполнительного механизма согласно поступившей на него команде было настолько мало, чтобы величина, измеряемая датчиком, не успела значительно измениться. Это время складывается из времени измерения датчиком требуемой величины, времени передачи данных прикладной программе, времени обработки данных прикладной программой, времени передачи данных исполнительному механизму и времени срабатывания исполнительного механизма. В результате, необходимо учитывать факторы, которые влияют на время реакции исполнительного механизма. Если общее время больше времени изменения величины датчика, и известно каждое слагаемое этой величины, то можно учесть это в программе и тем самым улучшить динамику системы. Это необходимо учитывать при выборе элементной базы.

Более критическим, чем общее время, фактором являются фазовые флуктуации – непредсказуемое варьирование времени передачи данных, которое заметно мешает управлению. Чаще всего их причиной являются прикладная программа и передача данных, реже − датчики и исполнительные механизмы. Фазовые флуктуации, возникающие при передаче данных, могут иметь самую различную природу. Маркерным методам доступа характерны фазовые флуктуации, зависящие от конкретного протокола и загруженности шины. Фазовые флуктуации, зависящие от нагрузки на шину, возникают и при использовании метода множественного доступа (Carrier Sense Multiple Access (CSMA)) или из-за появления коллизий (в обоих случаях причиной является высокая нагрузка на шину). Фазовые флуктуации, возникающие при высокой нагрузке, зависят от времени занятия шины отдельными устройствами. Это время зависит от длины сообщения и скорости передачи данных. Практически все протоколы, реализованные как аппаратно, так и программно, порождают зависящие от конкретной реализации фазовые флуктуации. Их можно избежать только при централизованном управлении доступом к среде передачи данных, но в этом случае увеличивается среднее время задержки. Особенно это заметно при небольшой нагрузке на шину [4].

Факторами, влияющими на скорость передачи данных, являются общее время реакции и фазовые флуктуации. Для обеспечения возможности работы в режиме реального времени необходимо при проектировании системы учитывать следующие особенности:

Вид передающей среды. В зависимости от задачи и конкретной ее реализации можно использовать различные передающие среды. Передающая среда определяет такие параметры, как скорость передачи данных, расстояние, на которое эти данные можно передавать. Выбор передающей среды должен быть ориентирован на указанные параметры. При изменении этих параметров структура системы не должна изменяться. Если структура системы изменяется, то возникают дополнительные затраты на создание новой. Также система должна обеспечивать возможность изменения передающей среды при ее функционировании. Эта характеристика должна быть учтена при выборе новой элементной базы.

Используемые устройства обработки информации. При реализации крупных систем устройства обработки информации должны удовлетворять параметру реального времени. Устройство должно обрабатывать сигналы с необходимой скоростью, для выдачи управляющего воздействия. Также устройство обработки данных должно обеспечивать выполнение функций и решение задач, реализуемых в этом узле.

Протокол передачи данных. Протокол передачи данных определяет способ доступа к среде передачи данных и отвечает за пересылку пакетов между узлами системы. В зависимости от используемого протокола в сети могут возникать задержки по передаче данных. При реализации системы это также необходимо учитывать. Модель системы должна быть универсальной, чтобы была возможна ее реализация с помощью любого протокола передачи данных. Изменение протокола передачи данных не должно влиять на работоспособность и функционирование системы. Особенно этот фактор не должен влиять на пользователей системы. Вне зависимости от протокола передачи данных система должна работать стабильно.

Способы доступа к шине. Способ доступа к шине определяет работу каждого узла в сети. При его выборе должны учитываться следующие факторы: время доступа к шине и скорость изменения параметров. При этом необходимо, чтобы этот фактор не влиял на все остальные. Только при учете данных особенностей можно обеспечить выполнение требования реального времени. Преимущество использования стандартных интерфейсов заключается в том, что все необходимые характеристики известны, и можно определить, подходит ли выбранный интерфейс для реализации системы. При разработке собственного интерфейса передачи дан-

ных эти факторы должны быть выявлены при тестировании системы на основе данных об элементной базе.

Применение стандартных интерфейсов передачи данных. При построении распределенной АИУС требуется, чтобы она обладала небольшой стоимостью. В АИУС на основе полевых шин это достигается использованием простых интеллектуальных узлов. Под каждую конкретную реализацию используются только минимально необходимые аппаратные средства.

Исторически сложилось, что в России для АИУС применяются микро-РС [1, 14]. Микро-РС представляет собой полноценный промышленный компьютер, выполненный в прочном к удару и взрывобезопасном исполнении [15]. Применение данной аппаратной базы обусловлено тем, что для нашей страны эта технология является стандартным решением, и существует множество разработок таких систем. Реалии сегодняшнего дня таковы, что дальнейшее использование микро-РС становится уже не эффективным. Возникают дополнительные затраты на модернизацию систем, изменение параметров и настроек в уже реализованных системах. Это особенно влияет на распределенные системы. В этом случае объект автоматизации располагается на большой площади и применение микро-РС становится просто нерентабельным. При автоматизации с применением микро-РС разработчики сталкиваются со следующими проблемами:

1. Нерентабельность крупных проектов. Применение микро-РС для работы с небольшим количеством датчиков увеличивает стоимость системы.

2. Неэффективное использование аппаратного обеспечения. Изначально заложенная мощность устройств не позволяет использовать их эффективно.

3. Излишняя универсальность Микро-РС. При проектировании распределенных систем необходимо использовать устройства, имеющие ограниченный и строго определенный спектр функций, необходимых для реализации отдельных функций узла.

4. Сложность разработки программного обеспечения. Для каждого конкретного случая системы автоматизации с применением микро-РС необходимо создавать свое собственное программное обеспечение. В большинстве случаев не существует программного обеспечения для конкретной реализации системы.

5. Малая мощность системы. Для того, чтобы максимально эффективно использовать ресурсы вычислительной системы, все устройства в ней необходимо объединить в сеть. При реализации систем на микро-РС возникает проблема управления всеми датчиками с помощью одного узла. В результате, вычислительная нагрузка на каждом уровне автоматизации возрастает в геометрической прогрессии. Если на программном уровне управление осуществляется небольшим количеством компонентов, и реализация системы не сложна, то на уровне датчиков и исполнительных механизмов сложность возрастает в десятки раз. А при использовании интеллектуальных узлов сетей на основе полевых шин, функции управления распределяются равномерно по всем узлам. В результате общая мощность работы приложения при одинаковых затратах на реализацию системы, с использованием микро-РС меньше, чем в распределенных системах.

6. Большая вычислительная нагрузка. При использовании микро-РС вычислительная нагрузка всей сети возлагается на отдельный узел системы. В такой системе датчики не обладают интеллектом и поэтому не могут реализовывать функции управления, поэтому при выходе из строя управляющего элемента, система полностью парализуется. При использовании датчиков, обладающих интеллектом, функции управления возлагаются на вычислительную сеть. У каждого узла строго определены функции и задачи, которые он должен выполнять, и он в этом случае не зависит от остальных элементов системы. В результате, при отключении такого устройства, работа системы не прекращается. Обмен информацией в этом случае выполняется с использованием специальных средств, и в обмене информацией участвует только необходимое количество датчиков.

Если при проектировании автоматизированной системы не учесть эти факторы, то при ее эксплуатации могут возникнуть трудности с поддержанием ее в рабочем состоянии. Реализация АИУС с применением стандартных интерфейсов передачи данных позволяет использовать технологии с применением интеллектуальных датчиков. Эта проблема является на данный момент актуальной только в пределах России. В странах Европы проектирование систем осуществляется с применением стандартных интерфейсов, для которых определены способы передачи данных в условиях автоматизированной системы [5].

Требование децентрализованного управления. Существующие разработки АСУТП можно разделить на две категории: Системы, использующие централизованное управление; системы, использующие интеллектуальные датчики и узлы управления.

На данный момент в России в большинстве случаев используются системы, принадлежащие к первой категории. Эта особенность обусловлена тем, что в автоматизированных системах применяются микро-РС, и реализовать децентрализованное управление на этом уровне достаточно сложно [5].

Для создания эффективной АИУС необходимо использовать полевые шины, базирующиеся на существующих стандартах по интерфейсам передачи данных, как европейских, так и российских.

Проблемы функционирования сетей информационного обмена. Постоянный рост числа информационно-управляющих сетей и увеличение сложности устанавливаемых систем, требуют все более сложных инструментов диагностики сетей для получения качественного сервиса, предоставляемого этими сетями. Таким инструментом может стать

программно-аппаратный комплекс оптимизации ресурсов сетей АИУС. Основой его является анализатор протокола или средство мониторинга сети. Подобно тому, как отладчик контролирует выполнение программы в процессоре и помогает программисту на этапе проектирования, анализатор протокола отслеживает трафики в канале связи и помогает системным интеграторам и администраторам сети обозревать, анализировать и диагностировать поведение сети.

Увеличение времени ответа. Проблемы такого рода для информационно-управляющей системы, использующей в качестве среды для передачи сигналов управления сети на основе полевых шин, выражаются в несоблюдении параметров процесса с течением времени. Эти проблемы могут быть связаны с неправильной конфигурацией узлов сети и ошибками программного обеспечения, на них функционирующего. Не существует четкого и однозначного решения проблем подобного типа. Пользуясь анализатором протокола необходимо исследовать время реакции узлов при выполнении тех или иных операций. Следует сравнить этот показатель с конкретными тактовыми интервалами данной системы и точно вычислить фактическое время реакции.

Некоторые анализаторы протоколов способны анализировать события сети и регистрировать соответствующие им интервалы времени. Анализатор протокола – средство, позволяющее "выхватить" событие целиком и определить узкое место в работе сети (Рис. 5). После локализации неисправности аналитик может исследовать конфигурацию сети и внести соответствующие коррективы.

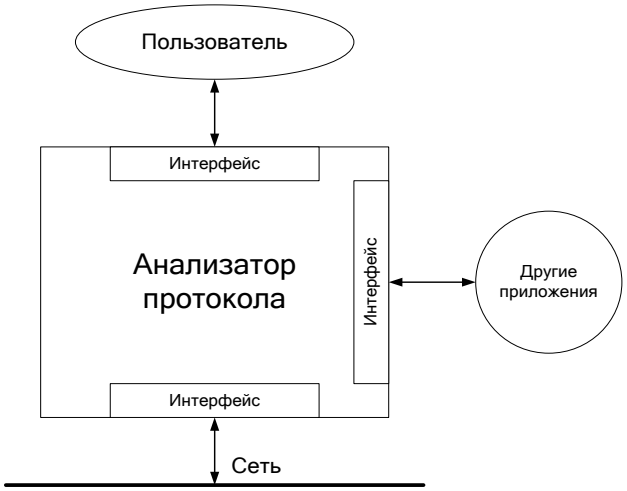


Рис. 5. Анализатор протокола [12]

Неэффективность программного обеспечения узлов сети. Эта проблема возникает в том случае, если программное обеспечение сетевого устройства написано неграмотно или содержит ошибки. Очень большое значение имеет реализация операции с плавающей точкой, так как многие из контроллеров не содержат средств поддержки таких операций. Анализатор протокола может определить, действительно ли программное обеспечение узла работает так, как это указано в паспорте разработчика.

Реализация аппаратных и программных технологий. Многие узлы сети используют лишь половину паспортной мощности и производительности. Большинство из них имеет некоторую совокупность конфигурационных параметров, которые можно изменять. Но единственный способ выяснить, действительно ли они хорошо работают в сети, заключается в проверке эффективности обмена информацией с конкретными устройствами. Анализатор протокола способен установить, справляется ли узел со своими задачами.

Несовместимость устройств в сети. Необходимо всегда обеспечивать возможность совместной работы всех устройств, включенных в инфраструктуру сети. Часто трудно выявить несовместимую рабочую версию программы или конкретный драйвер сети, для чего требуется анализатор протокола.

Тогда следует провести наращивание версии или реконфигурацию программного обеспечения с целью устранения сетевой ошибки и повышения степени взаимодействия между аппаратными платформами.

Изменение размеров блоков и пакетов. Размер блока является характеристикой различных типов пакетов, используемых протоколом при передаче в сети. Размер блока связан с объемом данных, который приложение или процесс помещает в пакет при передаче. С помощью анализатора протокола при передаче и приеме можно выявить пакеты, исходящие от различных устройств сети. Размеры блока могут считаться неэффективными в зависимости от инфраструктуры сети и используемого типа передачи.

Применение средств анализа и диагностики сетей является необходимым и актуальным. Возможности использования такого инструмента для отладки и тестирования сетей достаточно велики.

Литература

1. Артемов С. П. Проблемы автоматизации зданий и производственных процессов. // В кн.: Информационные управляющие системы // Межвузовский сборник научных трудов. – Пермь: ПТГУ, НИИУМС, 1999.

2. Башарин Г. П. Анализ очередей в вычислительных сетях. Теория и методы расчета / Г. П. Башарин, П. П. Бочаров, Я. А. Коган - М.: Наука. Гл. ред. физ.-мат. лит., 1989. - 336 с.

3. Башарин Г. П. Локальные сети программируемых контроллеров для гибких производственных систем./ Г. П. Башарин, В. А. Ефимушкин, А. Б. Черпаков – М., Изд-во УДН, 1987, 380 с.

4. Белковский С. В. Программно-аппаратный комплекс повышения производительности сетей промышленной автоматизации на основе анализа протокола: дис. канд. техн. наук: 05.13.07: защищена 24.05.2000: утв. 3.10.2000 / Белковский Сергей Викторович. – Пермь, 2000. – 176 с. – Библиогр.: С. 161-166.

5. Белковский С. В. Программно-аппаратный комплекс повышения производительности сетей промышленной автоматизации на основе анализа протокола: дис. канд. техн. наук: 05.13.07: защищена 24.05.2000: утв. 3.10.2000 / Белковский Сергей Викторович. – Пермь, 2000. – 176 с. – Библиогр.: С. 161-166.

6. Злотников Ю. С. Протоколы информационного обмена в цифровых сетях связи с интеграцией служб / Ю. С. Злотников // Зарубежная радиоэлектроника, 1990. – № 10. – С. 46-65.

7. Gaffney J. E. A Genera Economics Model of Software Reuse / J. E. Gaffney, Jr. and R. D. Cruickshank. - Association for Computing Machinery, Australia. - May 1992. – P. 22-32.

8. Принципы построения промышленных микроконтроллерных сетей в стандартах Profibus и P-NET / Артемов Н. И., Низамутдинов О.Б., Гордеев М.В. и др. - Пермь: ПГТУ, НИИУМС. - 1996.

9. Gaffney J. E. Software Reuse Key to Enhanced Production; Some Quantitative Models / J. E. Gaffney, Jr. and T. Durek. - Software Productivity Consortium, SPC-TR-88-015. - George Mason University, Center for Software and System Engineering. - Herndon, VA. - April 1988. – P. 42-52.

10. Gavin. Modeling and Analising of Security Protocols / Gavin [and a.]. – Addison Wesley. – 2000. – 352 p.

11. Hoare C. A. R. Formal Methods in Computer System Design / C. A. R. Hoare. - CERN School of Computing, Oxford, UK, 15-26. - CERN Sci. Rept. 6, 1989. - P. 1-7.

12. OSF/MOTIF, Open Software Foundation, MOTIF Release 1.2. – 43 p.

13. Белковский С. В. Концепция полевых шин в распределенных системах управления. // Информационные управляющие системы: Межвузовский сборник научных трудов./ Пермский ТГУ. – Пермь, НИИУМС, 1999. Вып. 42, С 116-128.

14. Белковский С. В. Анализ протокола в системах полевых шин/ С. В. Белковский // Теоретические и прикладные аспекты информационных технологий: Сб. науч. тр. / Пермский ТГУ. – Пермь, НИИУМС, 1999, Вып. 48, С 136-138.

15. Надежность и эффективность в технике: Справочник в 10 т. Т. 3. Эффективность технических систем / Под общ. ред. Ф. В. Уткина, Ю. В. Крючкова. – М.: Машиностроение, 1988. – 328 с.

Санкт-Петербургский университет Государственной противопожарной службы МЧС России

ANALYSIS OF THE CONCEPT CREATION OF NETWORKS OF INFORMATION EXCHANGE

A.S. Krutolapov, D.A.Sychev

Offers an analysis of methods of creation of networks of information exchange with use of field tires, advantages of the distributed control systems are shown, the main indicators of their working capacity are shown.

Keywords: *network, data transmission, automated system, dispatching management, message, information, quality of service.*

УДК 0.049 + 353.5

ПРОГРАММНО-АППАРАТНАЯ ПЛАТФОРМА ДЛЯ ОБЕСПЕЧЕНИЯ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ РУКОВОДИТЕЛЕЙ ТЕРРИТОРИАЛЬНЫХ ПОДСИСТЕМ РСЧС

В.А. Седнев, В.М. Клецов

Предлагается технология сбора и обработки информации, позволяющая объединить используемые в органе управления автоматизированные системы и информационные ресурсы на одной программно-аппаратной платформе для повышения эффективности деятельности должностных лиц РСЧС.

Ключевые слова: *территориальные органы исполнительной власти, поддержка принятия решений, автоматизированные системы, программно-аппаратная платформа.*

Специфика деятельности территориальных органов исполнительной власти (ТОИВ), характер их взаимодействия с другими органами исполнительной власти, населением и хозяйствующими субъектами обуславливает разнородность решаемых задач, выполняемых функций и сложность обрабатываемой информации. К одним из основных задач ТОИВ относятся: создание территориального звена городской территориальной подсистемы единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС); координация деятельности и взаимодействия с территориальными органами федеральных органов государственной власти в сфере обеспечения комплексной безопасности, и др. При этом основными приоритетами Российской Федерации на период до 2020 года являются создание и дальнейшее развитие информационного общества.

Целями государственной политики в области развития информационно-коммуникационных технологий (ИКТ) являются совершенствование системы государственного управления и развитие экономической, социально-политической, культурной сфер жизни общества. Государственное регулирование в сфере применения информационных технологий (ИТ) предусматривает регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации. Например, основным назначением информатизации задач управления административного округа (АО) Москвы является обеспечение ТОИВ оперативной, аналитической и прогнозной информацией для поддержки принятия решений в сфере управления округом и районом. В направлении информатизации управления АО можно выделить развитие средств совместной работы должностных лиц (ДЛ) ТОИВ на основе информационного ресурса (ИР) округа.

Интеграция городских информационных систем (ИС) и ресурсов возложена на метасистему «Электронная Москва», в то же время ИР АО не подлежат включению в ее состав. В зависимости от задач, решаемых ДЛ, используется различное программное обеспечение (ПО), при этом демонстрируется заинтересованность АО в повышении автоматизации и информатизации своей деятельности, а, с другой стороны, выявлены различные подходы к решению этих задач, что негативно влияет на их реализацию. Использованию потенциала ИКТ препятствует разрозненность ИР и систем; локальная автоматизация; дублирование функций различными системами; несовместимость данных в различных ресурсах; отсутствие полной и достоверной информации, а также необходимой нормативной правовой базы федерального и регионального уровней. Также остаются актуальными вопросы обеспечения информационной безопасности (ОИБ) и защиты персональных данных (ПДн) в ТОИВ [1].

