

**ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА**

**ПОСТАНОВЛЕНИЕ**  
**от 4 октября 2005 г. N 1505**

**О КОНЦЕПЦИИ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ**  
**ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ САНКТ-ПЕТЕРБУРГА**

Список изменяющих документов  
(в ред. Постановлений Правительства Санкт-Петербурга  
от 29.06.2007 N 716, от 30.03.2011 N 381,  
от 12.05.2012 N 453)

В целях повышения уровня обеспечения безопасности жизнедеятельности Санкт-Петербурга, информационного обеспечения граждан Санкт-Петербурга и органов государственной власти Санкт-Петербурга на основе полномасштабного использования информационно-коммуникационных технологий, а также рационального использования материальных и финансовых средств Правительство Санкт-Петербурга постановляет:

1. Одобрить [Концепцию](#) автоматизированной информационной системы обеспечения безопасности жизнедеятельности Санкт-Петербурга (далее - Концепция) согласно приложению 1.
2. Утвердить [План](#) мероприятий на 2005-2006 годы по реализации Концепции автоматизированной информационной системы обеспечения безопасности жизнедеятельности Санкт-Петербурга согласно приложению 2.
3. Контроль за выполнением постановления возложить на вице-губернатора Санкт-Петербурга Тихонова В.В.

Губернатор Санкт-Петербурга  
В.И.Матвиенко

ПРИЛОЖЕНИЕ 1  
к постановлению  
Правительства Санкт-Петербурга  
от 04.10.2005 N 1505

**КОНЦЕПЦИЯ**  
**АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ**  
**БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ САНКТ-ПЕТЕРБУРГА**

Список изменяющих документов  
(в ред. Постановлений Правительства Санкт-Петербурга  
от 29.06.2007 N 716, от 30.03.2011 N 381,  
от 12.05.2012 N 453)

1. Введение

### 1.1. Цель и задачи настоящей Концепции

Настоящая Концепция является методологической базой для создания автоматизированной информационной системы обеспечения безопасности жизнедеятельности Санкт-Петербурга.

Целью настоящей Концепции является выработка единого подхода к пониманию целей, задач и принципов построения автоматизированной информационной системы обеспечения безопасности жизнедеятельности Санкт-Петербурга (далее - АИС ОБЖ).

Основными задачами настоящей Концепции являются:

обоснование актуальности создания АИС ОБЖ;

постулирование принципов создания АИС ОБЖ;

выявление информационных ресурсов, используемых в рамках функционирования АИС ОБЖ;

определение основных функций и структуры АИС ОБЖ;

определение требований по обеспечению информационной безопасности АИС ОБЖ;

формулирование предложений по организационному и правовому обеспечению создания АИС ОБЖ;

определение этапности создания АИС ОБЖ.

### 1.2. Основания для разработки настоящей Концепции

Основанием для разработки настоящей Концепции является протокол совместного совещания Правительства Санкт-Петербурга и Министерства информационных технологий и связи Российской Федерации по вопросам развития информационных и коммуникационных технологий в Санкт-Петербурге от 04.03.2005.

Основой для предлагаемых в настоящей Концепции решений послужили следующие документы:

**Концепция** национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 17.12.1997 N 1300;

**Доктрина** информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации от 09.09.2000 N Пр-1895;

Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года, одобренная распоряжением Правительства Российской Федерации от 27.09.2004 N 1244-р.

### 1.3. Область действия настоящей Концепции

Предлагаемые в настоящей Концепции положения могут быть использованы при разработке и внедрении АИС ОБЖ в других субъектах Российской Федерации с развитой телекоммуникационной и информационной инфраструктурой.

Настоящая Концепция является основой для разработки программы создания АИС ОБЖ, разработки технических заданий, проектирования, создания опытных фрагментов, внедрения и ввода в эксплуатацию элементов АИС ОБЖ.

## 2. Актуальность создания АИС ОБЖ

### 2.1. Обеспечение безопасности жизнедеятельности - приоритетная задача управления социально-экономическим развитием Санкт-Петербурга

В современных условиях, характеризующихся снижением уровня военной опасности, угрозы техногенного, природного, криминогенного и террористического характера до сих пор представляют реальную опасность для населения регионов и развития государства в целом.

Характерной особенностью крупных мегаполисов, к числу которых относится и Санкт-Петербург, является большая плотность проживающего населения, концентрация культурных и материальных ценностей, наличие значительного количества потенциально опасных объектов. Это определяет высокую вероятность возникновения и тяжесть возможных последствий чрезвычайных ситуаций различного характера, повышенную опасность для жизни и здоровья населения.

Сложившаяся в данной области ситуация характеризуется следующими факторами, оказывающими существенное влияние на управленческие процессы в городском хозяйстве и на социальное и финансовое состояние Санкт-Петербурга:

возрастание угроз техногенного характера вследствие морального и физического старения объектов промышленной инфраструктуры, гидротехнического и жилищно-коммунального комплексов;

высокий уровень аварийности транспорта (ежегодно в стране на газо-, нефте- и продуктопроводах происходит около 50 тыс. аварий, а количество дорожно-транспортных происшествий доходит до 200 тыс.);

возрастание ущерба и числа погибших от пожаров (в 2004 году только на территории Северо-Западного федерального округа произошло более 26 тыс. пожаров, погибло около 2 тыс. человек. Средние потери, приходящиеся на один пожар, выросли до 320 тыс. руб.);

рост количества и масштабов последствий природных катаклизмов (лесных пожаров, наводнений и т.п.);

возрастание рисков при перевозке опасных грузов и усиление угроз химического, биологического и радиационного воздействия, напряженная санитарно-эпидемиологическая и санитарно-гигиеническая обстановка;

возникновение возможностей нарушения информационных ресурсов, систем и структур, разрушение их или искажение работы и содержания через специальные средства воздействия;

создание и провоцирование социальной, межнациональной, религиозной напряженности, возможность манипулирования массовым сознанием с использованием информационно-психологического воздействия;

нарастание угроз террористических проявлений.

