*На правах рукописи*


**Панов Алексей Алексеевич**

# МОДЕЛИ И МЕТОДИКИ ПОИСКА ИСТОЧНИКОВ ВНУТРЕННИХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА МЧС РОССИИ

**05.13.19 – методы и системы защиты информации, информационная безопасность**

**Автореферат диссертации на соискание ученой степени кандидата технических наук**

14 АПР 2011

**Санкт-Петербург – 2010**

Работа выполнена в Санкт-Петербургском университете Государственной противопожарной службы МЧС России

**Научный руководитель:** доктор технических наук, профессор
Иванов Александр Юрьевич

**Официальные оппоненты:** доктор технических наук, профессор
Искандеров Юрий Марсович;
кандидат технических наук, доцент
Пантюхин Олег Игоревич

**Ведущая организация**: Санкт-Петербургский университет
МВД России

Защита состоится «17» февраля 2011 года в «14» часов на заседании совета по защите докторских и кандидатских диссертаций Д 205.003.02 при Санкт-Петербургском университете Государственной противопожарной службы МЧС России (196105, Санкт-Петербург, Московский проспект, д.149).

С диссертацией можно ознакомиться в библиотеке Санкт-Петербургского университета Государственной противопожарной службы МЧС России.

Автореферат разослан «17» января 2011 г.

Ученый секретарь
диссертационного совета Д 205.003.02
доктор технических наук, профессор А.Ю. Иванов

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы.** Действенность государственной политики по защите населения и территорий от чрезвычайных ситуаций (ЧС) природного и техногенного характера в существенной степени определяется характером управления силами и средствами, выполняющими задачи в таких ситуациях. Двадцатилетний опыт напряженной работы МЧС России показал необходимость широкого внедрения информационных технологий в сферу предупреждения и ликвидации ЧС. Этот процесс требует построения и организации применения разнообразных систем и средств, обеспечивающих реализацию названных технологий. К настоящему времени в МЧС России поставлены на дежурство и активно применяются автоматизированные системы (АС) различного функционального назначения и звеньев управления.

Осуществление эффективного взаимодействия между такими АС требует интеграции их информационных ресурсов, что приводит к формированию информационного пространства (ИП) МЧС России. Одной из важнейших задач при создании и использовании этого информационного пространства является обеспечение его безопасности. В настоящее время признано, что в автоматизированных системах независимо от их принадлежности и целевой направленности на первый план выдвигается борьба с нарушениями безопасности, исходящими от авторизованных пользователей.

В ИП существует и функционирует множество субъектов и объектов информационных отношений, многие из которых являются нарушителями безопасности и дезорганизуют работу пользователей. Такое положение требует реализации процедур поиска и обнаружения указанных субъектов и объектов с целью нейтрализации их действий, а также рационального размещения средств противодействия им в информационном пространстве.

Значительный вклад в становление и развитие научного базиса безопасности компьютерной информации внесли видные ученые и специалисты: Артамонов В.С., Гайкович В.Ю., Галатенко А.В., Зегжда Г.П., Зима В.М., Куватов В.И., Лукацкий А.В., Молдавян А.А., Молдавян Н.А., Щербаков О.В. и

другие. Их научные труды послужили основой проведения исследований в обозначенной предметной области.

Традиционные подходы к обеспечению внутренней безопасности АС отличаются ориентацией на предотвращение нарушений, совершаемых пользователями, и ставят целью совершенствование систем аутентификации, разграничения доступа, криптографической защиты и т.д. Существующие системы обнаружения компьютерных атак, в том числе и внутреннего происхождения, основаны на статистических наблюдениях или экспертном анализе поведения субъектов и объектов информационной безопасности. Эти системы не лишены таких недостатков как ложные срабатывания, пропуски атак, слабая реакция на нетрадиционные каналы атак, а также отсутствие методологических основ обнаружения угроз безопасности. Таким образом, возникает *проблемная ситуация*, характеризующаяся противоречием между недостаточным уровнем развития методов и средств поиска источников внутренних угроз безопасности информационного пространства и противодействия им, с одной стороны, и потребностью в адекватном реагировании на проявления таких угроз – с другой стороны. Сложившаяся ситуация, несомненно, нуждается в разрешении. Анализ публикаций свидетельствует, что в настоящее время отсутствуют научные подходы к снятию названной проблемы. Этим определяется *актуальность* темы диссертационного исследования.

**Цель работы** состоит в повышении уровня защищенности информационной сферы МЧС России за счет развития научных основ технологии поиска источников внутренних угроз безопасности информации.

**Объект исследования** – информационное пространство МЧС России, формируемое на базе взаимосвязанной иерархической совокупности информационных ресурсов автоматизированных систем в области предупреждения и ликвидации чрезвычайных ситуаций.

**Предмет исследования** – модели и методы поиска и размещения объектов в параметрических пространствах.

**Научная задача** заключается в разработке моделей и методик поиска

источников внутренних угроз безопасности информационного пространства МЧС России.