Проведенный анализ показал: при создании ИС не решаются вопросы интеграции, стандартизации, унификации и обеспечения совместимости, отсутствуют механизмы контроля за использованием ИР, обеспечением их полноты и достоверности, ряд ИС не соответствует требованиям по полноте, доступности, целостности и конфиденциальности имеющихся в них информации, а держатели ИР часто не заинтересованы в том, чтобы информация их баз данных (БД) могла использоваться другими подразделениями или хозяйствующими субъектами; в отраслевых и ведомственных системах не учитываются потребности округов, за исключением возможностей просмотра информации и получения некоторых форм отчетности, а округа при решении задач информатизации пытаются эти задачи решать самостоятельно, не опираясь на общегородские проекты. Анализ ПО и ИТ, применяемых ДЛ ТОИВ, позволил выявить их типовые элементы: системное ПО, – основано на решениях Microsoft, и, как правило, присутствует сервер для хранения неструктурированной информации; для защиты информации используется антивирусное ПО; прикладные системы (документооборота, электронной почты, бухгалтерского учета, кадрового учета, геоинформационные); инфраструктура серверных помещений; телекоммуникационная инфраструктура.

В связи с необходимостью развития территориального звена Московской городской территориальной подсистемы РСЧС, и, в целом, для повышения эффективности управления территориями АО,

Седнев Владимир Анатольевич - Академия ГПС МЧС России, доктор технических наук, профессор, тел. 8(495) 617-27-79; e-mail: sednev70@yandex.ru;
Клецов Владимир Михайлович - соискатель Академии ГПС МЧС России, 8(499)149-69-82; kletsovVM@mos.ru.

на которых сосредоточены огромные социальные и материальные ресурсы, требуется разработка программно-аппаратной платформы (ПАП), позволяющей руководителю ТОИВ получать необходимую информацию из прикладных программ, которые функционируют независимо и являются специфичными для каждой сферы деятельности подразделений префектуры, подведомственных организаций и учреждений. Создание ПАП предполагает реализацию принципов: системности, обеспечивающего целостность отдельных систем и взаимодействие с другими системами; открытости системы, предполагающего расширение функций без нарушения ее функционирования; совместимости, реализующего интерфейсы, благодаря которым ПАП может взаимодействовать с другими системами; и стандартизации, применяя типовые элементы.

Программно-аппаратная платформа должна быть предназначена для: автоматизации процессов сбора, обработки, подготовки, хранения, отображения и передачи информации ДЛ всех уровней ТОИВ; доставки информации до автоматизированных рабочих мест (АРМ) ДЛ, принимающих решения и участвующих в их подготовке; автоматизации решения информационно-расчетных задач (ИРЗ); анализа данных и их прогнозирования; ведения БД; управления подчиненными объектами, и, в целом, для повышения эффективности информационного обеспечения и принятия различных управленческих решений ДЛ ТОИВ, при этом ПАП предполагает возможность подключения других АС и способствует расширению возможностей установленных систем, ранее не реализуемых. На основании проведенных исследований обоснованы требования к ПАП, включающие требования в целом, к ее функциям и видам обеспечения (рис. 1).

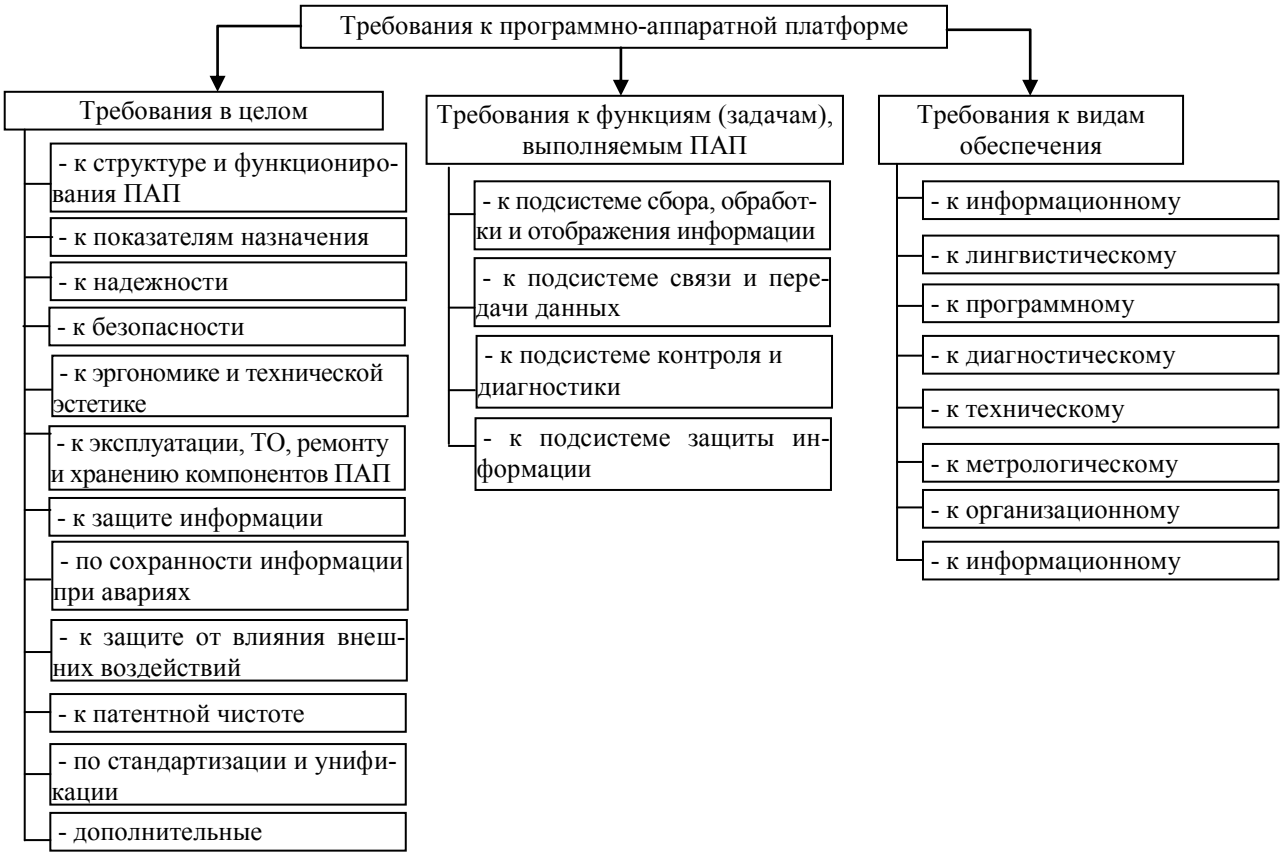


Рис. 1. Требования к программно-аппаратной платформе

Основные требования к ПАП в целом включают:

- требования к структуре и функционированию: ПАП должна быть реализована в виде стационарной иерархической территориально распределенной автоматизированной системы (АС) сбора, обработки, отображения и передачи информации; в структуре ПАП должны быть предусмотрены подсистемы: сбора, обработки и отображения информации – для приема данных от источников, их обработки, регистрации, хранения и выдачи ДЛ ТОИВ; связи и передачи данных; контроля и диагностирования работоспособности системы; информационный обмен данными должен обеспечиваться с использованием единого протокола обмена по каналам связи и передачи данных; должно быть предусмотрено два режима функционирования ПАП: рабочий, при котором обеспечивается круглосуточное решение функциональных задач, и режим технического обслуживания (ТО) для поддержания работоспособности системы;

- требования к показателям назначения: в процессе сбора, обработки, отображения и документирования информации должен предусматриваться ее отбор по видам и важности; представление средствами отображения информации (СОИ) АРМ ДЛ и руководителей ТОИВ одних и тех же данных должно быть одинаковым; должна быть обеспечена возможность разделения экрана СОИ руководителей ТОИВ на несколько «окон» для отображения разных районов с различными видами данных; в элементах ПАП должны быть обеспечены: регистрация входных и выходных сообщений; документирование результатов обработки информации, и др.;

- требования к надежности: за критерий отказа принимается прекращение выдачи информации или ее недостоверность, отказ элемента ПАП или функционирования какого-либо расчетно-аналитического модуля, приводящий к невозможности выполнения основных функций системы;

- требования к защите информации: защите подлежат данные, поступившие в ПАП на хранение и обработку от ДЛ; данные, полученные в процессе обработки исходных данных; нормативно-справочные, служебные и вспомогательные данные, включая и данные системы защиты, персональные данные; программы для обработки данных и обеспечения функционирования ПАП, включая и программы системы защиты информации; документация на объектах ПАП. Необходимость защиты информации объясняется предупреждением возникновения ситуаций (инцидент, авария, катастрофа), которые могут повлиять на работу ПАП и достоверность информации, получаемой ДЛ ТОИВ. Для обеспечения работы ПАП разработана модель угроз информационной безопасности (ИБ) и модель вероятного нарушителя системы, с учетом особенностей ее функционирования, включая взаимодействие с внешними источниками информации, и др.

Требования к функциям ПАП включают требования к функциям следующих подсистем:

- сбора, обработки и отображения информации: сбор, обработка, хранение, отображение и документирование информации от административных и хозяйствующих объектов; вывод на СОИ АРМ ДЛ обстановки; прогнозирование развития события; отображение результатов обработки данных; сбор, хранение, отображение и документирование информации о состоянии ресурсов и средств их использования; оповещение при возникновении нештатных ситуаций, и др.;

- связи и передачи данных: автоматизированный ввод в ТС обработки данных информации от АРМ ДЛ; автоматический обмен данными между взаимодействующими системами, и др.;

- защиты информации, – должны обеспечиваться управление доступом к информации; аудит событий; контроль целостности; администрирование; антивирусная защита; обнаружение и противодействие компьютерным атакам, и др.;

- контроля и диагностики: логический контроль вводимой в систему информации, контроль работоспособности системы в процессе функционирования, тестовый контроль системы в режиме ТО, диагностика неисправностей.

Основные требования к видам обеспечения включают требования:

- к информационному обеспечению, – должно быть реализовано в виде комплексов информационных средств, с помощью которых в отдельных частях системы осуществляется обработка информации, и обеспечивать: полноту отображения предметной области, многократное использование данных при их однократном вводе; информационную совместимость между частями системы; разграничение доступа к данным; системы управления базами данных (СУБД) должны иметь интерфейсы с языками программирования высокого уровня, и др.;

- к программному обеспечению, – должно обладать: функциональной достаточностью, надёжностью, адаптируемостью, модифицируемостью, модульностью построения, удобством в эксплуатации. В качестве общесистемного ПО должно использоваться, в части: операционной системы (ОС) – ОС семейства Microsoft Windows; СУБД – MS SQL Server 2008 R2; веб-сервера – Microsoft Internet Information Server; прикладное ПО должно быть разработано на платформе управляемого кода Microsoft NET в среде Visual Studio 2010. Специальное ПО включает имеющиеся в АС расчётно-аналитические модули, обеспечивающие обработку информации и прогнозирование показателей деятельности ТОИВ, и должно быть реализовано в виде комплексов программных средств составных частей системы. Общее ПО должно обеспечивать наращивание общесистемных функций системы, запуск и контроль ее функционирования, реализацию многозадачного режима работы, поддержку наращивания специального ПО;

- к техническому обеспечению, – в состав комплекса средств автоматизации (КСА) ДЛ, в зависимости от уровня, должны входить: средства сбора, обработки и отображения информации, сформированные в АРМ в соответствии с структурой ТОИВ; средства обмена информацией между АРМ ДЛ; средства связи и обмена данными с взаимодействующими объектами; аппаратно-программные средства защиты информации (СЗИ); необходимые контрольно-измерительные приборы, и др.;

Таким образом, программно-аппаратная платформа представляет собой программно-аппаратный комплекс поддержки принятия решений ДЛ ТОИВ, особенностью которого является объединение и использование возможностей установленных АС и ИР для анализа, моделирования и прогнозирования различных процессов в интересах повышения эффективности деятельности ТОИВ и управления подчиненными подразделениями и территориями на единой основе, реализуемой базой

данных, управляемой виртуальной оболочкой, включающей банк и систему управления данными, расчётные и графические модули, позволяющей реализовать модульность построения системы, использовать открытые промышленные стандарты, обеспечивающие интеграцию различных АС, и, в целом, системный подход к деятельности ТОИВ. Конечной целью создания ПАП является повышение эффективности деятельности ТОИВ и качества принимаемых его ДЛ управленческих решений. На ее основе обеспечивается информационно-аналитическая поддержка процессов анализа, моделирования и прогнозирования развития ситуации и выработки эффективных решений по направлениям деятельности ТОИВ. База данных (рис. 2) состоит из трёх функциональных модулей (СУБД, коррекции, банка данных) и четырёх программных генераторов (стохастизма, транзактов, динамики, расчётно-графического). Модуль коррекции БД предназначен для реализации динамических обратных связей, изменяющих банк данных (рис. 3).

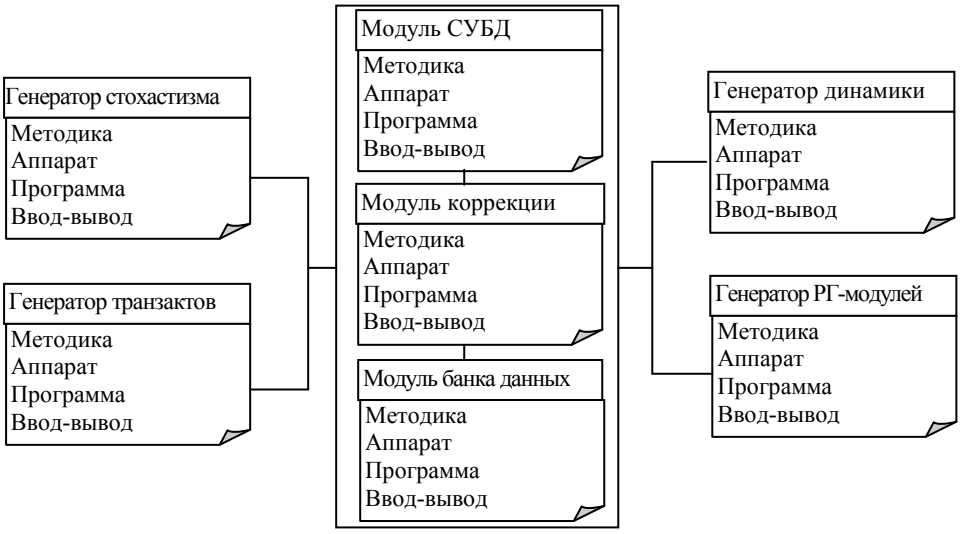


Рис. 2. Структура базы данных

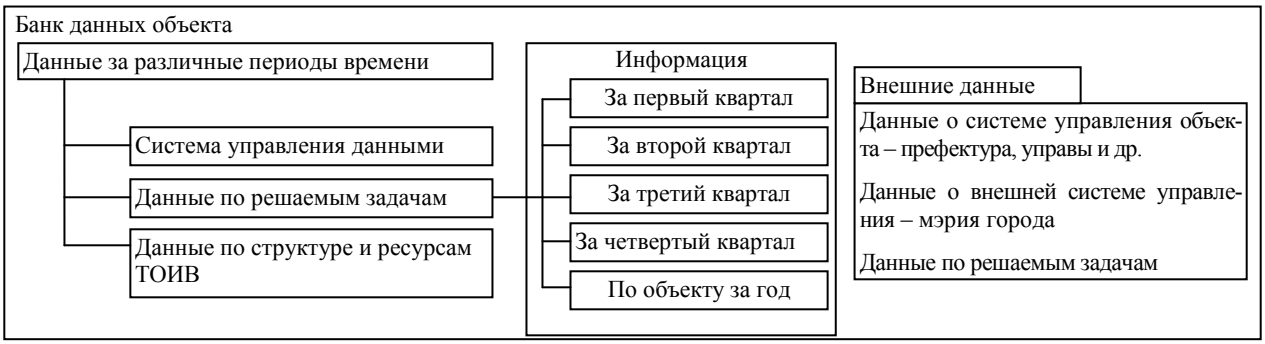


Рис. 3. Состав банка данных

Функционирование модуля обеспечивается программными генераторами [2]: стохастизма, транзактов, динамики, расчётно-графическим. Генераторы являются посредниками между БД и виртуальной оболочкой платформы и расчётно-графическими модулями и обеспечивают: стохастизма – реализацию случайных процессов, приводящих к изменению БД; транзактов – функции источника и поглотителя событий, требующих коррекции БД; динамики – устойчивость вектора модельного времени; расчетно-графический – связь БД с расчетно-графическими модулями. Банк данных должен включать структурированную, иерархически построенную, именованную совокупность данных ТОИВ, состоящих из внутренней и внешней частей: внутренняя формируется из системы управления и данных по задачам и структуре объекта, систематизируемых по годам, кварталам и месяцам; внешняя должна содержать динамическую информацию о системе управления префектуры и подчиненного объекта. При этом возможно два варианта использования ПАП: в одном случае она рассматривается как инструмент управления ТОИВ, во втором применяется для анализа и прогнозирования показателей ТОИВ. Основные уровни платформы ТОИВ (рис. 4): уровень первичной обработки данных, - включает в себя объектно-ориентированный интерфейс прикладного программирования и интерфейс объектного языка запросов – SQL-язык; уровень поставщика данных, - представлен СУБД Microsoft SQL Server

2008; уровень предметной обработки данных, - предполагает разработку решений на основе результатов решения задач, полученных от уровня первичной обработки данных; уровень взаимодействия ДЛ с ПАП, - отвечает за ввод/вывод информации, получение отчётов, визуализацию результатов. В качестве системы управления в ПАП предлагается использовать плагинную архитектуру, предполагающую наличие менеджера плагинов, самих плагинов, взаимозаменяемого модуля, программно-завершённого модуля, что позволяет обеспечить инкапсуляцию данных и функций, наследование и полиморфизм. Главное окно ПАП, управляемое виртуальной оболочкой, должно включать панели управления внутренней и внешней средой. Элементы управления и дизайн окна предлагается выполнять с помощью VSM-конструктора – совокупности скриптов и плагинов, разработанных в среде Visual Studio 2010, предназначенных для визуального и интерактивного отображения данных в Microsoft SQL Server 2008 R2. Для разработки панелей управления и согласованной работы плагинов оболочки и программных модулей предлагается использовать OLAP-технологию, основанную на аналитической обработке данных в режиме реального времени, позволяющую извлекать информацию из БД, структурировать, дополнять, обрабатывать данные, подготавливать их для расчётно-графических модулей, обновлять БД на основе полученных расчётов, осуществлять визуализацию результатов.

Рис. 4. Порядок обработки и учета данных

Информационное и программное обеспечение ПАП должно предполагать возможность ее функционирования в режимах моделирования, прогнозирования и управления. Информационный фонд (базы и банки данных) должен содержать набор данных по объектам управления, систему классификации и кодирования информации. В состав ПАП отдельных ДЛ будут входить средства автоматизации, система связи и передачи данных, система защиты информации, – с учетом этого ПАП, в целом, должна включать системы: сбора и обработки данных (ССОД); хранения информации (СХИ); сохранности данных; анализа информации; поддержки принятия решения; визуализации информации; обеспечения безопасности информации.