В целом сумма материального ущерба от чрезвычайных ситуаций только на территории Северо-Западного региона в 2004 году составила 861 млн руб., что на 73 процента больше, чем в 2003 году.

Подводя итог анализа состояния безопасности жизнедеятельности в регионе и, в частности, в Санкт-Петербурге, следует отметить, что при существующих тенденциях отсутствие кардинальных решений в этой области может привести к целому перечню катастрофических последствий, в том числе к:

авариям и катастрофам регионального масштаба;

гибели и физическому травмированию людей;

разрушению и заражению среды обитания;

нарушению системы обеспечения жизнедеятельности Санкт-Петербурга;

крупномасштабному уничтожению национальных ресурсов (природных, сельскохозяйственных, продовольственных, производственных, информационных);

нанесению крупного экономического ущерба государственным и частным предприятиям и организациям, физическим лицам;

массовым нарушениям правопорядка.

В этой связи обеспечение безопасности жизнедеятельности и объектов инфраструктуры, формирование, поддержание и развитие среды жизнедеятельности, соблюдение жизненно важных интересов личности, общества и государства, недопущение, предупреждение и оперативная ликвидация чрезвычайных ситуаций являются приоритетными направлениями деятельности исполнительных органов государственной власти Санкт-Петербурга, территориальных органов федеральных органов исполнительной власти и органов местного самоуправления в Санкт-Петербурге.

## 2.2. Пути повышения уровня безопасности жизнедеятельности Санкт-Петербурга

В настоящее время Правительством Российской Федерации осуществляется комплекс мер, направленных на предупреждение чрезвычайных ситуаций, повышение возможностей по ликвидации их последствий, сокращение материального ущерба и потерь населения.

Однако реалии жизни говорят о том, что для ощутимого эффекта необходимы действенные меры именно в субъектах Российской Федерации.

Следует отметить, что при существующем состоянии бюджетного финансирования территориальных органов федеральных органов исполнительной власти добиться кардинального изменения положения дел в обеспечении безопасности жизнедеятельности субъекта Российской Федерации применением экстенсивных методов (например, путем количественного наращивания сил и средств силовых структур) крайне сложно.

В этих условиях наиболее целесообразными являются организационно-технические мероприятия, позволяющие повысить уровень безопасности жизнедеятельности Санкт-Петербурга путем оптимизации использования имеющихся ресурсов и повышения эффективности управления ими.

Обеспечением безопасности на уровне субъектов Российской Федерации занимаются прежде всего территориальные органы федеральных органов исполнительной власти, специализированные городские службы и частные охранные предприятия, коммерческие организации технического обеспечения безопасности. Перечисленные структуры на сегодняшний день не имеют централизованного управления, слабо взаимодействуют друг с другом и, как следствие, неэффективно используют свои ресурсы и технический потенциал. Кроме того, практически отсутствуют действенные механизмы взаимодействия исполнительных органов государственной власти Санкт-Петербурга, территориальных органов федеральных органов исполнительной власти и органов местного самоуправления в Санкт-Петербурге, имеет место неэффективное использование бюджетных средств Санкт-Петербурга по многочисленным, слабо увязанным между собой федеральным и региональным программам.

Вследствие разобщенности структур, решающих задачи безопасности жизнедеятельности в Санкт-Петербурге, инвестиции на их техническое оснащение тратятся на создание изолированных систем, слабо увязанных по задачам и протоколам информационного взаимодействия и требующих чрезмерных затрат на разработку, внедрение и содержание.

Таким образом, решение насущных задач обеспечения безопасности жизнедеятельности требует комплексных организационно-технических мероприятий на уровне субъекта Российской Федерации.

Первым и наиболее очевидным мероприятием, которое позволило бы повысить эффективность функционирования исполнительных органов государственной власти Санкт-Петербурга, территориальных органов федеральных органов исполнительной власти и органов местного самоуправления в Санкт-Петербурге, является организационное и техническое объединение их ресурсов (в первую очередь - технологических и информационных).

Централизованное управление ресурсами позволит оптимизировать их распределение при обеспечении безопасности жизнедеятельности всех групп и слоев населения и городских объектов, что практически эквивалентно созданию большого количества обособленных эффективных систем, но менее затратно по финансированию.

Задачи обеспечения безопасности жизнедеятельности, как правило, решаются в условиях жесткого дефицита времени. Ограниченность временных и материально-технических ресурсов и возможностей человека при больших масштабах и скорости развития чрезвычайных ситуаций влияет на адекватность и достоверность информации, используемой при принятии решений, а также на оперативность принятия этих решений. Эти аспекты обуславливают необходимость использования для решения задач безопасности современных технологий автоматизированного сбора, обработки, анализа и визуализации информации. В наши дни становится очевидным, что для эффективного управления сложными территориально распределенными объектами (город, производственное предприятие или коммерческая компания), повышения их среднесрочной и долгосрочной стабильности, снижения нагрузки на первых лиц необходимо применять информационные системы и автоматизированные системы управления, реализующие последние достижения управленческой науки.

Таким образом, вторым мероприятием, направленным на повышение эффективности обеспечения безопасности жизнедеятельности, является внедрение в процессы управления новейших информационных и телекоммуникационных технологий.

В результате выполнения первого и второго мероприятий возникнет реальная возможность создания интегрированного технологического и информационного ресурса общего пользования для исполнительных органов государственной власти Санкт-Петербурга, территориальных органов федеральных органов исполнительной власти, органов местного самоуправления в Санкт-Петербурге и других организаций, участвующих в обеспечении безопасности Санкт-Петербурга, который и ляжет в основу АИС ОБЖ.