**Частные научные задачи** исследования:

1. Формирование общего подхода к защите информационного пространства МЧС России от внутренних угроз безопасности.

2. Построение представления информационного пространства как объекта защиты от внутренних угроз безопасности.

3. Разработка методики поиска источников внутренних угроз безопасности информационного пространства.

4. Разработка методики построения системы мониторинга информационного пространства для поиска источников внутренних угроз безопасности.

5. Выработка рекомендаций по применению моделей и методик, связанных с поиском источников внутренних угроз безопасности в информационном пространстве.

**Методы исследования.** Для решения научной задачи использовались методы общей теории систем, теории поиска, теории вероятностей, теории массового обслуживания, а также методы математического моделирования и математического программирования.

**Результаты исследования.** Основными результатами диссертационной работы, выносимыми на защиту, являются:

1. Модель информационного пространства как объекта защиты от внутренних угроз безопасности.

2. Методика поиска источников внутренних угроз безопасности информационного пространства.

3. Методика построения системы мониторинга информационного пространства.

**Научная новизна** результатов диссертационного исследования обусловлена представлением общего облика информационного пространства как совокупности информационных ресурсов автоматизированных систем управления МЧС России, подверженной деструктивному воздействию различных угрожающих

факторов, в особенности факторов внутреннего происхождении; адаптацией теоретических основ поиска объектов в дискретных пространствах к решению задач нахождения внутренних источников угроз безопасности информационного пространства, а также комплексным использованием методов размещения объектов и результатов моделирования системных образований на их основе при построении системы мониторинга информационного пространства.

**Достоверность** научных результатов обеспечивается использованием апробированного методологического аппарата сформировавшихся теорий в области математических методов и информационных технологий, а также корректностью основных положений и обобщений проведенного исследования.

**Практическая значимость** полученных результатов определяется их важностью для организации управления силами и средствами МЧС России при внедрении в этот процесс новых информационных технологий. Предпосылкой применения разработанных моделей и методик является стремление к повышению защищенности информационного базиса этих технологий за счет реализации научно-обоснованных подходов.

Определенная общность результатов позволяет сделать вывод о том, что модели и методики имеют научно-прикладное значение для других автоматизированных информационно-управляющих систем, функционирующих в потенциально небезопасной информационной обстановке.

**Публикации по теме диссертации**. Результаты диссертационного исследования опубликованы в пяти работах, в том числе в одном издании по перечню ВАК. Список публикаций приведен в конце автореферата.

**Реализация.** По результатам работы получены акты реализации от следующих организаций: Северо-Западный региональный центр МЧС России, Санкт-Петербургский университет ГПС МЧС России.

**Апробация результатов исследования**. Основные положения исследования докладывались и обсуждались в период с 2008 г. по 2010 г. на заседаниях постоянно действующего научно-тематического семинара Санкт-

Петербургского университета ГПС МЧС России, Международных научно-практических конференциях «Сервис безопасности в России: опыт, проблемы, перспективы» (Санкт-Петербург, 2008 и 2009 г.г.).

**Структура и объем работы**. Диссертация состоит из введения, трех глав, заключения, списка литературы и приложений. Общий объем диссертации составляет 92 страницы основного текста, в том числе 15 рисунков, 2 таблицы и список литературы из 85 наименований.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

**Во введении** обоснована актуальность работы, приведены основные атрибуты исследования, раскрыты полученные научные результаты и их характеристика, а также указаны сведения об апробации и реализации результатов диссертационного исследования.

**В первой главе «Анализ проблемы противодействия внутренним угрозам безопасности информационного пространства МЧС России»** обоснована актуальность и важность проблемы защиты информационного пространства МЧС России от внутренних угроз безопасности, для чего с системных позиций проведено исследование наиболее значительных и масштабных автоматизированных систем МЧС, изучено состояние их информационного обеспечения в аспекте формирования информационного пространства, выявлены угрозы внутренней безопасности этого пространства и показана их доминирующая роль, проанализированы существующие методы и средства защиты компьютерной информации от внутренних угроз безопасности и показан ограниченный характер их использования, а также выявлена и сформулирована проблема диссертационной работы и обозначено генеральное направление ее решения.

Сущность задач управления силами и средствами в чрезвычайных ситуациях состоит в расчете количественных и определения качественных характеристик, необходимых должностным лицам органов управления МЧС России при оценке обстановки в районе чрезвычайной ситуации, принятии

решений, планировании применения подчиненных подразделений, а также при проведении плановых и внеплановых мероприятий по предупреждению и ликвидации ЧС. Эффективное решение указанных задач в современных условиях не обеспечивается возможностями традиционного управления. Признанным направлением совершенствования управления силами и средствами в чрезвычайных ситуациях является автоматизация. Реализационная сторона автоматизации управления выражается в создании и применении автоматизированных систем (АС) МЧС России.