Система сбора и обработки данных должна аккумулировать данные с разных источников информации, находящихся на территории АО. Получение достоверной информации от ССОД или СХИ позволяет осуществлять быстрый анализ данных, применяя имеющиеся статистические и математические алгоритмы. Для получения необходимой информации потребуется собирать данные из БД различной структуры и содержания, которые характеризуются противоречивостью информации, – для устранения этого недостатка предлагается интегрировать в БД данные исторических архивов и поступающей информации из внешних источников.

Система хранения информации должна обеспечивать хранение разнородных данных с консолидированием поступающей информации в нескольких БД и представлять собой программно-аппаратное решение по организации надёжного хранения ИР и предоставлению гарантированного доступа к ним. В БД должна также сохраняться информация: об особенностях (типе) каждой подсистемы управления; о типах взаимоотношений между ними; о типах и количестве ТС подсистем; о типах ресурсов, потребляемых подсистемами; о величине потребления ресурса; о фактах перемещений ТС. Большинство задач ДЛ относится к классу информационно-аналитических, что требует соответствующего информационного обеспечения, которое не может быть реализовано классическими БД, так как они не предполагают изменения состояния объектов. Устранить этот недостаток могут информационные хранилища, строящиеся как многомерные структурированные совокупности данных, ориентированные на решение задач, связанных с анализом и прогнозом различных процессов. Объединение требований к динамике и разнообразию типов информационных потоков ПАП позво-

ляет дать характеристику технологий, формирующих архитектуру БД [2]: компонентная технология проектирования и перекомплектации предметно-ориентированных БД; расширенная технология хранилища различных данных, включающая средства оперативной аналитической обработки данных; открытость БД для включения в нее и получения из нее информации с использованием глобальной информационной магистрали. Предлагаемая структура БД позволяет хранить информацию об особенностях каждого объекта ТОИВ, при этом предполагается в качестве системы управления данными использовать MS SQL Server 2008 R2, графические и аналитические модули реализовывать в программной среде Mathcad, что повысит эффективность деятельности ДЛ ТОИВ. Разработанная ПАП позволяет реализовать механизм информационного обмена с использованием ИС и ресурсов АО посредством их интеграции, консолидации и унификации при обеспечении требований по полноте, доступности и целостности.

Таким образом, можно выделить следующие преимущества ПАП ТОИВ: единая точка доступа к ИР, с ограничением по доступу к ним ДЛ, зависящим от решаемых ими задач, что достигается модульностью формирования; быстрый поиск данных, экономия времени и повышение скорости принятия решений; удобство, - использование типового модульного компонента ПАП благоприятно влияет на ускорение рабочих процессов и эффективность работы ТОИВ в целом, при этом он реализует программно-целевые методы управления, предназначен для обеспечения информационной поддержки процессов управления и принятия управленческих решений ДЛ ТОИВ, и реализуется в режиме, обеспечивающем одновременную работу всех подразделений префектуры и управ районов АО, а формирование отчетов осуществляется с использованием механизмов выборки данных, не требующих навыков программирования.

Типовой компонент ПАП и сама ПАП обеспечивают: формирование сведений на основе данных ИС и ресурсов АО; мониторинг значений показателей и анализ их взаимозависимости; прогнозирование показателей; формирование отчётов. Модульность построения ПАП ДЛ позволяет, например, в сфере обеспечения безопасности, – повысить уровень безопасности населения, сократить число аварийных ситуаций, время реагирования экстренных служб. С целью повышения эффективности деятельности ДЛ ТОИВ разработаны предложения по применению и обеспечению функционирования ПАП, при этом успешное функционирование ПАП может быть осуществлено при выполнении ряда требований к организации БД: она должна обладать способностью к расширению; структура данных должна быть логичной и ясной; использование архитектуры и программных средств хранилища данных, средств оперативной аналитической обработки данных; применение методов компонентного проектирования предметных БД; исключение избыточности в данных; технологическая открытость, и др.

Реализация рассмотренного комплекса мероприятий обеспечивает информационно-аналитическую поддержку процессов анализа, моделирования и прогнозирования развития ситуаций и выработки эффективных управленческих решений по направлениям деятельности ТОИВ и повышает эффективность деятельности ДЛ территориальных подсистем РСЧС.

Литература

1. Подсистема информационной безопасности. Отчет о предпроектном обследовании: Отчет по НИР / ЗАО г. Москвы, Управление корпоративных сетей и администрирования информационных ресурсов ОАО «ГУП Экономика». – М., 2011. – 200 с.

2. Разработка требований и методов оценки качества энергосбережения и теплоснабжения населения и их влияние на риски чрезвычайных ситуаций: Отчет о НИР / ОАО «Средства спасения», ООО «КИЦ «Техноценоз»». – Москва, Калининград, 2011. – 454 с.

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Академия Государственной противопожарной службы МЧС России»

HARDWARE AND SOFTWARE PLATFORM TO SUPPORT DECISION-MAKING EXECUTIVES TERRITORIAL SUBSYSTEMS RSCHS

V.A. Sednev, V.M. Kletsov

New technology acquisition and processing features. It brings together all the used in the administration of automated systems and information resources on the same hardware and software platform to improve the effectiveness of emergency management officials.

Keywords: territorial executive authorities, decision support, information technology, automated information systems.

УДК 0.049 + 353.5

ПРЕДЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В ТЕРРИТОРИАЛЬНЫХ ОРГАНАХ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

В.М. Клецов, Н.С. Шимон*

В статье рассматриваются предложения по созданию системы информационной безопасности информации, обрабатываемой в разработанной программно-аппаратной платформе территориальных органов исполнительной власти, повышающие эффективность функционирования территориальных подсистем РСЧС (на примере административных округов).

Ключевые слова: *территориальные органы исполнительной власти, поддержка принятия решений, автоматизированные системы, программно-аппаратная платформа.*

Для обеспечения конфиденциальности и безопасности обрабатываемой в программно-аппаратной платформе (ПАП) информации от внешних и внутренних угроз разработана система информационной безопасности (СИБ) территориальных органов исполнительной власти (ТОИВ). Создание СИБ основывается на выявленных моделях угроз и модели нарушителя для информационных систем административного округа (ИС АО) и учитывает категорирование информации, обращающейся в системе, и систем, ее обрабатывающих. Объектами защиты являются прикладные системы, локальные вычислительные сети (ЛВС), телекоммуникационные компоненты, информационные ресурсы (ИР), средства вычислительной техники (СВТ). При этом реализуется комплекс защиты информации, обеспечивающий этапы ее передачи, обработки и хранения. В целом СИБ должна включать: инфраструктуру обеспечения безопасности, в которую входят средства защиты от несанкционированного доступа (НСД), антивирусную защиту и защиту от вредоносного содержимого, систему обнаружения и предотвращения вторжений и др.; комплекс механизмов и средств защиты информации (СЗИ), средств: разграничения и контроля доступа, обеспечения целостности информации, протоколирования и аудита и пр.; систему управления безопасностью (СУБ), включающую систему мониторинга и управления СЗИ, систему управления рисками, и др.

При создании СИБ должен реализовываться комплекс организационно-технических решений по обеспечению непрерывности деятельности ТОИВ, восстановлению работоспособности ИС и доступности информации после сбоев и аварий. Основываясь на проведенных исследованиях [1-3], определены основные требования к элементам СИБ, включающие:

- требования к структуре и функционированию СИБ, которая должна состоять из двух уровней решений: по защите ИР, осуществляющих обработку, передачу и хранение конфиденциальной информации; по обеспечению базового уровня защиты остальных ИР, компонент ИС, не обрабатывающих конфиденциальную информацию. Для реализации поставленных задач СИБ должна состоять из следующих технических решений: инфраструктуры сетевой безопасности, разграничения доступа и мониторинга сетевых активностей, обнаружения и предотвращения сетевых атак; системы безопасности узлов, приложений и баз данных (БД), обеспечения информационной безопасности (ОИБ) и мониторинга БД, ОИБ серверов; средств управления доступом в сети и в прикладных системах, идентификации и аутентификации должностных лиц (ДЛ) в ЛВС, идентификации ДЛ для систем, обрабатывающих конфиденциальную информацию; системы противодействия вредоносному содержимому, защиты от вредоносного содержимого электронной почты, антивирусной защиты на файловых серверах; системы обеспечения непрерывности предоставления информационных услуг (IT-услуг); СУБ; аналитические средства. Архитектура СИБ должна предполагать: многослойность, модульность и возможность адаптации системы к различным организационным и техническим условиям; независимость функционирования каждой из подсистем, и др.;

- требования к режимам функционирования системы, предполагающие обеспечение функционирования СИБ в следующих режимах: штатном (круглосуточный, 7 дней в неделю); сервисном (для проведения технического обслуживания без снижения уровня безопасности); аварийном (в случае возникновения нештатных ситуаций);

- показатели назначения, включающие: степень приспособляемости системы к отклонениям параметров объекта автоматизации: компоненты СИБ должны обеспечивать расширение круга защищаемых ресурсов, добавление или удаление объектов защиты, изменение времени хранения и накопления хранимой информации; технические решения должны обеспечить масштабируемость

Клецов Владимир Михайлович - соискатель Академия ГПС МЧС России, тел. 8(499)149-69-82; e-mail: kletsovVM@mos.ru;

Шимон Николай Степанович – начальник организационно-научного и редакционно-издательского отдела ФГБОУ ВПО «Воронежский институт ГПС МЧС России», кандидат технических наук, тел. 8(473)236-33-05; e-mail: vigps_onirio@mail.ru.

производительности и объема хранения данных в рамках ПАП при увеличении количества пользователей, узлов и компонент ИС, и др.

Требования к функциям, выполняемым СИБ, включают:

- требования к инфраструктуре сетевой безопасности, разграничения доступа и мониторинга сетевых активностей, - инфраструктура должна обеспечивать защиту ИР от сетевых атак; сегментирование сетей и выделение контуров, обрабатывающих конфиденциальную информацию;

- требования к единой системе идентификации, аутентификации и управления ДЛ и правами их доступа к сетевым и информационным ресурсам. Система должна обеспечить механизмы разграничения доступа к узлам и ресурсам ИС АО на основании матрицы доступа;

- требования к системе обеспечения непрерывности предоставления IT-услуг, которая должна функционировать в штатном и в экстренном режиме и обеспечивать резервное копирование и восстановление данных ИС префектуры; поддержку уровней иерархии для размещения резервных копий и архивных данных; создание дубликатов резервных копий данных и их удаленное хранение; мониторинг основных действий по копированию и восстановлению данных;

- требования к планированию аварийного восстановления. Система обеспечения непрерывности предоставления IT-услуг должна поддерживать: разработку планов аварийного восстановления для систем ТОИВ; включение в их состав в качестве статической информации схем, графиков, инструкций и других документов в общеупотребительных форматах, и др.;

- требования к средствам защиты – АРМ ДЛ и информация на них должны быть защищены от угроз, связанных с поступлением вредоносного содержимого, с сетевыми атаками, подключением внешних устройств и средств хранения информации. Для реализации этих задач комплекс технических средств (ТС) должен включать: системы антивирусной защиты; системы персонального межсетевого экранирования; системы контроля за действиями ДЛ и использованием съемных носителей, и др.

В целом СИБ должна выполнять задачи: контроля прав доступа ДЛ к ресурсам ИС; контроля текущего уровня защищенности; протоколирования и аудита, объединяющие в себе системы протоколирования прикладного общесистемного и специального программного обеспечения (ПО); оповещения администратора о сбоях в работе серверов, рабочих станций и средств защиты, о фактах вирусного заражения.

Требования к видам обеспечения СИБ включают:

требования к программному обеспечению, которое должно представлять собой совокупность общего и специального ПО, реализующего с техническими средствами цели и задачи СИБ. Для обеспечения интеграции смежных и наследуемых прикладных систем с СИБ и системой управления информационной безопасностью данные приложения должны обеспечивать интеграцию с внешними средствами идентификации, аутентификации и управления доступом ДЛ и интеграцию с внешними средствами протоколирования и аудита событий;

требования к техническому обеспечению. Аппаратные компоненты должны обеспечивать возможность диагностики, резервирования и взаимозаменяемости, устойчивость к ошибочным действиям ДЛ. Серверные компоненты должны обеспечивать возможность подключения внешних устройств хранения информации, дублирования критических компонентов и возможность их замены без выключения оборудования;

требования к организационному обеспечению. Организация работ по созданию СИБ должна включать оценку информационной инфраструктуры ТОИВ. В рамках создания СИБ должна быть определена: организационная структура, обеспечивающая реализацию мер по ОИБ, мониторинг и обслуживание СЗИ, анализ рисков и модернизацию систем защиты информации, и др.

Для защиты обрабатываемых персональных данных (ПДн) создана система защиты персональных данных (СЗПДн). Перечень объектов защиты определялся по результатам обследования префектуры ЗАО г. Москвы [1-2] и они включали: обрабатываемую информацию - персональные данные субъектов ПДн и сотрудников префектуры; технологическую информацию; программно-технические средства обработки; средства защиты; каналы информационного обмена; помещения, где размещены компоненты информационной системы Пдн (ИСПДн).

Персональные данные субъектов ПДн (гостей) и сотрудников префектуры включают более 70 категорий, в частности: фамилия, имя, отчество; место, год и дата рождения; гражданство; телефон; паспортные данные; фотография; информация об образовании, о пребывании за границей и др. Технологическая информация включает: управляющую информацию (конфигурационные файлы, настройки системы защиты и пр.); информацию средств доступа к системам управления; информацию на съемных носителях информации, содержащих информацию системы управления ресурсами; информацию о СЗПДн, их составе и структуре, принципах и решениях защиты; ИР, содержащие информацию о информационно-телекоммуникационных системах, о планах обеспечения бесперебойной работы, и др. Программно-технические средства включают в себя: общесистемное и специальное ПО (операционные системы, системы управления базами данных, и др.); копии общесистемного ПО; инструментальные средства и утилиты систем управления ресурсами ИСПДн; аппаратные средства обработки ПДн; сетевое оборудование.

Средства защиты ПДн состоят из аппаратно-

программных средств и могут включать в себя средства: управления и разграничения доступа пользователей; обеспечения регистрации и учета действий с информацией; обеспечивающие целостность данных; антивирусной защиты; межсетевого экранирования; анализа защищенности; обнаружения вторжений, и др. В ходе проверки определялись: состав и структура объектов защиты; конфигурация и структура ИСПДн; режим обработки ПДн; перечень и права лиц, участвующих в обработке ПДн; угрозы безопасности ПДн; существующие и необходимые меры защиты. Результаты обследования послужили основой для разработки соответствующих предложений. При обработке ПДн можно выделить угрозы: от утечки по техническим каналам; НСД к информации: угрозы уничтожения, хищения аппаратных средств, носителей информации; угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств; угрозы непреднамеренных действий ДЛ и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в ПО, от угроз неантропогенного и стихийного характера; угрозы преднамеренных действий внутренних нарушителей; угрозы удаленного запуска приложений, и др.

На основе оценки уровня защищенности ИСПДн рассчитывается коэффициент реализуемости угрозы и определяется возможность ее реализации. Оценка опасности угроз безопасности Пдн (УБПДн) определяется показателем опасности, который имеет три значения: низкая опасность – реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн; средняя опасность - реализация угрозы может привести к негативным последствиям для субъектов ПДн; высокая опасность - реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн. Оценка актуальности УБПДн показала, что для достижения требуемого уровня необходимо применять следующие методы и способы защиты: управление доступом; регистрация и учёт; обеспечение целостности; антивирусная защита; физическая охрана; тестирование функций системы защиты ПДн при изменении программной среды и пользователей; средства восстановления системы защиты ПДн.

Для обеспечения резервирования и восстановления работоспособности ТС, ПО, баз данных и СЗИ разработаны меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов, под которым понимается [2] некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн и с потерей защищаемой информации, которое может произойти в результате непреднамеренных действий пользователей, преднамеренных их действий и третьих лиц, нарушения правил эксплуатации ТС, возникновения внештатных ситуаций и обстоятельств непреодолимой силы. Обеспечение непрерывности работы и восстановления ресурсов при возникновении инцидентов основывается на технических и организационных мерах. К техническим относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как: жизнеобеспечения, обеспечения отказоустойчивости, резервного копирования и хранения данных, контроля физического доступа. Системы жизнеобеспечения включают [1]: пожарные сигнализации и системы пожаротушения; системы вентиляции и кондиционирования; системы резервного питания. После потери питания могут применяться локальные источники бесперебойного питания (ИБП) с различным временем питания для защиты отдельных компьютеров; ИБП с дополнительной функцией защиты от скачков напряжения; дублированные системы электропитания в устройствах; резервные линии электропитания в пределах здания; аварийные электрогенераторы.

Суть организационных мер состоит в следующем - резервное копирование и хранение данных необходимо осуществлять: для обрабатываемых ПДн - не реже раза в неделю; для технологической информации - не реже раза в месяц; копий ПО - не реже раза в месяц и каждый раз при внесении изменений в эталонные копии. На основании проведенных исследований разработан план мероприятий по обеспечению защиты ПДн (табл.), содержащий организационные, технические и контролирующие мероприятия.

Для обеспечения безопасности обработки ПДн при возникновении нештатных ситуаций и создания системы их защиты разработан: порядок реагирования на аварийную ситуацию, включающий действия при ее возникновении и уровни реагирования, а также технические и организационные меры обеспечения непрерывности работы и восстановления ресурсов. Аварийная ситуация становится возможной в результате реализации одной из возможных угроз: технологической; внешней; стихийных бедствий; телеком- и ИТ-угроз; угроз, связанных с человеческим фактором; угроз, связанных с внешними поставщиками.

При реагировании важно оценить критичность ситуации [1, 3]: уровень 1 - незначительный инцидент, определяется как локальное событие с ограниченным разрушением, которое не влияет на доступность элементов ИСПДн и средств защиты; уровень 2 – авария, - любой инцидент, который приводит или может привести к прерыванию работоспособности элементов ИСПДн и средств защиты, выходящий за рамки обязанностей ответственных за реагирование ДЛ, к ним относятся отказ элементов ИСПДн и средств защиты в результате повреждения водой, подтопления в период паводка или проливных дождей, и др.; уровень 3 – катастрофа, - любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей, к ним относят обстоятельства не-

преодолимой силы (пожар в здании, взрыв, просадка грунта с частичным обрушением здания, и др.).

Таким образом, под системой защиты персональных данных понимается комплекс организационных и технических мероприятий, направленных на обеспечение их безопасности. Комплекс средств защиты ИСПДн (КСЗ ИСПДн) – совокупность технических СЗИ, средств предотвращения НСД, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн, обрабатываемых автоматизированным способом. При этом под объектом внедрения понимается совокупность: ТС, позволяющих осуществлять обработку ПДн; помещений, в которых эти средства расположены; технологическое оборудование этих помещений; сетевая инфраструктура, обеспечивающая функционирование технических средств.