### 3. Методологические основы создания АИС ОБЖ

#### 3.1. Цель и задачи создания АИС ОБЖ

Конечной целью создания и внедрения АИС ОБЖ является повышение уровня безопасности жизнедеятельности Санкт-Петербурга.

Основными путями достижения поставленной цели являются:

повышение качества управления Санкт-Петербургом и городским хозяйством за счет высокой оперативности взаимодействия и улучшения информационного обеспечения заинтересованных

городских и федеральных структур с использованием современных телекоммуникационных и информационных технологий;

координация совместных действий исполнительных органов государственной власти Санкт-Петербурга, территориальных органов федеральных органов исполнительной власти и органов местного самоуправления в Санкт-Петербурге в периоды повседневной деятельности и чрезвычайных ситуаций, в частности, повышение эффективности их работы, а также улучшение взаимодействия между специализированными городскими службами и населением Санкт-Петербурга.

При этом приоритетными задачами, решаемыми для достижения цели, являются:

интеграция разнородных информационных систем на базе единого стандарта обмена данными в целях повышения эффективности принятия управленческих решений на всех уровнях городской инфраструктуры, улучшения координации взаимодействия между подразделениями исполнительных органов государственной власти Санкт-Петербурга, территориальных органов федеральных органов исполнительной власти и органов местного самоуправления в Санкт-Петербурге;

создание информационной базы для внедрения типовых административных, технических и технологических решений, обеспечивающих единообразное взаимодействие между разнородными системами, функционирующими на территории Санкт-Петербурга;

создание нормативной правовой базы для интеграции и совместного использования информационных и технологических ресурсов исполнительных органов государственной власти Санкт-Петербурга, территориальных органов федеральных органов исполнительной власти, органов местного самоуправления в Санкт-Петербурге и других организаций, участвующих в обеспечении безопасности Санкт-Петербурга;

внедрение новых технологий и автоматизации процессов сбора, обработки, анализа и представления актуальной и достоверной информации оперативного характера о текущей обстановке, физических лицах, объектах и их состоянии, в том числе краткосрочное ситуационное прогнозирование, а также информации стратегического характера, что соответствует задачам среднесрочного и долгосрочного планирования социально-экономического развития Санкт-Петербурга, то есть задачам обеспечения безопасности устойчивого социально-экономического развития Санкт-Петербурга.

### 3.2. Анализ объекта автоматизации АИС ОБЖ

Качество управленческих решений, оперативность их принятия во многом зависят от актуальности, достоверности и полноты информации об объектах управления и контролируемых объектах.

Этот аспект обуславливает необходимость использования в системе управления обеспечением безопасности жизнедеятельности Санкт-Петербурга современных технологий автоматизации процессов информационной поддержки принятия решений. Таким образом, объектом автоматизации АИС ОБЖ являются процессы сбора, обработки, хранения, анализа, представления и визуализации информации.

Для выявления существенных сторон объекта автоматизации АИС ОБЖ, которые подлежат обязательному учету при формировании требований к функциональности, составу и структуре АИС ОБЖ, необходимо определение места объекта автоматизации в системе управления обеспечением безопасности жизнедеятельности Санкт-Петербурга.

Структурная схема процесса автоматизации АИС ОБЖ Санкт-Петербурга отображена на рис. 1.

## Рис. 1 Структурная схема процесса автоматизации АИС ОБЖ Санкт-Петербурга

Управляющим объектом является совокупность исполнительных органов государственной власти Санкт-Петербурга, территориальных органов федеральных органов исполнительной власти и органов местного самоуправления в Санкт-Петербурге, руководство предприятий, учреждений и их структурных подразделений, дежурные и диспетчерские службы. Под объектами управления понимается совокупность контролируемых объектов, в качестве которых могут выступать население, все значимые объекты инфраструктуры Санкт-Петербурга, окружающей среды, хозяйственной и экономической деятельности, а также силы и средства, задействованные в обеспечении безопасности жизнедеятельности Санкт-Петербурга.

Процессы информационной поддержки принятия решений отображены на рис. 2

## Рис. 2 Процессы информационной поддержки принятия решений

Исходной информацией, необходимой для принятия управленческих решений в сфере обеспечения безопасности жизнедеятельности Санкт-Петербурга, являются:

- достоверные данные о текущем состоянии (местоположении) объектов управления;
- критические значения параметров, характеризующих состояние объектов управления;
- архивные данные об объектах управления;

прогнозная информация о тенденциях и перспективах изменений состояния объектов и процессов, полученная по результатам обработки архивных данных с использованием математических моделей;

эталонные данные информационных систем (карты, кадастры, регистры, реестры и т.д.);

данные других информационных систем.

В условиях отсутствия автоматизации процесс сбора информации об объектах является трудоемким и продолжительным. Как правило, информация передается по телефонным (радиотелефонным) каналам, каналам передачи телеметрической информации либо с использованием бумажных носителей. При этом на достоверность информации существенно влияет субъективный фактор, а ее актуальность по окончании сбора может утрачиваться.

Процесс контроля над объектами заключается в сравнении результатов наблюдения (текущих или архивных) с некоторыми критериями, на основании которого вырабатывается заключение о нормальном или критическом состоянии объекта.

В ряде случаев необходимо прогнозировать изменение состояния объекта (процесса) во времени. Решение этой задачи возможно при наличии соответствующего методологического и математического обеспечения, моделирующего процессы, и, как правило, требует использования больших массивов текущей и архивной информации.