К настоящему времени создана и развивается автоматизированная информационно-управляющая система (АИУС), которая обеспечивает деятельность Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС), объединяющей органы управления, силы и средства федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, органов местного самоуправления и организаций, в полномочия которых входит решение вопросов в области защиты населения и территорий от ЧС. В АИУС РСЧС автоматизирован сбор и обработка информации о ЧС и проводимых мероприятиях, их учёт и накопление. Функциональные комплексы и задачи этой системы призваны обеспечить решение информационно-аналитических, прогностических, функциональных и специальных технологических задач управления.

Управление РСЧС осуществляет МЧС России. Основным органом управления выступает Национальный центр управления в кризисных ситуациях (НЦУКС), который представляет собой территориально-распределенный информационно-управляющий комплекс с периферийными элементами, позволяющими управлять силами, средствами и ресурсами РСЧС и гражданской обороны в условиях кризисов и ЧС. НЦУКС включает в себя соответствующие органы повседневного управления системы МЧС России (ЦУКС МЧС России, ЦУКС региональных центров, ЦУКС главных управлений МЧС России по субъектам РФ), их пункты управления, сети связи и передачи данных, а также автоматизированную систему.

Анализ построения АИУС РСЧС и АС НЦУКС показал их следующие специфические особенности. Во-первых, комплекс технических средств этих систем базируется на сетевую архитектуру и характеризуется существенным территориальным размахом. Во-вторых, в них аккумулируется огромное количество информационных единиц, которые позволяют описывать предметную область, связанную с предупреждением и ликвидацией ЧС, и обеспечивают решение задач управления.

Взаимосвязанная совокупность информационных ресурсов названных и других АС образует информационное пространство МЧС России (рисунок 1).


Рисунок 1 – Вариант формирования информационного пространства на базе АС НЦУКС

В этом пространстве на базе единых системных принципов осуществляется *сбор, накопление, актуализация, хранение и выдача по запросам должностных* лиц органов государственного управления и органов управления МЧС России, в частности, информации, необходимой для реализации функций управления в ЧС.

Распределенный характер ИП обеспечивает ряд преимуществ, таких как повышение оперативности и обоснованности принятия решений, поскольку необходимая информация может быть затребована от любой АС и своевременно передана потребителю с помощью технических средств. Однако реализация концепции ИП в практику органов управления сопровождается определенными издержками. В этом аспекте необходимо отметить заметное обострение проблемы защиты информации от разнообразных угроз. Наиболее общей классификацией угроз безопасности ИП следует считать деление всего их множества на внешние и внутренние угрозы. Традиционно наи-

большое внимание уделялось защите от угроз первого типа. Для этого используются надежные средства (например, межсетевые экраны), что существенно повышает уровень безопасности внешнего периметра ИП. Что же касается угроз внутреннего происхождения, то в пространстве большого размаха отслеживание действий пользователей только на основе кадровой политики и службы внутренней безопасности не вполне эффективно, а ущерб от нарушения целостности, конфиденциальности или доступности информации может носить катастрофический характер. Это подтверждается оценками специалистов по безопасности информации (таблица 1).

Таблица 1 – Рейтинговая оценка угроз безопасности информации

| Характер угрозы | Оценка важности (%) |
|---|---|
| Вредоносные программы | 77 |
| **Неправомерные действия пользователей** | **60** |
| Почтовый спам | 56 |
| Атаки типа отказ в обслуживании (блокировки систем и их элементов) | 48 |
| Финансовое мошенничество | 45 |
| Слабые места в системах безопасности | 39 |

Источниками внутренних угроз безопасности ИП МЧС России могут выступать следующие объекты и субъекты: недобросовестные или неквалифицированные пользователи, нештатное оборудование, постороннее программное обеспечение, внедренный вредоносный код, программы, являющиеся инструментами нарушителей безопасности информации (перехватчики сетевых пакетов, сканеры портов, взломщики паролей) и др.

Современные системы обнаружения нарушений безопасности информации (компьютерных атак на информацию), в том числе и внутреннего происхождения, основаны на статистических наблюдениях или экспертном анализе поведения субъектов и объектов информационной безопасности. Их внедрение в практику связано с существенными материальными издержками. К тому же эти системы не лишены таких недостатков как ложные срабатывания, пропуски атак, слабая реакция на нетрадиционные каналы атак, а также отсутствие математических основ обнаружения атак.

Таким образом, существующие системы обнаружения угроз безопасности информации не в состоянии обеспечить надежную защиту ИП МЧС России. Выход из сложившейся ситуации состоит в разработке новых моделей и методик поиска внутренних угроз безопасности.

**В рамках второй главы «Поиск и обнаружение источников внутренних угроз безопасности информационного пространства МЧС России»** разработаны основы организации информационного пространства МЧС России, которые оформлены в виде концептуальной модели, включающей в себя целевую установку, принципы построения и архитектурный облик этого пространства. Здесь же рассмотрены математические методы поиска объектов в пространстве в условиях различной степени информированности о наличии угроз. При этом задача поиска сформулирована как оптимизационная, использующая в качестве критерия максимум вероятности обнаружения требуемого объекта при ограничениях на поисковые усилия. На базе названных методов разработана методика поиска источников внутренних угроз, представляющая собой итеративную процедуру определения узлов информационного пространства, подверженных этим угрозам.