План мероприятий по обеспечению безопасности ПДн

Мероприятие	Периодичность и исполнитель
Организационные	
Проведение обследования; определение ПДн и объектов защиты; определение ДЛ, участвующих в обработке ПДн, и их ответственности; определение прав разграничения ДЛ; организация порядка резервного копирования защищаемой информации и восстановления работоспособности технических средств, ПО, БД и СЗИ; разработка инструкций о порядке обработки ПДн, обеспечения режима защиты, о действиях в случае возникновения внештатных ситуаций.	Разовое / обслуживающая организация (ОО). Сроки устанавливаются отдельно.
Назначение ответственного за безопасность ПДн; введение режима защиты ПДн; собрание коллегиального органа по классификации ИСПДн; классификация ИСПДн; выбор помещений для установки аппаратных средств ИСПДн с целью исключения НСД лиц, не допущенных к обработке ПДн; организация контроля доступа в помещения, в которых установлены аппаратные средства ИСПДн; введение в действие инструкции по порядку формирования, распределения и применения паролей; организация учёта ТС защиты и документации к ним.	Разовое / территориальный орган исполнительной власти. Сроки устанавливаются отдельно.
Технические (аппаратные и программные)	
Внедрение: хранилища зарегистрированных действий ДЛ с ПДн; подсистемы: управления доступом, регистрации и учета; обеспечения целостности; антивирусной защиты.	Разовое / ОО. Сроки устанавливаются отдельно.
Контролирующие	
Создание журнала внутренних проверок (ЖВП).	Разовое / ОО. Сроки устанавливаются отдельно.
Поддержание ЖВП в актуальном состоянии.	Ежемесячно/ТОИВ
Контроль: над соблюдением режима обработки ПДн; над выполнением антивирусной защиты; за обновлениями ПО.	Еженедельно /администратор безопасности (АБ)
Выявление изменений в режиме обработки и защиты ПДн.	Ежегодно/АБ
Контроль за обеспечением резервного копирования.	Ежемесячно/АБ
Анализ и пересмотр имеющихся угроз безопасности ПДн, предсказание появления новых угроз.	Ежегодно

Работа с объектом внедрения предполагает также соблюдение правил разграничения доступа (ПРД) – совокупности правил, регламентирующих права доступа субъектов доступа к объектам доступа. В ИСПДн, использующих средства автоматизации, ПРД реализуются ТС, которые обеспечивают реализацию правил доступа субъектов доступа к объектам доступа, а также автоматический контроль за соблюдением этих правил с регистрацией в электронной форме происходящих при этом событий. Под объектом доступа понимается единица ИР АС, доступ к которой регламентируется ПРД. Для КСЗ ИСПДн такими объектами являются защищаемые ПДн, технические и программные средства.

Обеспечение безопасности ПДн должно осуществляться в рамках системы защиты ПДн и состоять из согласованных организационных и технических мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн, минимизацию возможного ущерба, восстановление данных и нормальное функционирование ИСПДн в случае реализации угроз. Обязательным требованием для ИСПДн является создание в их составе СЗПДн, которая основывается на данных о ИСПДн и включает определение: перечня ПДн, подлежащих защите от НСД; условий расположения ИСПДн относительно границ контролируемой зоны; конфигурации и топологии ИСПДн, физических, функциональных и технологических характеристик ИСПДн;

ТС и систем, общесистемных и прикладных программных средств, их характеристик и условий расположения; режимов обработки ПДн в ИСПДн и в отдельных компонентах; определение класса ИСПДн; разработка частной модели угроз безопасности ПДн.

Реализация рассмотренных мероприятий обеспечит безопасность информации, обрабатываемой в программно-аппаратной платформе территориальных органов исполнительной власти, а также поддержку процессов анализа, моделирования и прогнозирования развития ситуаций и выработки управленческих решений ДЛ ТОИВ и повысит эффективность функционирования территориальных подсистем РСЧС.

Литература

1. Подсистема информационной безопасности. Отчет о предпроектном обследовании: Отчет по НИР / ЗАО г. Москвы, ОАО «ГУП Экономика». – М., 2011. – 200 с.

2. Проведение технологических работ по защите персональных данных в информационных системах префектуры ЗАО г. Москвы. Отчет о проведенном анализе нормативно-правовой базы в области защиты персональных данных и дополнительных обследованиях ИСПДн и методики испытаний: Отчет по НИР / ЗАО г. Москвы, ЗАО «Центр новых технологий «Парус»». – М., 2011. – 253 с.

3. Работы по обеспечению безопасности доступа на объекты и управление персоналом территориальных органов исполнительной власти ЗАО г. Москвы. Этап 4. Проведение работ по подготовке к аттестации комплекса, обеспечивающего безопасность доступа на объекты, и управление персоналом территориальных органов исполнительной власти ЗАО г. Москвы: Отчет по НИР / ЗАО г. Москвы, ООО НПЦ «СОТИС». – М., 2010. – 198 с.

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Академия Государственной противопожарной службы МЧС России»

* Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежский институт Государственной противопожарной службы МЧС России»

PROPOSALS FOR ENSURING THE SAFETY AND CONFIDENTIALITY OF INFORMATION IN LOCAL BODIES OF THE EXECUTIVE POWER

V.M. Kletsov, N.S. Shimon

Proposals for the establishment of information security information are considered in the article. This information is processed in the developed hardware and software platform of territorial bodies of the executive power. These proposals improve the efficiency of the regional emergency management subsystem (for example, administrative districts).

Keywords: territorial executive authorities, decision support, information technology, automated information systems.

УДК 681.3

ПРИНЯТИЕ РЕШЕНИЙ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ В СЛУЧАЕ КОНФЛИКТНОСТИ МНОЖЕСТВА ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ

С.В. Белокуров, А.В. Душкин, В.В. Цветков, А.А. Змеев*

В статье предлагается алгоритм выбора контрастных точек в случае конфликтности множества показателей защищенности, имеющем место в сложных системах защиты информации, а на его основе формализуется функция и механизм выбора контрастных точек, позволяющие строить эффективные схемы принятия решений.

Ключевые слова: *информационная безопасность, моделирование, оптимизация, принятие решений.*

Современные системы защиты информации от несанкционированного доступа, как правило, описываются достаточно большим количеством качественных и количественных показателей, наличием сложных зависимостей между ними [1]. Моделирование и оптимизация параметров и режимов на всех этапах жизненного цикла и на всех уровнях организации, функционирования и управления таких систем представляет собой трудоемкую задачу большой размерности. Одним из путей решения таких задач является привлечение эффективного аппарата многокритериальной оптимизации (МКО) [2, 3].

Одной из проблем, возникающих при разработке методов анализа решений с использованием математического моделирования, является наличие многих показателей качества анализируемых решений. Если в ранних работах предполагалось, что различные зачастую противоречивые требования к принимаемым решениям можно тем или иным путем свести к единственному критерию качества решения, то в настоящее время большинство специалистов полагает, что необходимо учитывать существование несовпадающих частных критериев. Методы принятия решений, основанные на признании наличия многих частных критериев, образуют одно из направлений теории принятия решений - так называемые многокритериальные методы принятия решении.

Поэтапный поиск решений и проводимый на нем выбор в задачах МКО описывается разнородными способами формализации, привязанными к конкретному используемому методу. В то же время активно развивается новое научное направление - теория выбора, позволяющая строить эффективные функции и механизмы выбора на множестве любой мощности, оценивать на ранних стадиях принятия решения эффективность работы того или иного способа выбора, принимать обоснованные и взвешенные решения, привлекая богатый опыт экспертов. Следует отметить, что функция выбора представляет собой наиболее естественное, универсальное и удобное описание для генерации схем отсева части решений на итерациях поиска.

В статье предлагается алгоритм выбора контрастных точек [5] в случае конфликтности множества показателей защищенности, имеющем место в сложных системах защиты информации (СЗИ), а на основе этого алгоритма формализуется функция и механизм выбора контрастных точек, позволяющие строить эффективные схемы принятия решений.

Рассмотрим понятия фильтрации и дискретизации множеств. Термин фильтрация относится к процессу выделения подмножеств точек из конечного множества точек. Понятие дискретизация множеств относится к процессу описания непрерывного множества путем выбора из него конечного числа точек. Фильтрация - это инструмент, позволяющий нам справляться с большим количеством информации о конечных объектах. Есть два типа фильтрации: прямая и обратная. Пусть V - конечное множество векторов. Рассматривая прямую фильтрацию, обозначим буквой P объем так называемого прямого множества (т.е. число элементов подмножества, которое нужно вычислить). В процессе прямой фильтрации мы стараемся выбрать из множества V наиболее отличающиеся P векторов. Это сопровождается определением P векторов из V, отстоящих друг от друга дальше всего в некоторой заданной метрике. Рассмотрим теперь обратную фильтрацию.

Пусть $\overline{v} \in V$ и P означает объем так называемого обратного множества. Тогда при обратной фильтрации мы находим P-1 наиболее «похожих» на $\overline{v}$ векторов из V. Это выполняется путем определения P-1 векторов, ближайших к $\overline{v}$ в некоторой заданной метрике.

Фактически смысл прямой фильтрации - в построении *максимально дисперсных* (рассеянных) множеств. Пусть V - конечное множество точек. Под максимально дисперсным подмножеством множества V объема P будем понимать такое множество P точек из V, элементы которого отстоят друг от друга дальше, чем элементы любого другого множества P точек в V. То есть максимально

Белокуров Сергей Владимирович - ФКОУ ВПО «Воронежский институт ФСИН России», доктор технических наук, доцент, тел. (473) 260-68-19;
Душкин Александр Викторович - ФКОУ ВПО «Воронежский институт ФСИН России», доктор технических наук, доцент, тел. (473) 260-68-19;
Цветков Владимир Владимирович - ФКОУ ВПО «Воронежский институт ФСИН России», адъюнкт, тел. (473) 260-68-19;
Змеев Анатолий Анатольевич - ФГКВОУ ВПО «Военная академия ВКО имени Г.К. Жукова», аспирант, тел. (473) 260-68-19.

дисперсное подмножество размерности P - это множество точек, которое способно пройти через отношение .фильтрации с параметром d большим, чем любое другое множество из P точек.

Построение максимально дисперсного подмножества предполагает значительный объем вычислений. Например, применение методов ближайшей или наиболее удаленной точки вне окрестностей включало бы фильтрацию исходного множества точек до получения сокращенного множества размерности P таким образом, чтобы каждая из точек исходного множества служила бы начальной точкой. Тогда подмножество с наибольшим окончательным значением d и является максимально дисперсным. Так как объем вычислений, необходимый для построения максимально дисперсного подмножества, огромен, то мы обычно принимаем решением о построении подмножеств, близких к максимально дисперсному. Такие *приближенные* подмножества строятся с помощью метода первой, ближайшей и наиболее удаленной точек вне окрестностей при произвольно выбранной начальной точке.

Предложим способ выбора контрастных точек. Способ основывается на формуле Штойера [5], для расчета координат наиболее "контрастных" точек. Данных способ не использовался ранее для решения такого класса задач. На основе этого способа формализуем алгоритм, а затем и механизм выбора, реализующий соответствующую функцию выбора.

Данный способ, по сравнению с аналогами, позволяет получить асимптотически равномерное распределение точек Парето и дает хорошие результаты при любой конечной выборке, для различных законов распределения генеральной совокупности точек Парето, что подтверждено на практике. Анализ "контрастных" точек по формуле Штойера основывается на следующей формуле [5]:

$$L(X_A^i, Y_B^i) = \\ = \sum_{k=1}^{m} \frac{1}{R_k} \Big[\sum_{j=1}^{m} \frac{1}{R_j} \Big]^{-1} \cdot \left| x_{Ak}^i - y_{Bk}^i \right|^2 \qquad (1)$$

$$R_i = max(x_A{}^i{}_k, x_B{}^i{}_k) - min(x_A{}^i{}_k, x_B{}^i{}_k), k = \overline{1..m};$$

$$\sum_{k=1}^{m} \frac{1}{R_k} \Big[\sum_{j=1}^{m} \frac{1}{R_j} \Big]^{-1} = 1 \cdot$$

где: R_i – диапазон изменения i – го критерия из всей рассматриваемой совокупности; n – число рассматриваемых критериев; x_A^i, $x_Б^i$ – сравниваемые между собой вектора на i – той итерации поиска.

Сам алгоритм выбора контрастных точек, на основе формулы (1) можно формализовать в виде:

1. Выбор начальной точки X_i.

2. Перебор всех остальных точек $X_1, X_2, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n$ и вычисления расстояний до X_i, т.е. $R_1, R_2, \ldots, R_{n-1}$.

3. Нахождение максимального расстояния $R_{\max}^1 = \max\limits_{k=1..n-1} \{R_k\}$ и запоминание соответствующей точки x_j.

4. Выбор очередной j - й точки, кроме отобранных, перебор остальных точек $X_1, X_2, \ldots, X_{n-j}$ и вычисления расстояний до каждой из отобранных на предыдущем шаге $R_1, R_2, \ldots, R_{n-j}$.

5. Нахождение максимального расстояния до всех выбранных точек $R_{\max}^j = \max\limits_{k=1..n-j} \{R_k\}$ и запоминание соответствующей точки x_j.

6. Повторение шагов 4 и 5 ведется до тех пор, пока не будет выбрано заранее заданное количество решений.

Формализуем механизм и функцию выбора для поиска контрастных точек. Для этого введем основные понятия теории выбора.

Рассмотрим множество H – множество вариантов решений $\{x, y, \ldots\}$. $X \subseteq H$ – непустое множество H, предъявленное для выбора, $C(X) = Y \subseteq X$ $(Y \neq 0)$ – выбор из X по некоторому правилу С части вариантов. Это правило и называют функцией выбора. С позиции теории выбора общая формальная модель задачи выбора может быть представлена в виде:

$$C(\bullet) : \{X\} \to \{X\}, \{X\} \subseteq 2^H, \\ \forall X \subset \{X\}, C(X) = Y, \qquad (2)$$

где H – множество рассматриваемых вариантов $\{x, y, \ldots\}$, $X \subseteq H$ – непустое множество H, предъявленное для выбора, $C(X) = Y \subseteq X$ $(Y \neq 0)$ – выбор из X по некоторому правилу C части вариантов, $Y \subseteq X$.

Сам процесс выбора рассматривается как "черный ящик", на вход которому поступает множество рассматриваемых альтернатив $X \subseteq H$, называемое предъявлением, а на выходе получается множество $Y \subseteq X$ выбранных альтернатив, называемое выбором. Таким образом, функция выбора определяет "внешнее" описание процесса выбора.

В свою очередь "внутреннее" описание, т.е. описание того, как множество Y выделяется из X , определяется механизмом выбора, обозначаемый через $M = <\sigma, \pi>$, где σ – структура на множестве X (совокупность сведений, в том числе полученных от лица, принимающего решение (ЛПР), обо всех рассматриваемых вариантов из X , позволяющих сравнивать эти варианты), а π – правило выбора, которое указывает как, используя структуру σ , получить Y из X . Механизмы, порождающие одинаковую функцию выбора $C(X)$ являются эквивалентными.

Функции выбора чаще сводятся к двум основным заданиям [5]:

1) "Поэлементное задание", т.е. множество $Y = C(X) \subseteq X$ – это набор элементов, удовлетворяющих условиям:

$$C(X) = \{ y \in X \mid П \}, \qquad (3)$$

где: $П$ – некоторый оператор, формализующий условие выбора.

2) "Целостное задание", т.е. $C(X) = \{ Y \subseteq X \mid П \}$ есть некоторое подмножество множества X, которое

в отличии от других его подмножеств, удовлетворяет некоторому требованию *П*.

Механизмы выбора чаще представляются двумя компонентами: "структура" и "правило" выбора. При обеих формах выражения для *C(X)*, выделение *Y* из *X* опирается на некоторую заранее заданную совокупность сведений о вариантах *X*, помимо данного исходного множества *H*. Любая формализация таких сведений, использующуюся при описании механизма выбора, называется структурой и обозначается символом σ. В качестве примера можно привести шкалы критериальных оценок, или бинарные отношения, т.е. "структуры предпочтений". Каждый механизм выбора *M* характеризуется, во первых, заданием структуры σ, и, во вторых, правилом выбора π, которое указывает – как построить множество *C(X)*, для любого $\{x \in H^0\}$, на основе данной структуры σ. Здесь $H^0 = 2^H \setminus \{\varnothing\}$, т.е. множество всех непустых подмножеств *H*, | *H* | – мощность *H*.

Если используется определение "поэлементной" формы выбора (3), то правило выбора π – это то, что записано в виде оператора *П*, т.е. можно формализовать правило выбора в "поэлементной" форме:

$$\pi: \; y \in X \mid П. \qquad (4)$$

Аналогично в "целостной" форме:

$$\pi: \; Y \subseteq X \mid П, \qquad (5)$$

где: *П* – оператор выбора, в обоих случаях формализующий условие, которому удовлетворяют элементы *{y}*, или множества *Y* (5), выделяемые правилом π. При этом, в (4) корректное определение π требует, чтобы выражение на месте многоточий единственным образом определяло множество *Y*, при любом допустимом значении *X*.

Если использовать формулу (3) в качестве оператора *П*, то можно формализовать механизм выбора для ограничения мощности точек, основанный на поиске контрастных точек (1), в следующем виде:

$$C_{Contr} = \left\{ X^i_{Contr} \in X^i \mid X^i_{Contr} = \right.$$

$$\left. = \sum_{k=1}^{m} \frac{1}{R_k} \left[\sum_{j=1}^{m} \frac{1}{R_j} \right]^{-1} \cdot \left| X^i_{Ak} - Y^i_{Bk} \right|^2 ; \right.$$

$$\left. X^i_{Ak}, Y^i_{Bk} \in X^i \right\};$$

где: $R_i = max(X^i_{Ak}, Y^i_{Bk}) - min(X^i_{Ak}, Y^i_{Bk})$, $k = \overline{1..m}$; $\sum_{k=1}^{m} \frac{1}{R_k} \left[\sum_{j=1}^{m} \frac{1}{R_j} \right]^{-1} = 1$; X^i – множество вариантов для выбора.

Применение механизма прямой фильтрации позволяет в практических задачах принятия решений на множестве Парето позволяет проанализировать все множество альтернатив и избежать потери удаленных скоплений точек. Предложенный алгоритм, механизм и функция выбора на его основе, позволяют строить эффективные схемы принятия решений, отличающиеся от известных комплексным анализом множества показателей защищенности в сложных СЗИ, в случае их конфликтности для класса задач МКО.

Литература

1. Основы информационной безопасности: Учебник для высших учебных заведений МВД России / Под ред. В.А. Минаева и С.В. Скрыля. - Воронеж: Воронежский институт МВД России, 2001. – 464 с.

2. Белокуров С.В. Модели и алгоритмы автоматизированного контроля эффективности систем защиты информации в автоматизированных системах / С.В. Белокуров, С.В. Скрыль, В.К. Джоган и др. // Монография. – Воронеж: Воронежский институт МВД России, 2012. – 116 с.