Одним из факторов, влияющих на оперативность и качество принимаемых решений, является форма представления информации. Очевидно, что для выработки решений на основе массивов разнотипных количественных и качественных значений показателей необходимо гораздо больше времени, чем в том случае, когда результаты представлены в виде диаграмм, графиков, отражающих существенные стороны процессов. Однако на подготовку данных к представлению также необходимы временные ресурсы.

Существенной особенностью АИС ОБЖ является сложная иерархическая структура

управляющего объекта, отдельные элементы которого взаимодействуют между собой как в ходе повседневной деятельности, так и при ликвидации чрезвычайной ситуации. В настоящий момент отсутствует однозначное разграничение полномочий между ними, уровень взаимодействия и координации недостаточен. Перечисленные факторы снижают эффективность принимаемых решений, приводят к неоправданному увеличению времени их принятия.

Таким образом, анализ информационных процессов показывает, что необходима их комплексная автоматизация. Только в этом случае лицу, принимающему решение, будет представлена оперативная, актуальная, достоверная и полная информация в удобном для него виде, обеспечена возможность оперативного управления действиями подчиненных сил и средств в масштабе времени, соответствующем сложившейся обстановке.

### 3.3. Функции АИС ОБЖ

Для эффективной поддержки принятия решений по обеспечению безопасности жизнедеятельности АИС ОБЖ должна обеспечить автоматизацию следующих функций:

3.3.1. Обеспечение исполнительных органов государственной власти Санкт-Петербурга, территориальных органов федеральных органов исполнительной власти и органов местного самоуправления в Санкт-Петербурге достоверной и актуальной информацией, представляемой информационными ресурсами, техническими системами, иными источниками данных.

#### 3.3.2. Мониторинг в реальном времени:

состояния объектов, обеспечивающих жизнедеятельность субъектов Российской Федерации, важнейших с точки зрения техногенных катастроф;

состояния предприятий и учреждений с особо опасными технологическими циклами;

перемещения и состояния транспортных средств, перевозящих по территории Санкт-Петербурга и Ленинградской области опасные и особо опасные грузы;

перемещения пассажирского транспорта;

перемещений и состояния сил и средств, обеспечивающих общественную безопасность в Санкт-Петербурге;

миграционной обстановки;

правонарушений, отслеживание деятельности сил и средств обеспечения безопасности от момента обнаружения правонарушения до окончания выполнения оперативных мероприятий;

видеоинформации об оперативной обстановке на вокзалах, в аэропортах, в акваториях, на общественно-политических, спортивных, праздничных и других массовых мероприятиях на городских объектах, улицах и площадях, местах скопления транспорта, во дворах жилых домов;

информации, публикуемой или транслируемой средствами массовой информации.

3.3.3. Автоматизированное определение типа события, характеризуемого принятым сигналом, сообщением, информацией о чрезвычайных, аварийных или нештатных ситуациях.

3.3.4. Накопление и хранение ретроспективных данных для последующего использования.

3.3.5. Анализ, прогнозирование, моделирование и другие типы интеллектуальной обработки данных.

3.3.6. Позиционирование событий и реакций на них с использованием геоинформационной

системы.

3.3.7. Предоставление возможности контролируемого доступа к информационным ресурсам АИС ОБЖ для исполнительных органов государственной власти Санкт-Петербурга, территориальных органов федеральных органов исполнительной власти, органов местного самоуправления в Санкт-Петербурге и прочих пользователей, в том числе для контроля деятельности подчиненных структур.

3.3.8. Предоставление пользователям АИС ОБЖ единого интерфейса управления информационными ресурсами и отображения информации.

3.3.9. Обеспечение единой централизованной аутентификации пользователей и поддержка иерархии доступа с системой приоритетов.

3.3.10. Ведение отчетности о действиях пользователей и состоянии системы в целом.

3.3.11. Функции обратной связи, такие как:

экстренное оповещение о чрезвычайных ситуациях на социальных объектах Санкт-Петербурга;

управление нарядами милиции общественной безопасности.

Функциональность АИС ОБЖ обеспечит информационную поддержку при решении задач безопасности жизнедеятельности.

Ввиду того, что АИС ОБЖ объединяет ресурсы разнородных территориально распределенных информационных и технологических систем с различной ведомственной и отраслевой принадлежностью, кроме вышеперечисленных в состав АИС ОБЖ также должны входить следующие функции:

обеспечение безопасности информации и защиты информационных ресурсов в АИС ОБЖ;

обеспечение целостности и непротиворечивости информации в АИС ОБЖ;

обеспечение электронного удостоверения информации (документов) и прав пользователя;

обеспечение централизованного управления доступом к ресурсам АИС ОБЖ.

#### 3.4. Принципы создания АИС ОБЖ

Основными принципами построения АИС ОБЖ являются:

сохранение существующих механизмов управления в исполнительных органах государственной власти Санкт-Петербурга, территориальных органах федеральных органов исполнительной власти, органах местного самоуправления в Санкт-Петербурге и службах Санкт-Петербурга;

учет и объединение на функциональной основе созданных и создаваемых информационных и технологических систем для решения задач в интересах обеспечения безопасности жизнедеятельности;

интеграция на системном (транспортном, сетевом, прикладном) и организационно-информационном уровнях;

развитие функциональных возможностей в части числа решаемых задач, типов и числа взаимодействующих информационных систем, адаптация к различным условиям применения;

обеспечение защиты информации на всех уровнях в соответствии с категорией информации;

этапность создания АИС ОБЖ;

комплексное финансирование создания и содержания АИС ОБЖ;

приоритетное использование отечественных разработок, особенно в части обеспечения информационной безопасности;

обеспечение высоких потребительских свойств и коммерческого потенциала информационных продуктов АИС ОБЖ.