Под *информационным пространством* МЧС России предлагается понимать взаимосвязанную совокупность информационных ресурсов, ведущихся в интересах автоматизированного управления силами и средствами в операциях по предупреждению и ликвидации последствий ЧС.

Сложность ИП и важность решаемых с его помощью задач определяют необходимость обоснования *принципов* построения. Эти принципы устанавливают соответствие между объективными требованиями к организации ИП и субъективной деятельностью разработчиков во избежание принятия ошибочных решений на построение и управление пространством при функционировании АС. В более узком аспекте принципы можно рассматривать как общие требования, которым должно удовлетворять пространство. Множество принципов состоит из двух подмножеств (таблица 2).

Таблица 2 – Принципы формирования информационного пространства МЧС России

| Организационные принципы | Технические принципы |
|---|---|
| 1. Единство методических, организационных, технологических основ и нормативно-правовой базы | 1. Территориально распределенное многоуровневое построение в соответствии со структурой системы управления МЧС |
| 2. Соответствие уровня сервиса, полноты, актуальности и оперативности существующих АС и баз данных требованиям эффективности управления силами и средствами | 2. Реализация информационного взаимодействия с другими информационными системами, в том числе международными |
| 3. Соответствие информационного взаимодействия нормативным правовым актам, соглашениям и регламентам | 3. Защищенность информационного пространства |
| 4. Оценка социально-экономического эффекта от создания и внедрения ИП | 4. Стандартизация информационных технологий, унификация и типизация проектных решений |
| 5. Ответственность за достоверность, полноту и актуальность предоставляемых сведений со стороны владельцев информационных ресурсов | 5. Беспрепятственное предоставление доступа к информационным ресурсам всем группам пользователей в соответствии с потребностями, задачами и полномочиями |
| 6. Координация работ по созданию и развитию ИП со стороны МЧС России при руководстве созданием и развитием компонентов других министерств и ведомств | 6. Минимизация дублирования и исключение противоречивости информационных ресурсов |
| 7. Ответственность владельцев информационных ресурсов за его регулярное информационное наполнение и актуализацию | 7. Использование единых справочников и классификаторов, согласованных с министерствами и ведомствами |
| 8. Разграничение доступа пользователей ИП в соответствии с нормативными правовыми актами | 8. Наращивание ИП исходя из перспектив развития АС без нарушения его функционирования |
| | 9. Открытость и модульность построения |

*Архитектура* ИП определяется совокупностью решений по структурному построению системы управления МЧС, таких как территориально распределенный характер и иерархическая организация. В соответствии с этим ИП может быть представлено в виде решетчато-пирамидальной или графовой моделей (рисунок 2 и рисунок 3 соответственно).

Приведенные модели соответствуют дискретному характеру ИП. Каждый узел описывается вектором уязвимостей и угроз, которые могут быть реализованы через присутствующие уязвимости. Масштаб и сложная организация ИП определяют нетривиальность задачи поиска источников внутренних угроз безопасности. При этом под источником угрозы понимают либо присутствующую уязвимость узла, либо объект или процесс, свидетельствующий о реализации угрозы.

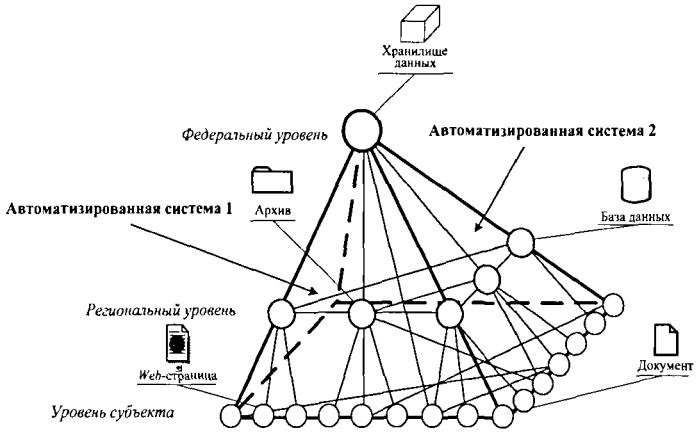


Рисунок 2 – Интерпретация ИП решетчато-пирамидальной моделью

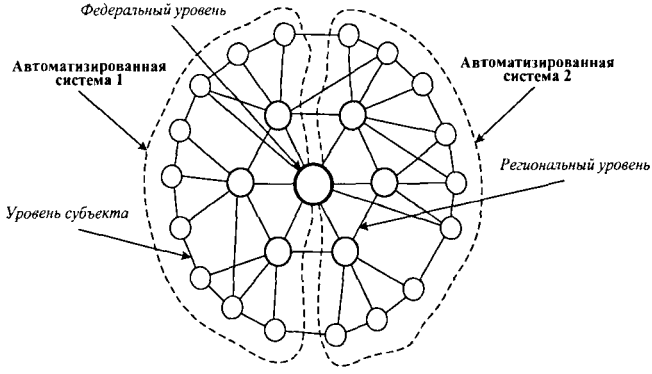


Рисунок 3 – Интерпретация ИП графовой моделью

Субъект поиска обычно называют *наблюдателем*, а объект поиска – *мишенью*. Таким образом, поиск определяется как *планирование и реализацию наблюдения с целью обнаружения мишени*. Совокупность ресурсов, необходимых для осуществления поиска, называют *поисковыми усилиями*.