3. Белокуров С.В. Методы и средства анализа эффективности систем информационной безопасности при их разработке / С.В. Белокуров, С.В. Скрыль, В.К. Джоган и др. // Монография. – Воронеж: Воронежский институт МВД России, 2012. – 83 с.

4. Белокуров С.В. Модели выбора недоминируемых вариантов в численных схемах многокритериальной оптимизации / С.В. Белокуров, Бугаев Ю.В., Сербулов Ю.С. и др. // Монография. – Воронеж : Научная книга, 2005. – 199 с.

5. Штойер Р.Е. Многокритериальная оптимизация. Теория, вычисления и приложения: Пер. с англ. – Москва: Радио и связь, 1992. – 504 с.

Федеральное казенное образовательное учреждение высшего профессионального образования «Воронежский институт Федеральной службы исполнений и наказаний России»

*Федеральное государственное казенное военное образовательное учреждение высшего профессионального образования «Военная академия воздушно-космической обороны имени Маршала Советского Союза Г. К. Жукова»

DECISION MAKING IN SYSTEMS OF THE GUARD OF THE INFORMATION IN THE CASE CONFLICTNESSES OF SET OF INDEXES OF SECURITY

S.V. Belokurov, A.V. Dushkin, V.V. Tsvetkov, A.A. Zmeev

In paper the algorithm of a choice of contrasting points in case of a conflictness of set of indexes of the security, taking place in complicated systems of a guard of the information is offered, and on its basis function and the mechanism of a choice of the contrasting points is formalized, allowing to build effective decision diagrammes.

Keywords: information security, modelling, optimisation, a decision making.

УДК 681.3

ОРГАНИЗАЦИЯ ДОСТУПА В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ НА БАЗЕ КОМПЛЕКСНОЙ ОЦЕНКИ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ

С.В. Белокуров, А.А. Змеев*

В статье рассматривается подсистема автоматизированного контроля доступа пользователей к информации в интегрированных системах безопасности, которая обеспечивает проведение организационно-технологического управления контролем доступа, с помощью управляемых параметров безопасности данных.

Ключевые слова: *информационная безопасность, информация, автоматизация.*

Оптимальное управление, применяемое в автоматизированных системах (АС), в случае, когда нерегулируемые параметры в системе на том или ином отрезке времени не меняются, сводится к поддержанию таких значений управляемых параметров, которые обеспечивают максимизацию (или минимизацию) соответствующего критерия оптимального управления [1]. В данном случае, в результате управленческого решения необходимо выбрать такой набор значений управляемых параметров функционирования системы защиты информации от несанкционированного доступа (СЗИ НСД), который обеспечивает максимальное значение комплексного критерия качества функционирования СЗИ НСД как объекта управления ($E_и$). В соответствии с [2-3] задачу принятия решения при организационно-технологическом управлении качеством СЗИ НСД можно формализовать как задачу математического программирования [1] следующим образом. Требуется выбрать такую альтернативу $a \in A$ из множества альтернатив A, чтобы было выполнено:

$$E_к \to \max,\ E_{ва} \geq E_{\min ва} \qquad (1)$$
$$E_ф \wedge E_{ра} \wedge E_{фа} \wedge E_{уи} = 1.$$

Второе и третье выражения в (1) дают ограничения по критериям, отражающим требования к СЗИ НСД в интегрированных системах безопасности (ИСБ). Выполнение приведенных ограничений предусматривает достаточную полноту реализуемого набора защитных функций СЗИ НСД, ресурсную и функциональную неконфликтность функционирования СЗИ НСД в ИСБ и допустимые усилиями персонала для реализации эффективного функционирования СЗИ НСД.

Таким образом, для организации оптимального управления качеством СЗИ НСД, при выполнении ограничений оцениваемых качественными критериями, требуется выбрать такие значения управляемых параметров, чтобы было выполнено:

$$E_к \to \max,\ E_{ва} \geq E_{\min ва} \qquad (2).$$

Анализ особенностей функционирования управляемых программных средств защиты информации (ПСрЗИ) показывает, что увеличение времени отводимого на реализацию их функций обеспечивает увеличение эффективности данных ПСрЗИ, т.е. увеличение значений частных критериев адекватности функционирования управляемых ПСрЗИ, определяющих критерий адекватности функционирования СЗИ НСД. Исходя из этого, задача оптимального управления качеством СЗИ НСД сводится к задаче оптимального использования времени отводимого на реализацию защитных функций СЗИ НСД, которую можно записать следующим образом:

$$E_{ва} - E_{\min ва} \to \min\ , \qquad (3)$$

$$E_{ва} \geq E_{\min ва}\ . \qquad (4)$$

При управлении качеством функционирования СЗИ НСД осуществляется формирование управляющего воздействия, обеспечивающего выполнение выражений (3), (4). Учитывая критичность ИСБ к обеспечению ИБ, организацию оптимального управления качеством функционирования СЗИ НСД предлагается осуществлять на основе критерия максимизации минимального значения частных критериев адекватности функционирования управляемых ПСрЗИ.

Управление качеством функционирования СЗИ НСД, при условии $E_{ва} < E_{\min ва}$ целесообразно осуществлять управляемым параметром, обеспечивающим выполнение ограничения (4) при минимальном снижении эффективности ПСрЗИ. Увеличение $E_{ва}$ осуществляется следующим образом. Уменьшается значение управляемого параметра на величину необходимую для выполнения ограничения (4), но не более величины обеспечивающей уменьшение значения соответствующего частного критерия на 1. Если в результате этих действий не удалось выполнить ограничение (4) то вышеназванные операции повторяются.

В случае если в процессе управления управляемым параметром достигнуто минимальное значение, заданные эксплуатационной документацией на ИСБ, а выполнить ограничение (4) не удалось, то данное СЗИ НСД заменяется на более эффективное. При условии $E_{ва} > E_{\min ва} + \delta$, где δ – малая величина, управление качеством функционирования СЗИ НСД осуществляется управляемым параметром ПСрЗИ. В этом случае управление осуществляется

Белокуров Сергей Владимирович - ФКОУ ВПО «Воронежский институт ФСИН России», доктор технических наук, доцент, тел. (473) 260-68-19;
Змеев Анатолий Анатольевич - ФГКВОУ ВПО «Военная академия ВКО имени Г.К. Жукова», аспирант, тел. (473) 260-68-19.

следующим образом. Увеличивается значение этого управляемого параметра на величину необходимую для выполнения неравенства $E_{\min ва} < E_{ва} \le E_{\min ва} + \delta$, но не более величины обеспечивающей увеличение значения соответствующего частного критерия на 1. Если в результате этих действий не удалось выполнить неравенства $E_{\min ва} < E_{ва} \le E_{\min ва} + \delta$, то вышеназванные операции повторяются.

Организационно-технологическое управление контролем доступа пользователей к информации в ИСБ осуществляется с помощью подсистемы автоматизированного контроля доступа пользователей в ИСБ. Подсистема автоматизированного контроля доступа пользователей в ИСБ включает в свой состав подсистему контроля качества функционирования СЗИ НСД, подсистему принятия решений, подсистему управляющих воздействий. Подсистема автоматизированного контроля доступа пользователей в ИСБ реализует приведенную выше математическую модель оптимального управления качеством СЗИ НСД в ИСБ с помощью управляемого параметра процесса ЗИ. Учитывая, что процесс оптимизации управляемого параметра носит итерационный характер, а реализуемое организационно - технологическое управление за счет организационных мероприятий предполагает достаточно продолжительный цикл управления, то целесообразно провести все процедуры по определению оптимального значения управляемого параметра, а затем формировать управляющее воздействие для модифицированная система защиты информации от несанкционированного доступа (МСЗИ) НСД.

Для этого на основе исходных данных, полученных от подсистемы регистрации и учета, а также от ЛПР, в подсистеме контроля качества функционирования СЗИ НСД определяется текущее значение количественного критерия $E_{ва}$. Затем, в подсистеме принятия решений проверяется выполнение неравенства $E_{\min ва} < E_{ва} \le E_{\min ва} + \delta$ и в случае отрицательного результата выбирается значение управляемого параметра для регулировки $E_{ва}$. Значение управляемого параметра изменяется на величину необходимую для выполнения неравенства, но не более величины обеспечивающей изменение значения соответствующего частного критерия на 1. Новое значение управляемого параметра передается через подсистему управляющих воздействий в подсистему контроля качества функционирования СЗИ НСД, в качестве параметра функции обратной связи, для определения $E_{ва}$ при новом значении управляемого параметра. Исходными данными соответствующими новому значению выбранного управляемого параметра, необходимыми для вычисления $E_{ва}$, являются ВВХ для данного значения управляемого параметра полученные при статистической обработке данных от подсистемы регистрации и учета в процессе эксплуатации МСЗИ НСД или заданные администратором ЗИ, в качестве предварительных. Новая оценка $E_{ва}$ поступает в подсистему принятия решений, замыкая цикл формирования оптимального значения управляемого параметра.

В конце процедуры оптимизации (при выполнении приведенного выше неравенства), значение управляемого параметра поступает в подсистему управляющих воздействий для формирования управляющих воздействий на ПСрЗИ МСЗИ НСД и администратору ЗИ (ЛПР) для контроля и проведения организационных управленческих мероприятий. После изменения качества функционирования МСЗИ НСД вновь оценивается значение её критерия $E_{ва}$ и уточняется выполнение условия $E_{\min ва} < E_{ва} \le E_{\min ва} + \delta$, замыкая цикл управления качеством функционирования МСЗИ НСД.

Подсистема контроля качества функционирования СЗИ НСД использует в качестве входных данных для своей работы исходные данные о параметрах выполнения МСЗИ НСД своих функций ЗИ при реализации сервисных задач в ИСБ. Эти данные предоставляются подсистемой регистрации и учета в процессе работы МСЗИ НСД в виде списка (M, s_m, t_m), где M – количество зарегистрированных переходов МСЗИ НСД из одного состояния в другое; s_m, $m = \overline{1, M}$ – состояние, в которое перешла МСЗИ НСД при m-ом переходе; t_m, $m = \overline{1, M}$ – момент времени осуществления m-го перехода. При своей работе подсистема контроля качества функционирования СЗИ НСД прежде всего преобразует входные данные в статистические данные реализации переходных процессов в МСЗИ НСД моделируемые КПП для оценки критерия временной агрессивности функционирования МСЗИ НСД: $N_{ва\,ij}$ – количество зафиксированных событий, заключающихся в том, что КПП перешел из состояния i непосредственно в состояние j; $N_{ва\,i}$ – количество зафиксированных событий, заключающихся в том, что КПП оказался в состоянии i; $\tau_{ва\,ijk}$ – значения при k-ом наблюдении времени перехода КПП из состояния i непосредственно в состояние j.

После обработки вышеназванных данных определяются текущие оценки переходных вероятностей $p_{ва\,ij}$, а также параметров законов распределений для функций $G_{ва\,ij}(\tau)$, которые используются для оценки временной агрессивности функционирования МСЗИ НСД.

Текущие оценки переходных вероятностей $p_{ва\,ij}$, $i = \overline{1, n_{ва}}$, $j = \overline{1, n_{ва}}$ определяются следующим образом:

$$p_{ва\,ij} = N_{ва\,ij} / N_{ва\,i} \,. \qquad (5)$$

Текущие оценки параметров законов распределений для функций $G_{ва\,ij}(\tau)$, $i = \overline{1, n_{ва}}$, $j = \overline{1, n_{ва}}$ определяются в зависимости от закона распределения по простой выборке объема $N_{ва\,ij}$ из генеральной совокупности с данным распределением [1]. Текущие оценки параметров рассматриваемых законов

распределения для данных функций определяются следующим образом [1].

Для равномерного закона определяются оценки параметров $a_{ва\ ij}$, $b_{ва\ ij}$ – минимальное и максимальное время соответственно перехода КПП, моделирующего динамику функционирования МСЗИ НСД для оценки временной агрессивности её функционирования, из состояния *i* в состояние *j*.

Несмещенными оценками с наименьшей дисперсией будут следующие оценки:

$$a_{ва\ ij} = \frac{N_{ва\ ij} \min\limits_{k=1,N_{ва\ ij}} \{\tau_{ва\ ijk}\} - \max\limits_{k=1,N_{ва\ ij}} \{\tau_{ва\ ijk}\}}{N_{ва\ ij} - 1}; \quad (6)$$

$$b_{ва\ ij} = \frac{N_{ва\ ij} \max\limits_{k=1,N_{ва\ ij}} \{\tau_{ва\ ijk}\} - \min\limits_{k=1,N_{ва\ ij}} \{\tau_{ва\ ijk}\}}{N_{ва\ ij} - 1}. \quad (7)$$

Для нормального закона определяются оценки параметров $\mu_{ва\ ij}$, $\sigma_{ва\ ij}$ – среднее значение и среднеквадратическое отклонение времени перехода КПП, моделирующего динамику функционирования МСЗИ НСД для оценки временной агрессивности функционирования, из состояния *i* в *j*.

Несмещенные состоятельные оценки для данных параметров:

$$\mu_{ва\ ij} = \frac{1}{N_{ва\ ij}} \sum_{k=1}^{N_{ва\ ij}} \tau_{ва\ ijk}; \quad (8)$$

$$\sigma^2_{ва\ ij} = \frac{1}{N_{ва\ ij} - 1} \sum_{k=1}^{N_{ва\ ij}} \left(\tau_{ва\ ijk} - \mu_{ва\ ij}\right)^2. \quad (9)$$

Для экспоненциального закона оценивается параметр $b_{ва\ ij}$ – среднее время перехода КПП, моделирующего функционирование МСЗИ НСД для оценки временной агрессивности функционирования, из состояния *i* в *j*.

Эффективная оценка для данного параметра:

$$b_{ва\ ij} = \frac{1}{N_{ва\ ij}} \sum_{k=1}^{N_{ва\ ij}} \tau_{ва\ ijk}. \quad (10)$$

При определении оценок параметров нет необходимости хранить в памяти ЭВМ все наблюдаемые значения $\tau_{ва\ ijk}$, $k = \overline{1, N_{ва\ ij}}$, так как вычисления можно проводить рекуррентно.

Для равномерного закона текущие оценки параметров $a_{ва\ ij}$, $b_{ва\ ij}$ (по результатам $N_{ва\ ij}$ наблюдений) определяются через предыдущие оценки $\tilde{a}_{ва\ ij}$, $\tilde{b}_{ва\ ij}$ (по результатам ($N_{ва\ ij} - 1$) наблюдений) следующим образом:

$$a_{ва\ ij} = \left(N_{ва\ ij} \min\left\{ \tilde{a}_{ва\ ij} + \frac{\tilde{b}_{ва\ ij} - \tilde{a}_{ва\ ij}}{N_{ва\ ij}}; \tau_{ва\ ijN_{ва\ ij}} \right\} - \right.$$
$$\left. - \max\left\{ \tilde{b}_{ва\ ij} + \frac{\tilde{a}_{ва\ ij} - \tilde{b}_{ва\ ij}}{N_{ва\ ij}}; \tau_{ва\ ijN_{ва\ ij}} \right\} \right) \Big/ \left(N_{ва\ ij} - 1\right); \quad (11)$$

$$b_{ва\ ij} = \left(N_{ва\ ij} \max\left\{ \tilde{b}_{ва\ ij} + \frac{\tilde{a}_{ва\ ij} - \tilde{b}_{ва\ ij}}{N_{ва\ ij}}; \tau_{ва\ ijN_{ва\ ij}} \right\} - \right.$$
$$\left. - \min\left\{ \tilde{a}_{ва\ ij} + \frac{\tilde{b}_{ва\ ij} - \tilde{a}_{ва\ ij}}{N_{ва\ ij}}; \tau_{ва\ ijN_{ва\ ij}} \right\} \right) \Big/ \left(N_{ва\ ij} - 1\right). \quad (12)$$

Рекуррентные формулы (11)-(12) используются вместо формул (6)-(7).

Для нормального закона текущие оценки параметров $\mu_{ва\ ij}$, $\sigma_{ва\ ij}$ (по результатам $N_{ва\ ij}$ наблюдений) определяются через предыдущие оценки $\tilde{\mu}_{ва\ ij}$, $\tilde{\sigma}_{ва\ ij}$ (по результатам ($N_{ва\ ij} - 1$) наблюдений) следующим образом:

$$\mu_{ва\ ij} = \left(\left(N_{ва\ ij} - 1\right)\tilde{\mu}_{ва\ ij} + \tau_{ва\ ijN_{ва\ ij}} \right) \Big/ N_{ва\ ij}; \quad (13)$$

$$\sigma^2_{ва\ ij} = \frac{\left(\tau_{ва\ ijN_{ва\ ij}} - \mu_{ва\ ij}\right)^2 + \left(N_{ва\ ij} - 2\right)\tilde{\sigma}^2_{ва\ ij}}{N_{ва\ ij} - 1} +$$
$$+ \left(\frac{\tau_{ва\ ijN_{ва\ ij}} - N_{ва\ ij}\mu_{ва\ ij}}{N_{ва\ ij} - 1} \right)^2 - \mu_{ва\ ij}\left(2\tilde{\mu}_{ва\ ij} - \mu_{ва\ ij}\right). \quad (14)$$

Рекуррентные формулы (13)-(14) используются вместо формул (8)-(9).

Для экспоненциального закона текущая оценка параметра $b_{ва\ ij}$ (по результатам $N_{ва\ ij}$ наблюдений) определяется через предыдущую оценку $\tilde{b}_{ва\ ij}$ (по результатам ($N_{ва\ ij} - 1$) наблюдений) следующим образом:

$$b_{ва\ ij} = \frac{1}{N_{ва\ ij}} \left(\left(N_{ва\ ij} - 1\right)\tilde{b}_{ва\ ij} + \tau_{ва\ ijN_{ва\ ij}} \right). \quad (15)$$

Рекуррентная формула (15) используется вместо формулы (10).

Итак, статистические данные о времени реализации переходных процессов МСЗИ НСД и их относительных частотах должны накапливаться подсистемой контроля в виде следующих величин: $N_{ва\ ij}$, $N_{ва\ i}$ (безотносительно к закону распределения); $\tilde{a}_{ва\ ij}$, $\tilde{b}_{ва\ ij}$ (для равномерного закона); $\tilde{\mu}_{ва\ ij}$, $\tilde{\sigma}_{ва\ ij}$ (для нормального закона); $\tilde{b}_{ва\ ij}$ (для экспоненциального закона). В результате обработки этих данных, а также величин $\tau_{ва\ ijN_{ва\ ij}}$ определяются по формулам (5), (6)-(15) текущие оценки параметров переходных процессов МСЗИ НСД в виде следующих величин: $p_{ва\ ij}$ (по формуле (5) безотносительно к закону распределения); $a_{ва\ ij}$, $b_{ва\ ij}$ (по формулам (11)-(12) для равномерного закона); $\mu_{ва\ ij}$, $\sigma_{ва\ ij}$ (по формулам (13)-(14) для нормального закона); $b_{ва\ ij}$ (по формуле (15) для экспоненциального закона). Вообще говоря, возможности метода не ограничиваются данными законами распределения, однако здесь другие законы не рассматриваются. Кроме вышеназванных параметров в вычислениях критерия временной агрессивности

функционирования МСЗИ НСД в качестве исходных данных используется среднее значение максимально допустимого времени реализации МСЗИ НСД защитных функций ($\tau_{тва}$) устанавливаемое администратором ЗИ в соответствии с разделом «Требования к подсистеме ЗИ от НСД» эксплуатационной документации на ИСБ. На основе этих данных вычисляется значение критерия $E_{ва}$, определенного равенством (16), являющееся выходным параметром подсистемы контроля качества функционирования СЗИ НСД.

$$E_{ва} = P\left(\tau_{ва} \le \tau_{\max ва}\right), \qquad (16)$$

где $\tau_{ва}$ – время реализации СЗИ НСД защитных функций; $\tau_{max\ ва}$ – его максимально допустимое значение (экспоненциально распределенная случайная величина со средним значением $\tau_{тва}$).