#### 4. Архитектура и структура АИС ОБЖ

##### 4.1. Архитектура АИС ОБЖ

Под архитектурой АИС ОБЖ понимаются общие принципы и логическая организация информационного взаимодействия элементов АИС ОБЖ.

##### 4.1.1. Принципы технологического взаимодействия компонентов АИС ОБЖ

##### 4.1.1.1. Принцип многоуровневой интеграции

Транспортный уровень:

Построение АИС ОБЖ на базе мультисервисной транспортной сети с унифицированными транспортными протоколами.

В основу построения такой сети должны быть заложены следующие принципы:

обеспечение централизованного сетевого мониторинга и администрирования;

максимальное использование существующих волоконно-оптических и прочих коммуникаций и оборудования;

комплексность, унификация и совместимость реализуемых проектных, технических и технологических решений;

открытость архитектуры построения;

унификация программного и методического обеспечения;

обеспечение стандартных интерфейсов и протоколов;

резервирование каналов передачи информации;

обеспечение возможности разграничения доступа пользователей к различным сетевым ресурсам;

обеспечение возможности организации круглосуточного сервисного обслуживания оборудования;

возможность поэтапного создания и ввода АИС ОБЖ в эксплуатацию без нарушения функционирования существующих элементов.

Следование указанным принципам позволит создать Единую мультисервисную транспортную сеть (далее - ЕМТС).

Сетевой уровень:

Унификация протоколов обмена и форматов данных.

Уровень приложений:

Применение единого пользовательского интерфейса.

Применение стандартизованного интерфейса на основе WEB-технологий.

#### 4.1.1.2. Принцип интеграции на уровне данных

Интеграция на уровне данных - это принцип унификации интеграции систем АИС ОБЖ на уровне данных.

#### 4.1.1.3. Принцип "одного окна" для авторизации, аутентификации и генерации отчетов

Использование централизованной аутентификации, авторизации и отчетности позволит осуществлять эффективное администрирование и обеспечивать информационную безопасность АИС ОБЖ в части управления доступом.

#### 4.1.1.4. Принцип делегирования прав доступа к информации

Доступ к данным ведомственных (отраслевых) информационных систем внешних пользователей должен осуществляться на основе взаимных соглашений и общих регламентов (законодательных актов), в соответствии с которыми определяются права доступа для организаций и физических лиц.

#### 4.1.1.5. Принцип открытости системы

В архитектуре АИС ОБЖ должна использоваться эталонная модель взаимодействия открытых систем, что позволит обеспечивать информационное взаимодействие с вновь создаваемыми и внешними системами регионального и федерального уровня.

Межсистемные интерфейсы могут реализовываться на базе следующих существующих стандартов: стандарты UN/EDIFACT, разработанные Европейской экономической комиссией Организации Объединенных Наций и принятые в качестве международных стандартов; стандарты ISO серии 8613 "Обработка информации. Текстовые и учрежденческие системы. Архитектура, ориентированная на обработку учрежденческих документов (ODA), и формат обмена"; стандарты ISO серии 10021 "Информационная технология. Передача текстов. Системы обмена текстами в режиме сообщений (MOTIS)".

4.1.1.6. Принцип сопрягаемости с действующими или проектируемыми федеральными и региональными системами управления, мониторинга, учета и регистрации, архивными, новостными ресурсами

Сопряжение АИС ОБЖ с внешними ресурсами и системами необходимо для обмена информацией и интеграции в вышестоящие системы управления мониторинга, учета и регистрации для реального создания единого информационного пространства Российской Федерации.

#### 4.1.1.7. Принцип единства построения подсистемы защиты информации в АИС ОБЖ

Подсистема защиты информации в АИС ОБЖ основывается на положениях и требованиях

существующих законов, стандартов и нормативно-методических документов по защите от утраты, искажения и несанкционированного доступа к информации (далее - НСД).

Основными принципами построения подсистемы защиты от НСД являются:

- системность и комплексность;
- простота и гибкость реализации;
- разумная достаточность;
- непрерывность защиты;
- равнонадежность механизма защиты;
- независимость от секретности проектирования;
- управление правами пользователя;
- возможность контроля.

#### 4.1.2. Логическая организация информационного взаимодействия

АИС ОБЖ представляет собой совокупность локальных узлов (далее - ЛУ), являющихся пунктами концентрации информации, объединенных одним специальным видом ЛУ, реализующим ретрансляцию информационных потоков и являющимся центром управления доступом (далее - ЦУД). ЛУ могут представлять собой информационные системы, группы информационных систем, отдельные компоненты систем (база данных, клиент-приложение, сервер-приложение) или группы компонентов.

Пользователи системы (должностные лица, службы, специализированные центры) в соответствии с правами доступа получают информацию от ближайшего ЛУ либо через ЦУД от любого другого ЛУ, входящего в состав АИС ОБЖ. Средствами ЛУ обеспечивается единый пользовательский интерфейс в АИС ОБЖ. ЦУД обеспечивает единые маршрутизацию, авторизацию и аутентификацию на основе хранящейся в нем информации о пользователях и источниках.

Схема логической организации информационного взаимодействия представлена на рис. 3.

Рис. 3 Схема логической организации информационного взаимодействия

#### 4.2. Структура АИС ОБЖ

Структура АИС ОБЖ представлена на рис. 4.

Рис. 4 Структура АИС ОБЖ

##### 4.2.1. Функциональные элементы АИС ОБЖ

Основным фактором, определяющим состав элементов АИС ОБЖ и их взаимосвязь, является требуемая функциональность системы. В соответствии с перечнем необходимых функций, которые должна обеспечивать АИС ОБЖ для решения задач по обеспечению безопасности жизнедеятельности, в состав АИС ОБЖ должны входить следующие функциональные элементы:

4.2.1.1. Совокупность функциональных систем, являющихся для АИС ОБЖ первичными источниками информации:

системы, обеспечивающие мониторинг объектов и процессов (датчиковые системы, системы дистанционного зондирования, системы видеонаблюдения и т.д.);

системы приема информации от населения, системы экстренной связи;

информационные системы, в том числе содержащие эталонные данные (кадастры, регистры, реестры, справочники, классификаторы и т.д.).