В наиболее неблагоприятном случае наблюдатель ничего не знает о координатах мишени в поисковом пространстве. Ему может быть известно лишь то, что мишень находится в некоторой области $W$, состоящей из $N$ узлов.

Вероятность обнаружения мишени в подобласти $W_i$ $(W_i \in W)$, состоящей из $M_i$ узлов, определяется как произведение вероятности того, что мишень окажется в этой подобласти $(M_i/N)$ на вероятность того, что мишень будет

обнаружена, если она действительно находится в подобласти $W_i$ – $P(g_i)$, где $g_i$ – величина поисковых усилий, затрачиваемых в подобласти $W_i$. Полная вероятность успешного поиска определится как

$$P(g)=\sum_{i=1}^{n}(M_i/N)P(g_i), \qquad (1)$$

где $n$ – число подобластей поиска, на которое разделена область $W$.

Если же распределение усилий в области $W$ проводить неравномерно, перераспределив поисковые усилия между равными по количеству узлов областями $W_i$ и $W_j$ следующим образом: $g_i=(g/n)+\Delta g$ и $g_j=(g/n)-\Delta g$, где $g$ – общие поисковые усилия, то вероятность обнаружения мишени $P(g)$окажется ниже, чем при равномерном распределении поисковых усилий. Действительно, если принять

$$P(g_i)=1-e^{-g_i}, \qquad (2)$$

то удвоение поисковых усилий $g_i$ не приводит к удвоению вероятности $P(g_i)$. Поскольку $P(g_i+\Delta g)-P(g_i)<P(g_i)-P(g_i-\Delta g)$, вероятность обнаружения мишени уменьшается на величину $(M_i/N)[P(g_i+\Delta g)+P(g_i-\Delta g)-2P(g_i)]$.

Таким образом, в условиях абсолютной неопределенности о координатах мишени оптимальным является распределение имеющихся поисковых усилий по всем $N$ узлам, составляющим область $W$.

Предположим, что по априорным оценкам вероятность нахождения мишени в узле $k$ определяется как $\xi_k$, при этом $0\le\xi_k\le1$, но условие $\sum_{k=1}^{N}\xi_k=1$ выполняется не обязательно. Связь между вероятностью обнаружения мишени в $k$-м узле (если мишень действительно находится в этом узле) и поисковыми усилиями в этом узле $g_k$ задается функцией $P(g_k)$, которая инвариантна при переходе от одного узла к другому.

Суммарные поисковые усилия представляются в виде $G=\sum_{k=1}^{N}g_k$. Тогда требуется найти вариант распределения этих усилий по $N$ узлам, обеспечи-

вающий $\max\left[\sum_{k=1}^{N}\xi_k P(g_k)\right]$.

Воспользовавшись ранее принятым отношением (2), можно определить вид целевой функции

$$\max \mathrm{P}(G)=\sum_{k=1}^{N}\xi_k\left(1-e^{-g_k}\right), \tag{3}$$

при $G=\sum_{k=1}^{N}g_k$, $g_k\geq 0$, $k=1...N$.

Преобразовав правую часть выражения (3) как

$$\sum_{k=1}^{N}\xi_k\left(1-e^{-g_k}\right)=\sum_{k=1}^{N}\left(\xi_k-\xi_k e^{-g_k}\right)=\sum_{k=1}^{N}\xi_k-\sum_{k=1}^{N}\xi_k e^{-g_k}=Y-\sum_{k=1}^{N}\xi_k e^{-g_k}, \tag{4}$$

получаем возможность трансформировать целевую функцию к виду

$$\min Q(G)=\sum_{k=1}^{N}\xi_k e^{-g_k}, \tag{5}$$

при тех же ограничениях.

Решение поставленной задачи может быть найдено в соответствии со следующим *алгоритмом*.

*Шаг 1*. Вычисляются значения $\ln(1/\xi_k)$, в последующем располагаемые в возрастающей последовательности. Здесь же вычисляются частные суммы $R_n=\sum_{k=1}^{n}\ln(1/\xi_k)$ и строится возрастающая с увеличением $n$ последовательность $Z_n=(R_n/n)-\ln(1/\xi_n)$, $n=1...N$.