Учитывая, что принятие управленческого решения производится на основе оценок $E_{ва}$, реализующих функцию обратной связи управления, то выходные данные подсистемы контроля входят в состав исходных данных для подсистемы принятия решений. Кроме того, в состав исходных данных входит параметр, отражающий условия функционирования ИСБ как с точки зрения ЗИ, так и с точки зрения требований к ИСБ в плане функционирования по прямому назначению $E_{\min ва}$. Этот параметр задаётся администратором ЗИ в соответствии с разделом «Требования к подсистеме ЗИ от НСД» эксплуатационной документации на ИСБ.

В подсистеме управляющих воздействий входными данными являются значение управляемого параметра, полученное подсистемой принятия решений или заданное директивно администратором ЗИ (ЛПР). Данная подсистема формирует управляющее воздействие на управляемые ПСрЗИ в соответствии с оптимальным значением управляемого параметра, с целью реализации технологической части организационно-технологического управления качеством функционирования МСЗИ НСД. При этом выбранное значение управляемого параметра используется подсистемой управляющих воздействий для определения конкретного момента времени начала очередной контрольной аутентификации пользователей. Причем, с целью обеспечения фактора неожиданности для злоумышленника, момент запуска очередной контрольной аутентификации пользователей целесообразно определять по результатам сравнения значений параметра $p_{ка}$ и датчика случайных чисел на интервале [0;1] [1].

Таким образом, предлагаемая подсистема автоматизированного контроля доступа пользователей в ИСБ обеспечивает проведение организационно-технологического управления контролем доступа пользователей в ИСБ, с помощью управляемого параметра процесса ЗИ.

Литература

1. Основы информационной безопасности: Учебник для высших учебных заведений МВД России / Под ред. В.А. Минаева и С.В. Скрыля. - Воронеж: Воронежский институт МВД России, 2001. – 464 с.

2. Белокуров С.В. Модели и алгоритмы автоматизированного контроля эффективности систем защиты информации в автоматизированных системах / С.В. Белокуров, С.В. Скрыль, В.К. Джоган и др. // Монография. – Воронеж: Воронежский институт МВД России, 2012. – 116 с.

3. Белокуров С.В. Методы и средства анализа эффективности систем информационной безопасности при их разработке / С.В. Белокуров, С.В. Скрыль, В.К. Джоган и др. // Монография. – Воронеж: Воронежский институт МВД России, 2012. – 83 с.

Федеральное казенное образовательное учреждение высшего профессионального образования «Воронежский институт Федеральной службы исполнений и наказаний России»

*Федеральное государственное казенное военное образовательное учреждение высшего профессионального образования «Военная академия воздушно-космической обороны имени Маршала Советского Союза Г. К. Жукова»

THE ACCESS ORGANIZATION IN SYSTEMS OF A GUARD OF THE INFORMATION ON BASIS COMPLEX ESTIMATION OF QUALITY OF FUNCTIONING

S.V. Belokurov, A.A. Zmeev

In paper the subsystem of the automated control of access of users to the information in the integrated security arrangements which ensures carrying out of organizational-technological control by access control, by means of controlled parametres of data security is considered.

Keywords: information security, the information, automation.

УДК 614.841.44

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ЛЕСНЫХ ПОЖАРОВ НА ПРИМЕРЕ ВОРОНЕЖСКОЙ ОБЛАСТИ

Р.Ю. Поляков, Н.В. Мозговой*

Рассмотрены существующие методики предупреждения возникновения лесных пожаров. Предложена система дистанционного мониторинга.

Ключевые слова: *горимость лесов, лесопирологические характеристики, информационная система дистанционного мониторинга.*

Основную угрозу лесам Российской Федерации и экологической обстановке в ряде регионов страны представляют пожары. Главная причина их возникновения связана с хозяйственной деятельностью людей, то есть определяется факторами антропогенного происхождения. При этом почти 80% возгораний происходит по вине местного населения, что подтверждают данные по горимости лесов в пересчете на 1 млн. га. Наибольшее число пожаров приходится в регионах с высокой плотностью населения и развитой дорожной сетью. Крупные лесные пожары возникают в засушливые периоды года и, прежде всего, в местах распространения сосновых насаждений, которые являются наиболее пожароопасными.

В этих условиях необходимо применять комплекс мероприятий, обеспечивающих предупреждение возникновения, распространение и развитие лесных пожаров. Разработка такого комплекса должна основываться на анализе физико-географических условий и факторов возникновения пожаров, районировании территории по лесопирологическим условиям, информации о количестве, интенсивности и классе лесных пожаров в регионе. Однако в настоящее время лесные службы обычно располагают лишь планами лесов Воронежской области с оценкой их пожарной опасности. При этом полностью не учитываются антропогенные и географические факторы, отсутствует анализ современной пирологической структуры лесов в регионе, недостаточно используется долгосрочный прогноз возникновения лесных пожаров.

Поэтому важнейшими задачами в настоящее время являются: разработка методологии проведения комплексной оценки природных и антропогенных условий возникновения лесных пожаров, ранжирование площадей по степени пожарной опасности, выделение районов, нуждающихся в первоочередном проведении мониторинговых работ, долгосрочное прогнозирование пожароопасной обстановки и обоснование полного комплекса мероприятий, предупреждающих возникновение чрезвычайных ситуаций.

Своевременное предупреждение, организация борьбы с лесными пожарами и ликвидация их последствий требует использования современных информационных технологий и возможностей географических информационных систем. Лесоустройство практически повсеместно трансформировало таксационные и картографические данные на бумажных носителях и создало совмещенные базы данных на магнитных носителях, позволяющих использовать современные информационные технологии.

Для формирования пирологических характеристик земель лесного фонда, таксационные характеристики в большинстве случаев требуют обобщения и создания специализированной лесопирологической информационной системы. Необходимость в этом отмечалась рядом исследователей.

Принятая Федеральной службой лесного хозяйства России концепция устойчивого управления лесами Российской Федерации предусматривает совершенствование системы охраны лесов от пожаров. Поскольку это непосредственно связано с развитием профилактики лесных пожаров, то целесообразно его осуществлять на базе ГИС-технологий, тем более что лесные пожары представляют собой географическое явление.

Существующая в отдельных районах система предупреждения и ликвидации лесных пожаров не соответствует современным требованиям. Для организации и поддержания системы по обнаружению и тушению лесных пожаров на всей территории лесов различных районов Воронежской области имеющихся ресурсов недостаточно. В результате, оперативность обнаружения возникающих пожаров и принятия мер по их ликвидации, особенно на неохраняемых территориях, постоянно снижается. Поэтому предлагается создать аэрокосмическую систему, которая будет включать в себя наземные наблюдательные пункты, воздушные патрули, космические средства слежения за лесными пожарами.

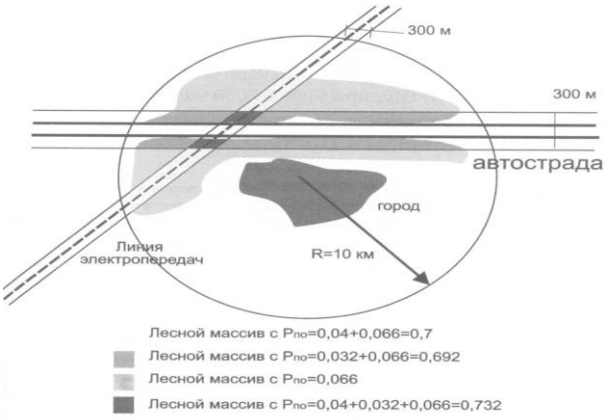
Современные технологии сбора и обработки данных о горимости лесов, о состоянии грозовых

Поляков Роман Юрьевич – преподаватель кафедры гражданской защиты ФГБОУ ВПО «Воронежский институт ГПС МЧС России», e-mail: polyakov_gps@mail.ru;
Мозговой Николай Васильевич – заведующий кафедрой промышленной экологии и БЖД ФГБОУ ВПО ВГТУ, д.т.н., профессор, e-mail: nv_moz@mail.ru.

разрядов и метеорологической информации, применяемой в Воронежской области, позволяют разработать эффективную информационную систему дистанционного мониторинга лесных пожаров. Ее основной задачей будет являться информационная поддержка работ по обнаружению и тушению лесных пожаров, предоставление информации и технологий для анализа последствий лесных пожаров в авиационную службу охраны лесов от пожаров «Авиалесоохрана». Основу предлагаемой информационной системы дистанционного мониторинга лесных пожаров будет составлять ряд описываемых ниже систем.

1. Система сбора информации о горимости лесов по данным наземных наблюдений. Эта информация собирается из регионов на активно охраняемой территории лесного фонда наземными методами наблюдения.

2. Геоинформационная система (ГИС) мониторинга лесных пожаров. Основными задачами представленной системы являются: пространственная интеграция оперативных данных, анализ текущей пожарной обстановки, обработка и предоставление стандартных информационных продуктов, необходимых для принятия решений по обнаружению и тушению лесных пожаров, подготовка отчетной картографической информации.



Динамика возникновения лесных пожаров с применением ГИС-технологий

В последнее десятилетие в России активно развивались методы и технологии анализа и обработки спутниковых данных для решения задач мониторинга лесных пожаров. Был создан ряд систем для обеспечения работ по организации обнаружения и тушения лесных пожаров на федеральном и региональном уровне, и на их основе разработана система спутникового мониторинга пожаров в интересах службы авиационной охраны лесов от пожаров России (ФГУ «Авиалесоохрана», в дальнейшем АЛО).

При поддержке программы «TACIS» предлагается создание центров приема и обработки данных NOAA АЛО. За время эксплуатации системы апробированы не только методики обработки спутниковых данных, но и методы их использования в работе авиаохраны, что позволит более эффективно использовать спутниковый мониторинг в оперативной практике. До 2003 г. космические компоненты системы мониторинга лесных пожаров базировались на данных метеорологических спутников NOAA и радиометров высокого разрешения AVHRR, наблюдающих одну и ту же территорию несколько раз в сутки. Появление новых космических систем (TERRA/AQUA) с радиометром среднего пространственного разрешения MODIS и развитие телекоммуникационных сетей существенно расширяют возможности космических средств и методов наблюдения за лесными пожарами. Кроме того, предлагается ввести в эксплуатацию модуль первичной и тематической обработки данных MODIS для создания производных продуктов с очагами возгорания по температурным каналам этого прибора.

Немаловажное значение для системы авиационной охраны лесов от пожаров имеет получение количественных оценок площадей, пройденных лесными пожарами на всей территории региона, как в течение пожароопасного сезона, так и по его завершению. Здесь решающую роль будут играть данные дистанционного зондирования, обеспечивающие накопление большого массива информации за продолжительный период времени, наблюдение и долгосрочный мониторинг.

Данная система работает со следующими видами оперативной информации:

1. Данные о лесных пожарах подразделений наземной охраны лесов;

2. Спутниковые данные, собираемые в центрах приема со спутников серии NOAA;

3. Данные прибора MODIS спутников TERRA и AQUA, собираемые в специализированных центрах приема;

4. Метеорологические данные, получаемые с наземных станций Госкомгидромета РФ;

5. Данные о молниевых разрядах, поступающие из Центра сбора и обработки данных системы регистрации молниевых разрядов.

Основными элементами предлагаемой системы являются:

1. Блок спутникового мониторинга лесных пожаров, состоящий из:

- центров приема и обработки данных со спутников NOAA;
- системы сбора, хранения, обработки и представления спутниковых данных, поступающих из специализированных центров приема;
- системысбора информации о горимости лесов по данным наземных наблюдений;
- системы интеграции данных о молниевых разрядах.

2. Блок интеграции данных метеонаблюдений на наземных станциях Роскомгидромета РФ.

3. ГИС мониторинга лесных пожаров.

4. Система представления информации о горимости лесов в составе информационных серверов.

Все блоки системы состоят из территориально распределенных элементов, обмен данными между которыми осуществляется по сети Интернет.

Спутниковый мониторинг, входящий в данную систему позволяет решать целый спектр задач:

- получение информации для оценки синоптической обстановки;
- регистрация зон с подозрениями на лесные пожары на охраняемых территориях;
- детектирование пожаров и контроль динамики пожаров на неохраняемых территориях;
- оценка площадей, пройденных лесными пожарами.

Для работы с данной системой потребуется высокая оперативность, поэтому для практической реализации мониторинга лесных пожаров также потребуется создать специальную систему для работы со спутниковыми данными.

Данная система решает следующие основные задачи:

1. Сбор, хранение и обработка спутниковых данных;
2. Интеграция результатов обработки спутниковых данных с информацией, полученной из других источников;
3. Представление результатов обработки данных в удобном виде для анализа и принятия решений.

Система должна обеспечивать:

1. Получение информации из центров приема несколько раз в день для решения оперативных задач;
2. Возможность работы с информацией, поступающей от различных спутниковых систем;
3. Высокий уровень оперативности и автоматизации сбора, обработки данных и представления информационных продуктов пользователям;
4. Интеграцию информации, полученной в результате обработки спутниковых данных, с другими видами информации;
5. Удобный инструментарий работы и схем доступа к оперативной информации для пользователей, в том числе удаленных;
6. Высокий уровень автоматизации работы системы, простоту ее управления и контроль работоспособности;
7. Устойчивость и, по возможности, независимость реализованных в системе процедур обработки и анализа данных от условий и районов наблюдений;
8. Достаточную гибкость и удобные возможности модификации и расширения системы;
9. Низкую стоимость эксплуатации системы.

Такжев представленную систему входят:

- центры сбора и обработки данных;
- система обработки, хранения и представления данных;
- система обеспечения работы региональных и локальных пользователей.

В настоящий момент данная система рассчитана на работу с различными источниками данных. Одновременно с данными, получаемыми и обрабатываемыми в центрах, в системе организован поток данных NOAA из специализированных центров приема**.** Это позволяет повысить устойчивость работы системы и расширить зону реагирования.

Автоматическая система рассылки данных рассчитана на пользователей, которые на своих рабочих местах имеют средства для работы с получаемой информацией.

Внедрение предлагаемой системы на территории Воронежской области поможет существенно решить проблему лесных пожаров.

Литература

1. Андреев Ю.А. Оценка и прогноз пожарной опасности в лесу //Лесохоз. информ. - 1990. - № П.- С.33-38.

2. Волокитина А.В., Софронов М.А., Назимова Д.И. Картографирование РГМ на базе ГИС для контролирования пожаров вблизи населенных пунктов // Аэрокосмические методы и геоинформационные технологии в лесоведении и лесном хозяйстве. (Доклады Всерос. конф.). - Томск: изд-во ТГУ, 2002. - С. 253-257.

3. Государственный доклад о состоянии защиты населения и территорий Воронежской области. Воронеж: Главное управление МЧС РФ по Воронежской области. 2004. - 104 с.

4. Овчинникова Т.В. Дистанционные методы исследования опасных природных процессов: учеб. пособие / Т.В. Овчинникова, С.М. Пасмурнов, В.И. Федянин. Воронеж: ВГТУ. 2005. - 269 с.

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежский институт Государственной противопожарной службы МЧС России»

*Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежский Государственный технический университет»

MODERN TECHNOLOGIES OF PREVENTION AND LIQUIDATION OF FOREST FIRES ON THE EXAMPLE OF THE VORONEZH REGION

R.Y. Poliakov, N.V. Mozgovoy

The current methods of prevention of occurrence of forest fires. Proposed system of remote monitoring.

Keywords: combustibility forests, forest pyrologyc behavior, information system of remote monitoring.

УДК 621.797

СТРУКТУРА И ГАЗОЧУВСТВИТЕЛЬНЫЕ СВОЙСТВА НАНОКОМПОЗИТА Sn-Y-O КАК ПЕРСПЕКТИВНОГО МАТЕРИАЛА ДЛЯ ОБНАРУЖЕНИЯ ТОКСИЧНЫХ И ВЗРЫВООПАСНЫХ ГАЗОВ

Е.А. Русских*, С.И. Рембеза*, Е.С. Рембеза*, Д.В. Русских

В статье приведены результаты исследования структуры и газочувствительных свойств пленок-композитов Sn – Y – O с различной концентрацией примеси иттрия к различным газам в воздухе. Показано, что легирование диоксида олова иттрием снижает температуру максимальной газовой чувствительности к различным газам.

Ключевые слова: *нанокомпозиты, диоксид олова, газовая чувствительность.*

Введение

Нанокомпозиты на основе диоксида олова являются перспективными материалами газовой сенсорики. Они могут быть использованы в качестве сенсорных элементов датчиков газов для мониторинга окружающей среды, обнаружения токсичных и взрывоопасных газов, в медицине и других областях обеспечения безопасной жизнедеятельности человека.

Известно, что величиной газовой чувствительности можно управлять за счет изменений размеров зерен поликристалла и исходной электропроводности пленок [1-3]. Так как адсорбция газа приводит к модуляции высоты потенциальных барьеров на границах зерен для дрейфа носителей заряда, то наиболее эффективны материалы, у которых величина дебаевской длины экранирования сравнима с радиусом зерна. Уменьшение размеров зерен в связи с этим условием приводит также к тому, что увеличивается вклад поверхности поликристаллов в общую электропроводность образца. Кроме того, повышение поверхностной активности наноразмерных поликристаллов может привести не только к увеличению их газовой чувствительности, но и к снижению энергетического порога реакции ионов газов с поверхностными состояниями, то есть к уменьшению температуры максимальной чувствительности пленки к различным газам в воздухе [3].

Взаимодействие газа с поверхностью окисного полупроводника характеризуется определенными значениями энергии адсорбции, легирование позволяет варьировать эту величину так, чтобы вероятность взаимодействия измеряемого газа с поверхностью полупроводника превышала вероятность взаимодействия с остальными газами, присутствующими в газовой среде, и, таким образом, обеспечивалась селективность измерения газа. Для повышения селективности в состав полупроводникового чувствительного элемента вводят легирующий материал - металл, полупроводник, диэлектрик или их комбинацию. При этом легирующий материал обеспечивает увеличение концентрации групп ионов, более активно взаимодействующих с измеряемым газом.

Целью работы является изучение влияния состава, морфологии и электрофизических свойств плёнок Sn-Y-O на адсорбционную активность поверхностных состояний.