4.2.1.2. Расчетно-аналитические системы, обеспечивающие обработку информации по заданным алгоритмам.

4.2.1.3. Система управления доступом, обеспечивающая централизованное назначение пользовательских прав по использованию информационных ресурсов АИС ОБЖ.

4.2.1.4. Система обеспечения информационной безопасности, выполняющая требования нормативных и законодательных актов Российской Федерации в области защиты конфиденциальной информации при ее автоматизированной обработке и передаче по каналам связи.

4.2.1.5. Интеграционные системы:

ЕМТС, объединяющая элементы АИС ОБЖ в единое информационное пространство и обеспечивающая пользователям полноту доступа (в рамках предоставленных прав) ко всей информации;

модули взаимодействия, реализующие клиент-серверные технологии взаимодействия элементов АИС ОБЖ и единый пользовательский интерфейс;

базы метаданных об источниках информации.

4.2.1.6. Терминальное оборудование, обеспечивающее прием, заданное представление и отображение информации (автоматизированное рабочее место (далее - АРМ), оборудование отображения коллективного пользования, средства документирования).

4.2.2. Территориально распределенные элементы АИС ОБЖ

Перечисленные в [пункте 4.2.1](#) настоящей Концепции элементы АИС ОБЖ могут иметь территориально распределенный характер. Примером такого построения может служить ЕМТС, выполняющая задачу информационного объединения всех составляющих АИС ОБЖ. Особенностью этой сети является обеспечение передачи разнородной информации (видеоизображение, звук, данные информационных систем) и предоставление пользователям широкого спектра телекоммуникационных услуг. Основу ЕМТС составляют волоконно-оптические сети, связывающие между собой подсистемы АИС ОБЖ с исполнительными органами государственной власти Санкт-Петербурга, территориальными органами федеральных органов исполнительной власти, органами местного самоуправления в Санкт-Петербурге, органами министерств и ведомств, бюджетными учреждениями Санкт-Петербурга. Сети должны обеспечить потенциально полноту доступа информационное взаимодействие всех элементов АИС ОБЖ, минимальную удельную стоимость единицы трафика, высокоскоростную качественную цифровую связь, в том числе передачу мультимедийной информации в режиме реального времени. Для решения частных задач в ЕМТС могут использоваться ведомственные и государственные линии магистральной связи, а также каналы, предоставляемые различными операторами связи, в том числе каналы телефонной сети Санкт-Петербурга, прямые каналы радиорелейной связи. Для обеспечения взаимодействия и доведения управленческой информации до исполнительных органов государственной власти Санкт-Петербурга, территориальных органов федеральных органов исполнительной власти и органов местного самоуправления в Санкт-Петербурге могут использоваться каналы радиосвязи и транкинговой связи.

#### 4.2.3. Компактно размещенные узлы АИС ОБЖ

В ряде случаев территориально распределенные составные части элементов АИС ОБЖ могут объединяться в компактно размещенные узлы.

Примерами подобной организации являются ЦУД, ЛУ, ситуационные центры.

ЛУ представляют собой аппаратно-программные комплексы, обеспечивающие какую-либо линейную комбинацию следующих функциональностей: сбор, хранение, обработка или предоставление информации пользователям.

При создании ЛУ могут учитываться отраслевая (ведомственная) принадлежность и тип источников информации, их территориальное размещение, экономическая целесообразность и т.д. Так, например, ЛУ могут быть реализованы на базе одной или нескольких территориально разнесенных однородных информационных систем. В качестве альтернативного может рассматриваться вариант создания в рамках одного ведомства ЛУ, объединяющего несколько разнородных систем. Общее количество ЛУ не имеет значения для АИС ОБЖ. Действительно, АИС ОБЖ должна позволять увеличение количества ЛУ в любое время без ограничения их числа, например, в случае необходимости развертывания мобильных, оперативных, специальных и других типов ЛУ.

Следует отметить, что пользователями информационных ресурсов ЛУ могут быть не только внешние клиенты, подключенные через ЦУД, но и клиенты, подключенные непосредственно к ЛУ. В этом случае функциональность ЛУ должна повышаться. Фактически ЛУ может выполнять функции ЦУД, касающиеся управления пользователями.

В общем случае ЛУ является полноценным, законченным программно-аппаратным решением, способным функционировать в условиях отсутствия связи с другими компонентами АИС ОБЖ.

Программно-аппаратная реализация ЛУ строится по модульному принципу и обеспечивает высокую масштабируемость. Модульность реализации обусловлена необходимостью использования различных устройств сопряжения и преобразования интерфейсов. Выбор необходимых модулей определяется в зависимости от конкретных требований и уже имеющихся в ЛУ программно-аппаратных средств.

Доступ к ресурсам ЛУ является многопользовательским. В ситуациях, связанных с невозможностью реализации многопользовательского доступа, реализуется механизм разграничения доступа на основе пользовательских приоритетов. Пользователь с более высоким приоритетом получает эксклюзивные права на доступ к ресурсу во время работы с ним.

Для качественного информационного сопровождения, синхронизации взаимодействия со всеми входящими в систему ЛУ, решения задач информационной безопасности организуется ЦУД АИС ОБЖ, в задачи которого входят:

управление пользователями;

разграничение прав доступа к информационным ресурсам и функциональным подсистемам;

предоставление пользователям информации из различных ресурсов, а также прав пользования компонентами соответствующей системы на основе единого пользовательского интерфейса.