*Шаг 2*. Если выполняется неравенство $Z_1=0\leq G\leq Z_2$, то поиск ведется только в узле, соответствующем первому месту последовательности $\langle\ln(1/\xi_k)\rangle$, вероятность попадания мишени в которую наибольшая. Тогда принимается $g_i=G$ при $i=1$ и $g_i=0$ при $i>1$. Соответственно $\mathrm{P}=g_1\left(1-e^{-G}\right)$.

В случае, когда выполняется неравенство $Z_n\leq G\leq Z_{n+1}$, поиск следует осуществлять в $n$ узлах, которые характеризуются относительно большими значениями вероятностей нахождения в них мишени. Тогда

$$g_i=\left[(R_n+G)/n\right]-\ln(1/\xi_i) \text{ при } i\leq n;\ g_i=0 \text{ при } i>n. \tag{6}$$

$$P = \sum_{i=1}^{n} P_i,\ P_i = \xi_i - e^{-(R_n+G)/n} \text{ при } i \le n. \quad (7)$$

Если же $Z_n < G$, необходим поиск во всех $N$ узлах и

$$g_i = [(R_N + G)/N] - \ln(1/\xi_i), \quad (8)$$

$$P = \sum_{i=1}^{N} P_i,\ P_i = \xi_i - e^{-(R_N+G)/N},\ G = \sum_{i=1}^{N} g_i. \quad (9)$$

Возможно, что после исполнения полученного плана реализации поисковых усилий $G$ мишень окажется необнаруженной. Тогда следует затратить дополнительные поисковые усилия $\Delta G = \hat{G} - G$. После этого алгоритм реализуется повторно, при этом в расчетные соотношения (6-9) вместо $G$ подставляется $\hat{G}$, и на $i$-й узел направляются дополнительные поисковые усилия $(\hat{g}_i - g_i)$, $i = 1...N$.

Предложенные методы составляют основу методики поиска источников внутренних угроз безопасности ИП. Процедурная часть этой методики может быть представлена следующим алгоритмом (рисунок 4).

**Третья глава «Мониторинг информационного пространства МЧС России для поиска источников внутренних угроз безопасности»** определяет общий подход к построению системы мониторинга информационного пространства, содержит решения по анализу этой системы при помощи моделирования, а также охватывает материал, связанный с ее синтезом на основе методов математического программирования.

*Мониторингом* называют систему наблюдений и контроля, проводимых регулярно по определенной программе для оценки состояния контролируемой среды, анализа происходящих в ней процессов и своевременного выявления тенденций ее изменения. Мониторинг проводится в режиме реального времени, что имеет решающее значение при организации мониторинга в интересах обеспечения безопасности информационного пространства.

Реализация мониторинга ИП возможна при наличии аппаратно-программных комплексов, ориентированных на сканирование пространства с целью обнаружения уязвимостей или признаков аномальной деятельности объектов безопасности. Такие комплексы получили название «сенсоры».

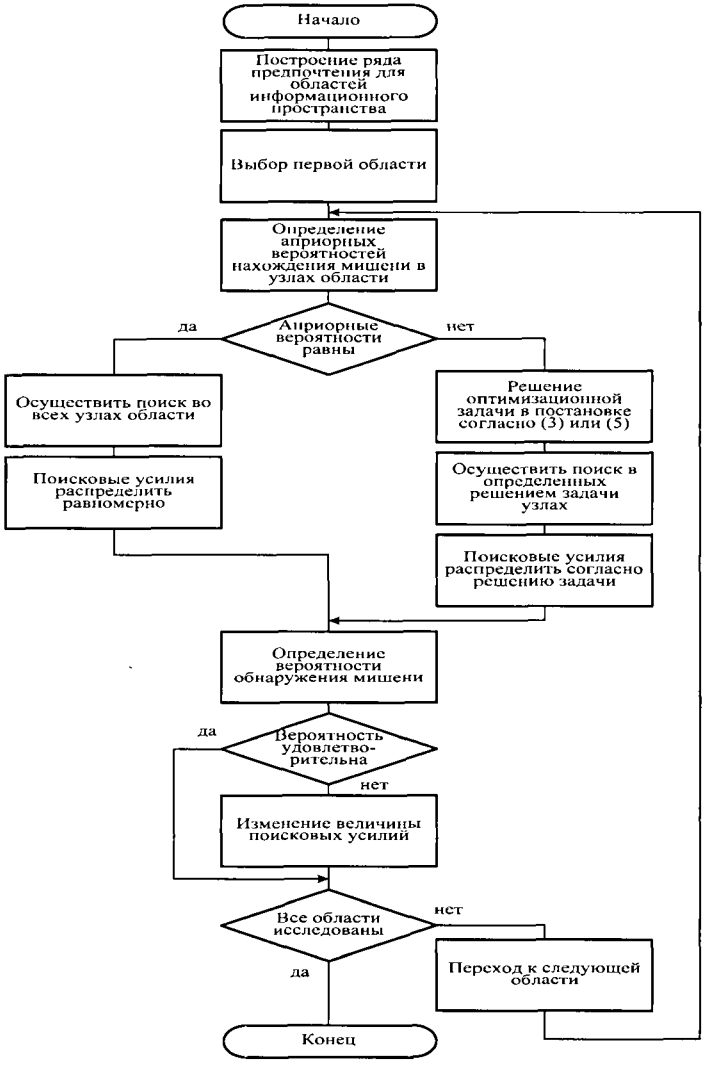


Рисунок 4 – Блок-схема алгоритма поиска объектов в информационном пространстве

Очевидно, что большой масштаб ИП требует наличия множества подобных комплексов, каждому из которых выделяется часть пространства для мониторинга. Данные мониторинга подлежат обработке на некоторых узлах (станциях), осуществляющих сбор информации от сенсоров. Таким образом, структура системы мониторинга может быть представлена следующим образом (рисунок 5).