Методика эксперимента

Пленки-нанокомпозиты Sn-Y-O изготавливались методом реактивного ионно-лучевого распыления составной мишени из олова и полосок иттрия в атмосфере Ar + O_2. Напылительная установка была изготовлена на основе вакуумного поста УВН-2М [4]. В зависимости от выбора состава мишени можно было изготавливать пленки с различным соотношением оксидов Sn и Y и концентрацией иттрия.

Толщина пленок измерялась на интерференционном микроскопе МИИ-4. Элементный состав нанокомпозитов определялся с помощью рентгеновского микроанализатора JXA-840. В качестве эталонов были использованы образцы чистых металлов олова и иттрия. К сожалению, эта методика не позволяет определить точный фазовый состав исследуемых образцов, поэтому соотношение оксидов оценивалось расчетным путем по содержанию олова, кислорода и марганца в разных образцах ($x \leq 2$, $y < 2$). Морфология поверхности отожженных пленок изучалась с помощью атомного силового микроскопа (АСМ) FemtoScan-001. Так же после отжига провели исследование морфологии и структуры пленки-композита Sn-Y-O (5 ат.% иттрия) методом HRTEM на просвечивающем электронном микроскопе H800 фирмы Philips Tecnai F-30. Электросопротивление пленок измерялось

Рембеза Станислав Иванович – заведующий кафедрой полупроводниковй электроники и наноэлектроники ФГБОУ ВПО ВГТУ, д-р физ.-мат. наук, профессор, тел. 8(473)243-76-95;

Русских Елена Алексеевна – аспирант ФГБОУ ВПО ВГТУ, тел. 8(473) 243-76-95;

Рембеза Екатерина Станиславовна – профессор ФГБОУ ВПО ВГТУ, д-р физ.-мат. наук, профессор, тел. 8(473) 243-76-95;

Русских Дмитрий Викторович – заместитель начальника кафедры прикладной математики и инженерной графики ФГБОУ ВПО «Воронежский Институт ГПС МЧС России», кандидат технических наук, e-mail: russcience@mail.ru.

четырехзондовым методом (установка ЦИУС-4) либо методом Ван-дер-Пау. Концентрация и подвижность свободных носителей заряда в пленках определялись с помощью эффекта Холла методом Ван-дер-Пау.

Газовая чувствительность пленок определялась как отношение сопротивления пленки на воздухе ($R_в$) к сопротивлению пленки при напуске исследуемого газа известной концентрации в герметичную кювету ($R_г$): $S_g = R_в/R_г$ [1]. Объем кюветы составлял 10 л, концентрация исследуемых газов в воздушной среде рассчитывалась по формуле Клапейрона-Менделеева.

Результаты и обсуждение

Непосредственно после изготовления пленки имеют аморфную структуру, для кристаллизации и для стабилизации поверхностного сопротивления применялся изотермический отжиг. Был выбран режим обработки образцов: T = 400 ^{0}C. Образцы отжигались при заданной температуре от 13 до 56 часов с контролем поверхностного сопротивления через каждый час. В результате отжига в течение первого часа сопротивление пленок, легированных 2 – 6 ат. % Y, уменьшается и уже после 5 часов начинает стабилизироваться.

Данные микроанализа показывают, что примесь иттрия в исследованных пленках SnO_2 распределена следующим образом: от 0,4 до 6 ат. % Y, что соответствует содержанию оксида металла от 0,6 до 9 ат. % Y_2O_3.

Изготовленные ионно-лучевым реактивным распылением плёнки Sn-Y-O имеют толщину 1,59 – 5,43 мкм. В пленках, содержащих 2,8 ат. % Y, толщина увеличивается, а затем уменьшается (рис. 1). Это может быть следствием неравномерности распыления мишени.

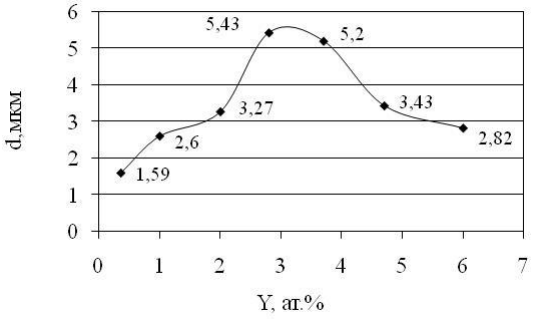


Рис. 1. Толщина пленок – композитов SnO_2:Y_2O_3 в зависимости от процентного содержания иттрия

Исходя из данных АСМ изображений был оценен средний размер зерен (рис. 2). Результаты исследований показывают, что композиты Sn-Y-O обладают наноструктурой со средним размером зерна от 3 нм до 40 нм. В зависимости от процентного содержания примесей оксида металла размеры зерен в пленках меняются: при увеличении содержания примеси величина зерна уменьшается. Это говорит о том, что наличие примеси иттрия препятствует росту больших конгломератов зерен. С уменьшением размера зерна пленок-нанокомпозитов увеличивается площадь поверхности, которая взаимодействует с газовой средой, таким образом, улучшая газочувствительные свойства.

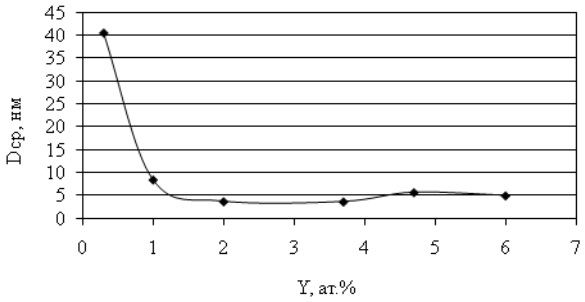


Рис. 2. Зависимость шероховатости поверхности пленки SnO_2:Y_2O_3 с различной концентрацией примеси иттрия

После отжига провели исследование структуры пленки-композита Sn-Y-O (5 ат.% иттрия) методом HRTEM на просвечивающем электронном микроскопе H800 фирмы Philips Tecnai F-30 (рис. 3).

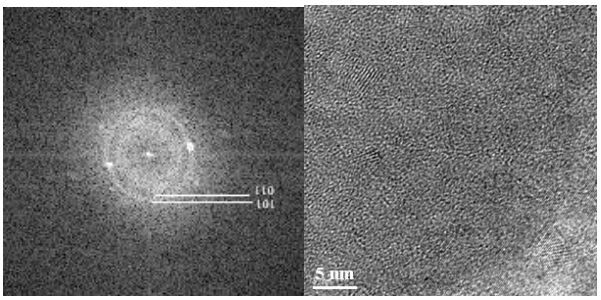


Рис. 3. Микродифракция и микроструктура пленки-композита Sn –(5 ат.%)Y-O, изготовленной ионно-лучевым распылением

Дифракционные кольца соответсвуют структуре SnO_2, наличие отдельной фазы Y_2O_3 не наблюдается. Это может быть объяснено тем, что Y_2O_3 находится в межзеренных границах SnO_2. Это расположение повышает эффективную высоту потенциального барьера для перехода электронов от одного зерна к другому.

Из картинки микроструктуры пленки-композита Sn–(5 ат.%)Y-O видно, что пленка состоит из хорошо закристаллизованного зерна, средний размер которых составляет приблизительно 3 нм, эти данные согласуются с данными, полученными методом АСМ.

Было рассчитано, что в нанокомпозите Sn –Y – O (5 ат.% иттрия) интервал между смежными краями решетки находятся в диапазоне от 0,324 нм до 0,335 нм, которые соответствуют значению C = 0,3185 нм координации [110] SnO_2 кристаллической решетки типа рутила.

Исследовалась газовая чувствительность пленок диоксида олова, легированных иттрием до 2,8 ат. %, 4,7 ат. % и 6 ат. % к парам этанола, ацетона, изопропилового спирта и формальдегида. Из полученных данных построены графики зависимости температуры максимальной газовой чувствительности к парам различных веществ в воздухе от процентного содержания примеси иттрия в исследуемых пленках (рис. 4.).

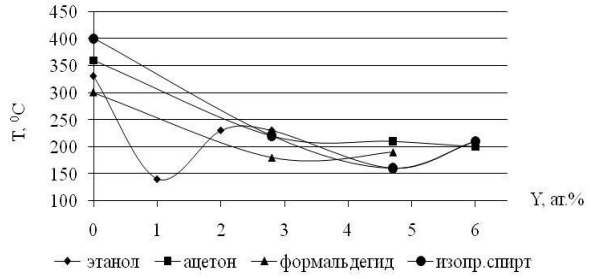


Рис. 4. Зависимость температуры максимальной газовой чувствительности к парам различных веществ от концентрации иттрия в образце SnO_2:Y_2O_3

Известно, что нелегированные пленки SnO_2 определяют наличие спирта при T = 330 °C, ацетона при T = 360 °C, изопропилового спирта при T = 400 °C, формальдегида при T = 300 °C [5]. Плёнки SnO_2: (2,8 ат. %) Y обнаруживают пары этанола при температуре 230 °C; ацетона – 220 °C; изопропилового спирта - 220 °C; формальдегида - 180 °C. Плёнки SnO_2: (4,7 ат %) Y обнаруживают пары этанола при температуре 150 °C; ацетона – 260 °C; изопропилового спирта – 160 °C; формальдегида – 190 °C. Плёнки SnO_2: (6 ат %) Y обнаруживают пары этанола при температуре 210 °C; ацетона – 220 °C; изопропилового спирта – 210 °C; аммиака – 180 °C.

Установлено, что легирование иттрием снижает температуру максимальной газовой чувствительности к различным газам на 100 – 160 °C. Причем, этот эффект для каждого газа проявляется по-разному, что можно использовать для повышения селективности пленки к различным газам. Этот результат показывает, что исследованные пленки при их применении в датчиках газов позволят уменьшить величину потребляемой мощности датчика при контроле примесей исследованных газов в воздухе.

На рис. 5 представлена диаграмма селективности измерения газовой чувствительности к парам различных веществ в воздухе в зависимости от процентного содержания примеси иттрия в пленке SnO_2:Y_2O_3 и показаны температуры максимальной газовой чувствительности.

Из диаграммы видно, что наибольшей чувствительностью к парам этанола обладает образец 3,7 ат.% иттрия в композите Sn-Y-O. Для исследуемых образцов с концентрациями примеси иттрия от 1 ат.% до 6 ат.% чувствительность к парам этанола меняется от 10% до 28% . Так же из диаграммы видно, что наибольшей чувствительностью ко всем исследуемым веществам в воздухе имеет образец с концентрацией 4,7 ат.% иттрия. Его чувствительность приблизительно в 2 раза больше чем у других образцов. При увеличении концентрации примеси чувствительность практически не меняется, следовательно, наиболее оптимальный режим для легирования пленок диоксида олова иттрием составляет от 2,8 ат.% до 5 ат.%.

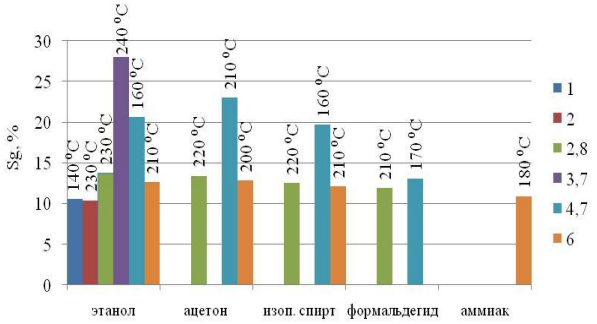


Рис. 5. Диаграмма селективности измерения газовой чувствительности к парам различных веществ в воздухе в зависимости от процентного содержания примеси иттрия в пленке SnO_2:Y_2O_3

Выводы

Из проделанной работы можно сделать следующие выводы:

1) Методом реактивного ионно-лучевого напыления изготовлены пленки нанокомпозиты Sn-Y-O с содержанием примеси иттрия от 0,4 до 6 ат. %. Установлена зависимость толщины плёнки от процентного содержания иттрия.

2) Исследована морфология поверхности пленок в зависимости от содержания примеси иттрия. На основании результатов АСМ-исследований рассчитана средняя высота зёрен в пленке в зависимости от процентного содержания иттрия. Содержание примеси иттрия заметно влияет на размер зерна поликристаллов. Увеличение концентрации Y приводит к уменьшению среднего размера зерна поликристаллов в пленках.

3) Исследована структура пленки с содержанием 5 ат.% примеси иттрия методом HRTEM на просвечивающем электронном микроскопе. Из картинки микроструктуры установили, что средний размер зерна составляет приблизительно 3 нм. Было рассчитано, что интервалы между смежными краями решетки находятся в диапазонах от 0,324 нм до 0,335 нм, которые соответствуют значению C = 0,3185 нм координации [110] SnO_2 кристаллической решетки типа рутила.

4) Исследованы газовая чувствительность пленок нанокомпозитов Sn-Y-O к различным газам-восстановителям, а также зависимость температуры максимальной газовой чувствительности пленок Sn-Y-O к парам различных газов в воздухе от процентного содержания примеси иттрия. Увеличение концентрации Y приводит к снижению температу-

ры максимальной газовой чувствительности нанокомпозита, что может быть использовано для уменьшения потребляемой мощности сенсоров газов и улучшения селективности газовой чувствительности пленок к различным газам. Таким образом, пленки Sn-Y-O являются перспективным материалом для чувствительных элементов микроэлектронных датчиков газов, так как обладают хорошей чувствительностью и селективностью к разным газам и позволяют контролировать газы при более низких температурах по сравнению с нелегированными пленками SnO_2.

Литература

1. Watson J., Ihokura K., Coles G.S.V. The tin dioxide gas sensor // Meas. Sci. Technol. 1993. № 4. P.711- 719.

2. Рембеза С.И., Свистова Т.В., Рембеза Е.С., Горлова Г.В. Электрические и оптические свойства полупроводниковых пленок на основе SnO_2 и SiO_2 // Электротехника. 2004. Т.10. С. 10-14.

3. Рембеза Е.С., Свистова Т.В., Рембеза С.И., Комарова А.С., Дырда Н.Н. Структура и электрофизические свойства нанокомпозита SnO_x:MnO_y // Нано- и микросистемная техника. 2006. Т.4. С. 27-29.

4. Золотухин И.В., Калинин Ю.Е, Стогней О.В. Новые направления физического материаловедения. Воронеж: ВГУ, 2000. 360 с.

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежский институт Государственной противопожарной службы МЧС России»

* Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежский Государственный технический университет»

STRUCTURE AND GAS SENSING PROPERTIES OF Sn-Y-O NANOCOMPOSITE AS PERSPECTIVE MATERIAL FOR DETECTION OF TOXIC AND EXPLOSIVE GASES

E.A. Russkih, S.I. Rembeza, E.S. Rembeza, D.V. Russkih

In article are reported results research structure and gas properties of films-composites Sn - Y - O with various concentration of an impurity yttrium in various gases in air. It is shown, that dopant film nanocomposites Sn-Y-O of yttrium reduces temperature of the maximum gas sensitivity to various gases.

Keywords: test structures, volt-amper characteristic, gas sensitivity.

УДК 37.034

К ВОПРОСУ О МОДЕЛИ ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ ГАЗОДЫМОЗАЩИТНИКА

А.В. Гуров

Предлагаемая модель подготовки газодымозащитника в системе непрерывного профессионального образования включает три ключевых этапа: изучение профессиональных интересов школьников старших классов, получение специального образования пожарно-технического профиля, адаптация молодого специалиста, связанная со спецификой его практической деятельности.

Ключевые слова: *газодымозащитник, модель профессиональной подготовки газодымозащитника, этапы, принцип комплексности.*

Каждый год на промышленных объектах страны регистрируется несколько тысяч пожаров, которые сопровождаются не только огромными материальными затратами, но и человеческими жертвами. Ими наносятся крупные, порой невосполнимые потери населению и экономике страны.

Пожар представляет собой неконтролируемое горение горючих и сопутствующих материалов, причиняющее значительный материальный ущерб, несущий угрозу жизни и здоровью жильцам помещений, интересам всего общества и государства в целом.

Сложность в тушении пожаров обусловлена следующими аспектами:

психологическая подготовленность к встрече с новым опасным, специальная профессиональная подготовка,

теоретические и практические навыки,

правильность принятия решения в экстремальных условиях,

тактика ведения действий по ликвидации пожара и последствий ЧС [1].

Труд специалистов пожаротушения и ликвидации последствий ЧС сопряжен с психофизиологическими факторами, связанными с экстремальными условиями их профессиональной деятельности:

- непрерывным нервно-психическим напряжением, вызванным систематической работой в необычной среде (при высокой температуре, сильной концентрации дыма, ограниченной видимости и т.д.), постоянной угрозой жизни и здоровью (возможны обрушения горящих конструкций, взрывы паров и газов, отравление ядовитыми веществами, выделяющимися в результате горения), отрицательными эмоциональными воздействиями (вынос раненых и обожженных и т.п.);

- большими физическими нагрузками, связанными с демонтажем конструкций и оборудования, прокладкой рукавных линий, работой с пожарно-техническим вооружением и оборудованием различного назначения, эвакуацией материальных ценностей, высоким темпом работы и т.д.;

- необходимостью поддерживать интенсивность и концентрацию внимания, чтобы следить за изменением обстановки на пожаре, держать в поле зрения состояние многочисленных конструкций, технологических агрегатов и установок в процессе выполнения поставленных задач на горящем объекте;

- трудностями, обусловленными необходимостью проведения работ в ограниченном пространстве (в тоннелях, подземных сооружениях, газопроводных и кабельных коммуникациях), что нарушает привычные способы продвижения и т.д.;

- высокой ответственностью каждого участника тушения пожара при относительной самостоятельности действий и решений по спасанию жизни людей, материальных ценностей и т.д.;

- наличием непредвиденных и внезапно возникающих препятствий, осложняющих выполнение поставленных боевых задач.

Исключительно важную роль при крупных пожарах играет деятельность газодымозащитной службы. Следовательно, от профессиональной подготовки газодымозащитника зависит жизнь, и пожарного и спасаемого им человека [1,2].

Профессиональная подготовленность газодымозащитников определяется степенью профессиональных знаний и умением выполнять оперативные действия по тушению пожаров и ликвидации чрезвычайных ситуаций в непригодной для дыхания среде [3].

В педагогической литературе отсутствует модель процесса подготовки газодымозащитника в системе непрерывного профессионального образования. При построении педагогической модели можно выделить следующие основные элементы ее построения:

• Личность;

• Социальный институт;

• Условия будущей профессиональной деятельности.

Построение модели подготовки будущего газодымозащитника в условиях непрерывного профессионального образования реализуется в следую-

Андрей Викторович Гуров – старший преподаватель кафедры пожарно-спасательной и газодымозащитной подготовки ФГБОУ ВПО «Воронежский институт ГПС МЧС России», тел. +7-951-567-27-61.

щем виде:

• Определение основополагающих принципов подготовки газодымозащитников, включающих в себя общепрофессиональные компоненты (знания по развитию пожара в замкнутых объемах, по тушению пожаров) и профессионально-ориентированные составляющие (практические навыки, физическая подготовленность, психологическая подготовка, профессиональная культура);

• Разработка практической модели подготовки газодымозащитника должна отражать постоянную связь между самостоятельными элементами.