Назначением ЦУД является интеграция всех информационных потоков, поступающих из ЛУ и предоставление их пользователям АИС ОБЖ в соответствии с правами доступа. ЦУД является

основной компонентой системы и предназначен для накопления информации о пользователях и источниках системы и ретрансляции потоков от ЛУ к пользователям АИС ОБЖ. ЦУД должен обеспечивать возможность автоматизированного управления информационной средой АИС ОБЖ и распределения различного рода информационных потоков, поступающих из ЛУ.

В целях распределения нагрузки аппаратно-технические средства ЦУД могут быть территориально распределены, при этом оставаясь составной частью АИС ОБЖ.

Каждое обращение внешнего пользователя к тому или иному ЛУ сопровождается подтверждением ранее выданных ключей временного срока действия на предмет аутентификации соединяющихся сторон. При этом под сторонами следует понимать именно коммуникационное оборудование, например, персональная электронно-вычислительная машина пользователя, с одной стороны, и один из пользовательских интерфейсов ЦУД - с другой.

Процесс выдачи, замены и продления полномочий электронных ключей доступа в АИС ОБЖ осуществляет ЦУД. Таким образом, участники АИС ОБЖ образуют приватную сеть передачи данных с асимметричным алгоритмом шифрования, базирующемся на использовании пар открытых и закрытых ключей, что открывает широкие возможности подключения пользователей с минимизированным ущербом для информационной безопасности.

Для разграничения прав доступа и контроля над использованием ресурсов АИС ОБЖ в рамках информационного пространства создается система единой аутентификации непосредственно пользователей и авторизации их с учетом иерархических приоритетов, а также ведения отчетности по использованию информационных ресурсов АИС ОБЖ.

Система единой аутентификации, авторизации и отчетности позволяет:

осуществлять аутентификацию пользователей системы;

осуществлять авторизацию пользователей с учетом иерархических приоритетов;

подключать к ресурсам системы новых пользователей по заранее установленному регламенту и изменять права доступа существующих, в том числе формировать группы с одинаковыми правами доступа;

получить отчет о работе пользователей и использовании ресурсов АИС ОБЖ.

Для получения доступа к информационным ресурсам ЛУ и другим источникам информации через единый интерфейс ЦУД АИС ОБЖ пользователь должен иметь соответствующие личные или групповые права доступа, установленные для него политикой доступа к ресурсам.

Ситуационные центры представляют собой организационно-техническое объединение компактно размещенных технических подсистем и рабочих мест для высших должностных лиц и экспертов, предназначенное для обеспечения поддержки принятия решений руководством и специалистами исполнительных органов государственной власти Санкт-Петербурга, территориальных органов федеральных органов исполнительной власти и органов местного самоуправления в Санкт-Петербурге в повседневной деятельности и в условиях чрезвычайных ситуаций.

В рамках терминологии АИС ОБЖ ситуационный центр представляет собой пример ЛУ. Основное отличие ситуационного центра от традиционных систем автоматизации управления состоит в предоставлении возможности просчитывать и анализировать последствия любых управленческих решений.

Аппаратно-программный комплекс ситуационного центра должен обеспечивать:

непосредственный доступ руководства и экспертов к достоверной информации из ресурсов АИС ОБЖ и внешних информационных систем;

вывод информации на средства отображения коллективного пользования;

наглядное и рациональное представление многоаспектной информации, включая представление оперативной информации в реальном масштабе времени;

прогнозирование развития ситуации на основе анализа поступающей информации;

моделирование последствий управленческих решений;

экспертную оценку принимаемых решений и их оптимизацию;

информационную и технологическую поддержку проведения совещаний, коллегий с использованием современных методик коллективной работы, протоколирования проводимых мероприятий.

На первых этапах создания АИС ОБЖ предполагается создание городского ситуационного центра, в дальнейшем - создание ситуационных центров для районов Санкт-Петербурга.

Состав ситуационного центра может варьироваться в зависимости от его места в системе управления Санкт-Петербургом.

В общем случае в его состав могут входить:

расчетно-аналитическая система;

терминальное оборудование, обеспечивающее прием, заданное представление и отображение информации (АРМы, оборудование отображения коллективного пользования, средства документирования);

средства организации и проведения совещаний (средства конференц-связи, аудиосистемы, средства совместной работы над документами);

средства звукозаписи, видеозаписи;

телекоммуникационные средства, обеспечивающие доступ к телекоммуникационной сети и информационным ресурсам АИС ОБЖ и внешним источникам информации;

технологические средства обеспечения деятельности функциональных систем и персонала ситуационного центра (специализированное коммутационное оборудование, системы энергообеспечения, кондиционирования, освещения и т.д.).

#### 4.3. Выделенные ресурсы АИС ОБЖ

В настоящее время в банках, гостиницах, аэропортах, супермаркетах, обменных пунктах и на других объектах уже созданы или создаются локальные системы наблюдения и контроля обстановки в помещениях и на прилегающих территориях. Во многих отраслях в целях совершенствования управления имеются разного рода информационные системы и автоматизированные системы управления.

Таким образом, локальные системы безопасности, обеспечившие технологический доступ к своим ресурсам для АИС ОБЖ, могут рассматриваться как составные части АИС ОБЖ. Следовательно, для вновь создаваемых отраслевых локальных систем безопасности АИС ОБЖ может выделять часть объединенных ресурсов. Прежде всего речь идет о ресурсах телекоммуникационных сетей, систем мониторинга объектов, систем видеонаблюдения,

информационных систем.