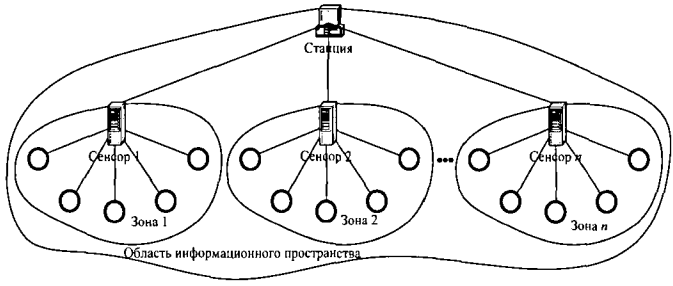


Рисунок 5 – Структура системы мониторинга информационного пространства

Поскольку мониторинг должен выполняться в реальном времени, доминирующим свойством системы мониторинга признается оперативность. Это свойство можно оценить через суммарные временные задержки в реализации процедур контроля. Названные задержки зависят от множества факторов и, следовательно, являются случайными величинами. Такое положение приводит к необходимости рассмотрения процесса мониторинга как случайного и исследования его в рамках теории вероятностей и теории массового обслуживания. Тогда система мониторинга может быть интерпретирована сетью массового обслуживания (рисунок 6), состоящей из различных систем массового обслуживания (СМО), таких как сенсоры (СМО 1), станции мониторинга (СМО 2), узлы информационного пространства (СМО 3), каналы передачи данных (СМО 4).

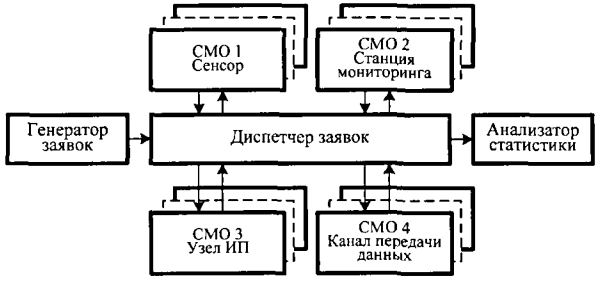


Рисунок 6 – Структурное построение модели системы мониторинга

Построение системы мониторинга информационного пространства требует определения числа и мест размещения компонентов этой системы, к наиболее важным и многочисленным из которых относятся сенсоры. Насы-

щение ИП большим количеством сенсоров приводит к существенному увеличению стоимости системы мониторинга. Снижение их числа относительно некоторого значения, способно привести к увеличению времени сбора и обработки информации. В такой ситуации возникает необходимость решения задачи размещения сенсоров в ИП. Эта задача относится к классическим задачам размещения с дискретным пространством решений – задачам о покрытии множества, т.е. определения числа и мест размещения объектов. Ее формулировка выглядит следующим образом.

*найти*

$$\min C = \sum_{j=1}^{n} c_j f_j \tag{10}$$

*при ограничениях*

$$\sum_{j=1}^{n} k_{ij} f_j \geq 1, \quad i = 1...m, \tag{11}$$

$$f_j = (0,1), \quad j = 1...n. \tag{12}$$

где $k_{ij}$ – коэффициент покрытия, причем $k_{ij}$ =1, если $i$-й узел информационного пространства располагается в пределах $j$-й зоны и $k_{ij}$ =0 в противном случае; $f_j$ =1, если в $j$-й зоне расположен некоторый сенсор и $f_j$ =0 в противном случае. Указанные ограничения требуют, чтобы каждый из $m$ узлов попадал в зону ответственности, по крайней мере, одного из $n$ сенсоров. В этом случае цель состоит в том, чтобы обеспечить попадание узлов в зону ответственности с минимальными затратами, причем $c_j$ – затраты на размещение сенсора в $j$-й зоне. При $c_j$=1, $j$=1…$n$ задача (10-12) сводится к задаче о полном покрытии.

На практике не всегда возможно разместить в сети такое количество сенсоров, которое полностью удовлетворяло бы потребности всех узлов (например, из-за ограничений на стоимость системы мониторинга). Обычно реальное количество сенсоров способно удовлетворить только некоторое подмножество узлов. Тогда целесообразно вести речь о частичном покрытии. Эта задача связана с связана с определением размещения заданного сенсоров, при котором своевременно удовлетворяются потребности максимального числа узлов.