Процесс непрерывной профессиональной подготовки газодымозащитника должен состоять, как минимум, из трех этапов, на каждом из которых не только доминируют те или иные социально-педагогические условия, но и различную роль играют субъекты, осуществляющие педагогическое воздействие:

• Первый этап - довузовский, задачей которого является выбор будущей профессии и проверка профессиональной пригодности.

• Второй этап — вузовский, период получения профессиональных знаний и выработки профессиональных практических навыков.

• Третий - послевузовский, период совершенствования знаний и умений.

Первый этап работы включает в себя изучение интересов школьников 9-11 классов, собеседований с ними, проведение психологический исследований и спортивных испытаний, что в данной профессии является основополагающим аспектом.

Первый этап можно разбить на стадии: формирование у школьников целостного представления о будущей профессии; формирование устойчивого интереса к службе в системе ГПС МЧС России. В результате, школьник должен составить свой индивидуальный план овладения будущей профессией.

В данном случае общеобразовательная подготовка является основополагающей в профессиональном образовании, так как призвана не только формировать знания, но и формировать личность, систему оценки ценностей.

Второй этап процесса подготовки газодымозащитника получение специального образования пожарно-технического профиля.

Основные задачи этапа:

- устойчивый интерес к службе в ГПС МЧС России;

- приобретение теоретических знаний и выработка навыков и умений использования этих знаний для решения профессиональных задач.

Третий этап (послевузовский) адаптация молодого специалиста, связанная со спецификой его практической деятельности.

На данном этапе газодымозащитник должен овладеть навыками комплексного использования полученных знаний и умений на двух предыдущих этапах. Ввиду специфики профессии данный этап реализуется в большей части путем самообразования и постоянными тренировками в соответствии с требованиями «Программы подготовки личного состава ГПС МЧС России», «Наставления по ГДЗС Государственной противопожарной службы…», «Методическими рекомендациями по организации и проведению занятий с личным составом ГДЗС ФПС МЧС России» (утверждены Главным военным экспертом МЧС России генерал-полковником Платом П.В. 30.06.2008г.), приказами МЧС, ЦРЦ, Главного управления, в меньшей степени посредством существующей системы повышения квалификации сотрудников, а также обучением в адъюнктуре и докторантуре [4,5,6].

Подводя итог изложенному, необходимо отметить, что в процессе построения модели профессиональной подготовки газодымозащитника, лежит принцип комплексности, что означает использование знаний, умений и навыков, приобретенных ранее, для решения поставленных задач в реальных условиях. Данная модель неизменна на протяжении всего периода времени (от момента выбора профессии), динамична лишь система подготовки кадров, с целью постоянного совершенствования.

Литература

1. Фонарев А.Р. Психология становления личности профессионала. М., 2005.

2. Гадышев В.А. Психолого-педагогические методы организации работы с кадрами государственной противопожарной службы. СПб., 2002.

3. Пономаренко Р.В. «Проблемы подготовки газодымозащитников». Материалы III всероссийской научно-практической конференции с международным участием «Пожарная безопасность: проблемы и перспективы» часть 1. с. 176.

4. Приказ № 234 от 30.04.96 г. «Об утверждении наставления по газодымозащитной службе Государственной противопожарной службы МВД России».

5. Приказ МЧС России № 624 от 31.12.02 года приложение 1 «Концепция совершенствования газодымозащитной службы в системе Государственной противопожарной службы МЧС России».

6. «Программа подготовки личного состава подразделений Государственной противопожарной службы МЧС России» (письмо от 16.02.2004г.).

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежский институт Государственной противопожарной службы МЧС России»

TO THE QUESTION ON MODEL OF PREPARATION OF A FIREMAN

A.V. Gurov

The offered model of preparation of a fireman in system of continuous professional education includes three key stages: studying of professional interests of school students of the senior classes, receiving vocational education of a fire and technical profile, the adaptation of the young specialist connected with specifics of his practical activities.

Keywords: fireman, model of vocational training of a fireman, stages, principle of complexity.

УДК 614.8.01

ПРОБЛЕМАТИКА РАЗВИТИЯ ПРОПАГАНДЫ В ОБЛАСТИ ПРОТИВОПОЖАРНОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ МЕДИАПРОСТРАНСТВЕ

Е.Н. Борзенкова, А.С. Харлан, Ю.М. Богатский, А.В. Калач

В статье рассмотрены проблемы развития пропаганды в области противопожарной безопасности и предложены пути их решения путем разделения объектов пропаганды на возрастные группы. Рассмотрены наиболее эффективные методы пропаганды для каждой группы с учетом использования достижений инновационного медиапространства.

Ключевые слова: *пропаганда в области противопожарной безопасности, медиапространство, возрастные группы, ОКСИОН.*

Современное восприятие медиа-пространства, сформированное благодаря развитию информационно-коммуникативных технологий, предлагает широкий спектр возможностей в области пропаганды противопожарной безопасности. Важнейшей характеристикой данного вида пропаганды является её эффективность, то есть 100% попадание в конкретную целевую аудиторию с использованием конкретного метода. Так, например, очень важно заранее разделить объекты пропаганды по группам, это могут быть как крупные деления (по возрастному критерию, гендерному признаку), так и, в зависимости от поставленных задач, небольшие группы (например: пассажиры поезда или самолета). Сегодняшнее медиа-пространство предлагает нам следующие каналы пропаганды: многочастотное радиовещание, цифровое и аналоговое телевидение, полиграфическая печать, уличные телевизионные экраны и графические билборды, мобильная связь и, наконец, интернет-коммуникация. Система ОКСИОН, функционирующая на территории РФ, рассчитана больше на информационную помощь непосредственно в условиях ЧС или в условиях проведения учебных запланированных ЧС. В задачи пропаганды входит постепенное накапливание аудиторией знаний о пожарах и верных правил поведения непосредственно в условиях данной ситуации. При современном уровне технического развития цивилизации, когда каждый имеет мобильный телефон, а порой не один и разных сотовых операторов, поразило следующее наблюдение: из 15 опрошенных 12 не знают, как позвонить с мобильного телефона в случае пожара. А если посмотреть на данные статистики за 2011 год, складывается следующая пожарная обстановка в Российской Федерации: зарегистрировано 168205 пожаров; прямой материальный ущерб от пожаров составил 16882,3 млн. руб.; при пожарах погибли 11962 человека, в том числе 492 ребенка; при пожарах получили травмы 12425 человек [6].

Возможно, какой-то пожар и не попал бы в печальную статистику, если бы граждане знали, как звонить в пожарную охрану с мобильного. Если мобильный аппарат не поддерживает набор номеров, состоящих из двух цифр, при звонках в экстренные службы после номера службы необходимо набирать знак *: 01* – Вызов пожарной охраны и спасателей; 010 – МТС, Мегафон, Теле-2, U-tel; 001 – Билайн; 901 – Скай-Линк, Мотив; “112” – экстренный вызов специальных служб на русском и английском языках. Опрос показал, что только возрастные группы «подростки» и «юноши» знают эти номера.

В целом крупное деление объекта пропаганды по возрастному критерию, на наш взгляд, в целях достижения основной функции эффективности является наиболее удачным. У социологов существует следующая шкала: период дошкольного возраста (1-7 лет), младшего школьного возраста (7-12 лет), подростковый период (12-16 лет), юношеский период (16-23 лет), зрелый возраст (два этапа 24-35 лет и 36-60 лет), преклонный возраст (60-74). Рассмотрим эффективные методы противопожарной пропаганды для каждой группы с учетом использования достижений инновационного медиа-пространства.

Период дошкольного возраста (1-7 лет). Противопожарная пропаганда для этого периода представляет собой устную пропаганду в основном родителей и воспитателей, кроме того, современные дети – это дети «телевоспитания», поэтому очень важно снимать для них добрые мультфильмы пропагандистской направленности, а еще лучше, если уже известные им герои смогут рассказать им о правилах пожарной безопасности, например, сегодня мультипликационный фильм «Маша и Медведь», «Аркадий Паровозов» могут перехватить эстафету пропаганды от советской книжки «Вера и Анфиса». На рис. 1-2 приведены примеры противопожарной безопасности для детей дошкольного возраста [7, 8].

Для этой группы будут интересны и сувениры пропагандистской направленности – это могут быть и обычные магниты на холодильник, но, например, необычной формы – в виде противогаза, огнетуши-

Борзенкова Елена Николаевна – библиограф библиотеки ФГБОУ ВПО «Воронежский институт ГПС МЧС России», тел. (473) 236-39-28;
Харлан Андрей Сергеевич – курсант 5 курса ФГБОУ ВПО «Воронежский институт ГПС МЧС России»;
Богатский Юрий Михайлович – юрисконсульт юридического отделения ФГБОУ ВПО «Воронежский институт ГПС МЧС России», тел. (473) 242-12-75;
Калач Андрей Владимирович – заместитель начальника ФГБОУ ВПО «Воронежский институт ГПС МЧС России» по научной работе, доктор химических наук, доцент, тел. (473) 220-99-29.

теля, своеобразная игрушка-напоминание.

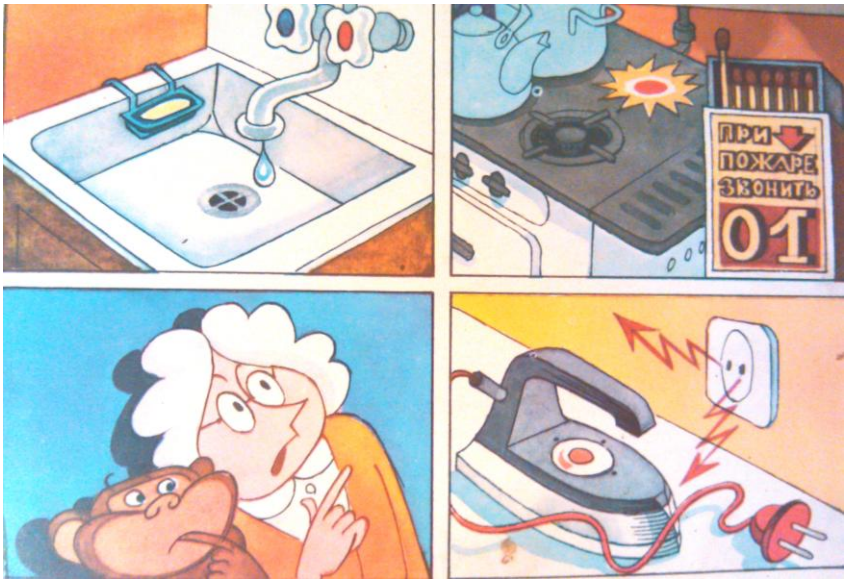


Рис. 1. Иллюстрация из книжки Э. Успенского «Вера и Анфиса»

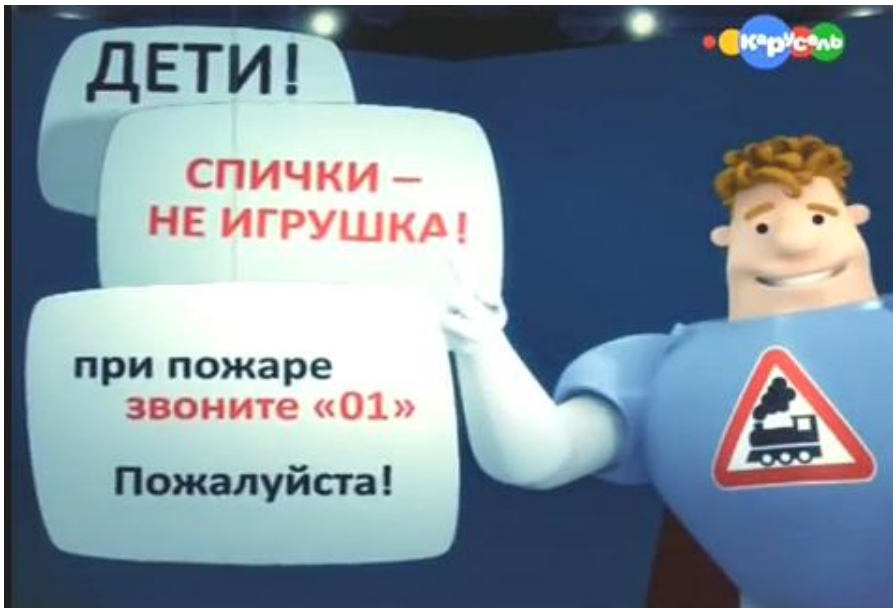


Рис. 2. Фрагмент из мультипликационного фильма «Аркадий Паровозов спешит на помощь»

Период младшего школьного возраста (7-12 лет). К предыдущим возможностям добавляем уже участие в школьных тренировочных эвакуациях в случае пожара, посещение пожарных частей (в этом году по всей России были организованы дни открытых дверей в пожарных частях), открытые уроки ОБЖ, которые проводят сотрудники МЧС России, не просто с текстовым материалом, но и с демонстрацией возможностей пожарной техники, например, на школьном стадионе. Метод визуального воздействия и чувство вовлеченности в происходящее однозначно оставит больше впечатлений, чем обычное повествование. В настоящее время торгово-развлекательные центры организуют выставки детских работ, которые периодически посвящены проблемам пожарной безопасности. Это ненавязчивый, легко воспринимаемый метод пропаганды; каждый участник нашего деления по возрастным группам так или иначе оказывается вовлечен в тематику пожарной безопасности. В качестве примеров на рис. 3,4 показаны образцы детских работ с выставок на тему противопожарной безопасности [8,9].

Рис. 3. Детский рисунок на тему «Противопожарная безопасность»

Рис. 4. Детский рисунок на тему «Противопожарная безопасность»

Подростковый период (12-16 лет). Ко всему описанному добавляем следующее: не просто участие, а активное участие в школьных тренировочных эвакуациях в случае пожара, например, с возможностью «выноса на носилках» раненого манекена, тушения небольшого очага возгорания при контроле сотрудников МЧС России. Этот возрастной период характеризуется повальным увлечением компьютерными играми, реальность переносится на экраны ноутбуков. Разработка игры крупными корпорациями – дорогостоящее дело, поэтому распространение получили игры-«квесты» online. В ходе игры запоминаются автоматические действия, которые при реальной опасности легко можно перенести в настоящую жизнь. На рис. 5-7 приведены «обложки» некоторых игр [10].

Юношеский период (16-23 лет), зрелый возраст (два этапа 24-35 лет и 36-60 лет) - это уже достаточно осмысленный период зрелой личности, поэтому на этих этапах уместно прибегать к проти-

вопожарной пропаганде, привязанной к месту, например, пропаганда на видеоэкранах или щитах в метро, автовокзалах и железнодорожных вокзалах, общественном транспорте, многофункциональных центрах предоставления государственных услуг, в помещениях ГИБДД и многих других местах массового скопления людей. Удачным примером является система ОКСИОН - общероссийская комплексная система информирования и оповещения населения в местах массового пребывания людей. Составной частью системы являются огромные плазменные или жидкокристаллические экраны, камеры видеонаблюдения, звукоусиливающее оборудование, оборудование для радиационного и химического контроля, расположенные как внутри помещений, так и на улицах. На рис. 8 приведены примеры работоспособности системы ОКСИОН [11].

Рис. 5. Фрагмент компьютерной игры «Iveco Magirus Fire Trucks»

Рис. 6. Фрагмент компьютерной игры «Fire Truck»

Рис. 7. Фрагмент компьютерной игры «American Firefighter»

Рис. 8. Фрагменты системы ОКСИОН

Преклонный возраст (60-74 лет) – эта категория воспитана еще на советской пропаганде гражданской обороны; для обеспечения эффективности пропаганды противопожарной безопасности можно использовать ретро-картинки. На рисунках 9-10 приведены их примеры [8].

Рис. 9. Календарь 1988 года на тему «противопожарная безопасность»

Рис. 10. Фрагмент плаката противопожарной пропаганды советского периода

Для того чтобы все функционировало комплексно и слаженно, а главное эффективно, должна быть подобрана грамотная команда разноплановых специалистов, в которую должны входить не только сотрудники МЧС, но и психологи, мультипликаторы, сценаристы, учителя, журналисты, социологи, рекламисты и многие другие. От эффективности пропаганды зависит далеко не научное, но самое важное - возможность жизни каждого из нас.

Анализируя и обобщая материалы по противопожарной пропаганде, можно сделать следующие выводы: пропаганда является важным этапом в формировании навыков и умений у населения безопасной жизнедеятельности, в том числе и противопожарной безопасности; современное медиапространство предлагает инновационные технологии для создания противопожарной медиапропаганды для каждой категории граждан; в настоящее время система противопожарной пропаганды доказывает свою жизнеспособность и эффективность, она совершенствуется и развивается с учетом запросов современного общества.

Литература

1. Калач Е.В. Киновоспитание гражданина: монография / Е.В. Калач. – Воронеж: Издательско-полиграфический центр Воронежского государственного университета, 2009. – 62 с.

2. Дзялошинский И.М. Информационное пространство России: структура, особенности функционирования, перспективы эволюции / И.М. Дзялошинский. – М., 2001. – 30 с.

3. Модели успеха: развлекательность, популярность, массовость, как явления культуры. – Тамбов, 2001. - 171 с.

4. Система средств массовой информации России: Учеб. пособие для студ. вузов / Под ред. Я.Н. Засурского. – М.: Аспект – Пресс, 2001. – 259 с.

5. Сметанкина Г.И., Вытовтов А.В.: Проведение

противопожарной пропаганды и обучение мерам пожарной безопасности // Материалы II научно-практической конференции. Воронеж, 2007. С. 287-291.

6. Лупанов С.А., Зуева Н.А. : Обстановка с пожарами в Российской Федерации в 2011 г // Пожарная Безопасность № 1 2012. Москва, 2012. С. 150-153.

7. Фотография предоставлена одним из авторов данной работы – Борзенковой Е.Н.

8. Интернет - ресурс http://images.yandex.ru/yandsearch?text [доступ 6.12.2012].

9. Интернет - ресурс http://www.pojarnayabezopasnost.ru/images/foto/pojarnayabezopasnost-26-big.jpg [доступ 6.12.2012].

10. Интернет - ресурс http://www.superigri.ru/%D0%B8%D0%B3%D1%80%D0%B0/s/fire+trucks+driver.html [доступ 6.12.2012].

11. Интернет - ресурс http://www.mchs.gov.ru/powers/oksion [доступ 7.12.2012].

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежский институт Государственной противопожарной службы МЧС России»

PROBLEMATICS OF DEVELOPMENT OF PROPAGATION IN THE FIELD OF FIRE-PREVENTION SAFETY IN MODERN MEDIA - SPACE

E.N. Borzenkova, A.S. Kharlan, Y.M. Bogatskiy, A.V. Kalach

In the article there are considered the problems of development of advocacy in the field of fire safety and suggested the ways of their solution by the division of objects of propaganda on the age group. Considered the most effective methods of propaganda for each group with the use of achievements of innovative media-space.

Keywords: advocacy in the field of fire safety, the media-space, age groups, OKSION.