*найти*

$$\max Z = \sum_{i=1}^{m} \max k_{ij} f_i, \quad 1 \le j \le n, \tag{13}$$

*при ограничениях*

$$\sum_{j=1}^{n} f_j \le K, \tag{14}$$

$$f_j = (0,1), \quad j = 1...n. \tag{15}$$

где $K$ – максимальное количество сенсоров, подлежащих размещению.

Задача построения системы мониторинга информационного пространства МЧС России по своей сущности является задачей синтеза, направленной на отыскание структуры и параметров названной системы в зависимости от ее характеристик, значения которых определяются требованиями по оперативности выдачи результатов мониторинга. Для ее решения предложено использование подхода, известного под названиями «итеративный синтез» или «синтез через анализ». Традиционный способ решения таких задач предполагает построение итеративной процедуры. В каждой итерации помимо расчета величины критерия проводится модификация очередного варианта построения системы, после чего вариант подвергается оценке. Тогда методика построения системы мониторинга имеет структуру, представленную на рисунке 7.

*Первый этап* связан с формированием начального построения системы мониторинга информационного пространства. Для этого в зависимости от цели построения системы (полное или частичное покрытие) используются задачи (10-12) или (13-15). На *втором этапе* осуществляется оценка полученного варианта системы мониторинга с помощью ранее представленной модели. *Третий этап* заключается в проверке соответствия полученных значений параметров системы мониторинга и их требуемых величин. Содержание *четвертого этапа* составляет изменение варианта построения системы мониторинга. Для этого задачи (10-12) или (13-15) решаются на модифицированных исходных данных, таких как новое зоновое построение пространства или другое количество сенсоров.


Рисунок 7 – Структурное представление методики построения системы мониторинга в виде блок-схемы алгоритма

Разработанная методика построения системы мониторинга рекомендуется к применению должностными лицами, ответственными за разработку и сопровождение комплексной системы обеспечения безопасности информационного пространства МЧС России, в частности, средств защиты от угроз внутреннего происхождения.

## ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

В диссертационной работе приведены решения, связанные с разработкой моделей и методик поиска внутренних источников угроз безопасности информационного пространства МЧС России с целью повышении уровня его защищенности.

Предложена концептуальная модель информационного пространства МЧС России, которая определяет принципиальные и архитектурные основы его организации и особенности как объекта защиты от внутренних угроз безопасности.

Представлены методы поиска объектов в дискретных пространствах, на основе которых разработана методика поиска источников внутренних угроз

безопасности информационного пространства МЧС России, позволяющая оптимизировать распределение поисковых усилий по критерию максимума вероятности обнаружения указанных источников.

Сформирована методика построения системы мониторинга информационного пространства с целью его исследования на наличие признаков внутренних угроз безопасности. Методика базируется на оценочную модель и методы размещения объектов в пространстве, применение которых обеспечивает рациональное структурное построение системы, отвечающее требованиям к оперативности ее функционирования.

Представленный в работе инструментарий рекомендуется использовать при разработке и модернизации комплексной системы защиты информационного пространства МЧС России.

**Основные работы, опубликованные по теме диссертации.**

*Издания по Перечню ВАК РФ:*

1. Иванов А. Ю., Панов А.А. Поиск источников угроз безопасности в информационных системах // Проблемы управления рисками в техносфере. 2010. № 2 [14]. (0,85/0,6 п.л.).

*Ведомственные издания:*

2. Панов А.А., Ходасевич Г.Б. Размещение компонентов системы мониторинга информационного пространства // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. Научный электронный журнал. http://vestnik.igps.ru. – СПб.: Санкт-Петербургский университет ГПС МЧС России, № 4, 2010. (0,8/0,4 п.л.).

3. Алексеева Е.В., Панов А.А. Реализация требований сервиса безопасности при организации управления в информационном пространстве МЧС // II междунар. науч.-практ. конф. «Сервис безопасности в России: опыт, проблемы, перспективы». – СПб, Санкт-Петербургский университет ГПС МЧС России, 2009. (0,3/0,2 п.л.).

4. Панов А.А. Проблемные вопросы формирования единого информационного пространства МЧС России и обеспечения его безопасности // Междунар. науч.-практ. конф. «Сервис безопасности в России: опыт, проблемы, перспективы». – СПб.: Санкт-Петербургский университет ГПС МЧС России, 2008. (0,2 п.л.).

5. Иванов А.Ю., Панов А.А. Защита информации от угроз, создаваемых факторами внутреннего риска. // Вестник Санкт-Петербургского института Государственной противопожарной службы МЧС России, Научно-практический журнал. 2006. №1[12]-2[13]. (0,8/0,5 п.л.).

Подписано в печать 14.01.2011 Формат 60x84 $^{1}/_{16}$
Печать цифровая Объем 1,0 п.л. Тираж 100 экз.
Отпечатано в Санкт-Петербургском университете ГПС МЧС России
196105, Санкт-Петербург, Московский проспект, дом 149