Такой подход позволит заинтересованной в локальной системе стороне минимизировать сроки реализации и затраты на ее создание. Данное положение подтверждается опытом создания в Санкт-Петербурге в 2004 году системы безопасности отрасли связи и системы безопасности учреждений образования, использующих выделенные ресурсы телекоммуникационных сетей и системы мониторинга стационарных и мобильных объектов.

## 5. Обеспечение информационной безопасности в АИС ОБЖ

В соответствии с [пунктом 4.1.1.7](#) настоящей Концепции подсистема защиты информации в АИС ОБЖ основывается на следующих принципах:

### 5.1. Принцип системности и комплексности

Принцип системности подразумевает необходимость учета всех факторов, влияющих на защищенность АИС ОБЖ, при проектировании, разработке, внедрении и эксплуатации АИС ОБЖ.

Комплексность системы защиты подразумевает сочетание и согласованное использование организационных мер и инженерно-технических (в том числе программных и аппаратных) средств в рамках единой системы защиты.

### 5.2. Принцип простоты и гибкости реализации

Принцип простоты реализации означает, что используемые меры и средства защиты должны быть понятны и просты в использовании. Существование системы защиты не должно, по возможности, затруднять работу пользователей АИС ОБЖ.

Гибкость системы защиты означает предпочтительное использование мер и средств защиты, обеспечивающих широкие возможности по настройке и совместимости с используемым программным обеспечением АИС ОБЖ.

В целом данный принцип означает, что система защиты не должна существенно ухудшать основные функциональные характеристики АИС ОБЖ (надежность, быстродействие, возможность изменения конфигурации).

### 5.3. Принцип разумной достаточности

Практика эксплуатации зарубежных и отечественных автоматизированных систем показывает, что создать абсолютно непреодолимую систему защиты невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту. Кроме того, создание и поддержание в рабочем состоянии системы защиты требует затрат людских и технических ресурсов (как правило, тем больших, чем выше обеспечиваемая надежность).

Таким образом, необходимо выбирать уровень защиты, оптимизирующий соотношение риска, размера возможного ущерба и требуемых затрат.

### 5.4. Принцип непрерывности защиты

Защита информации должна обеспечиваться на всех этапах проектирования, разработки, внедрения и эксплуатации АИС ОБЖ. Защита информации должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Развитие системы защиты должно вестись параллельно с развитием АИС ОБЖ.

Действительно, развитие компонентов АИС ОБЖ должно в обязательном порядке сопровождаться мероприятиями по поддержанию требуемого уровня защищенности.

#### 5.5. Принцип равнонадежности механизма защиты

Различные каналы НСД, реализуемые с примерно равной вероятностью и приводящие к примерно равному ущербу, должны перекрываться с одинаковой степенью надежности.

Принцип подразумевает дифференциацию требований к надежности защиты в зависимости от величины возможного ущерба и вероятности его нанесения.

#### 5.6. Принцип независимости от секретности проектирования

Поскольку задачу сокрытия деталей реализации системы защиты, предназначенной для эксплуатации в течение продолжительного периода времени, нельзя считать стопроцентно выполнимой, механизм защиты должен быть эффективен даже в том случае, когда его структура и принципы функционирования становятся известными.

Данный принцип, однако, не означает, что информация о системе защиты АИС ОБЖ должна быть общедоступна.

#### 5.7. Принцип управления правами пользователей

Каждому сотруднику из числа пользователей, обслуживающего и эксплуатирующего персонала АИС ОБЖ должен предоставляться наименьший набор полномочий по доступу к информации и процедурам ее обработки. В то же время эти полномочия должны быть достаточными для успешного выполнения сотрудниками своих служебных обязанностей.

#### 5.8. Принцип возможности контроля

Данный принцип утверждает, с одной стороны, необходимость создания специальных средств и методов, направленных на предотвращение попыток несанкционированного вмешательства в работу механизмов защиты, и, с другой стороны, необходимость разработки мероприятий по проверке работоспособности и корректности этого механизма.

### 6. Нормативные правовые и организационные аспекты создания АИС ОБЖ

#### 6.1. Правовое обеспечение создания АИС ОБЖ

Правовое обеспечение создания АИС ОБЖ должно базироваться на правовых актах, регламентирующих информатизацию субъекта Российской Федерации.

Существующие в настоящее время правовые акты регламентируют только отдельные вопросы информатизации и не предусматривают возможность передачи внутриведомственной информации, необходимой для формирования информационных ресурсов АИС ОБЖ. В этой связи для реализации функций АИС ОБЖ в полном объеме необходимо привести в соответствие действующее законодательство в сфере информационного взаимодействия исполнительных органов государственной власти Санкт-Петербурга, территориальных органов федеральных органов исполнительной власти и органов местного самоуправления в Санкт-Петербурге.

#### 6.2. Сертификация, стандартизация продукции и лицензирование деятельности при создании АИС ОБЖ

##### 6.2.1. Сертификация и стандартизация

Функциональные компоненты АИС ОБЖ, как и большинство автоматизированных систем управления, автоматизированных информационных систем и информационных систем органов государственной власти, сертифицируются в соответствии с действующим законодательством Российской Федерации.

Целями стандартизации применительно к АИС ОБЖ являются обеспечение научно-технического прогресса, повышение конкурентоспособности продукции (работ, услуг), техническая и информационная совместимость. К нормативным документам в области стандартизации относятся базовые и функциональные стандарты (профили).

Стандарты в сфере создания АИС ОБЖ должны определять общую архитектуру АИС ОБЖ, порядок ее создания, основные функции, порядок интеграции и обеспечения информационного взаимодействия с государственными информационными системами федерального значения.

Стандартизация продукции должна осуществляться в соответствии с Федеральным [законом](#) "О техническом регулировании", ГОСТами и отраслевыми руководящими документами.

#### 6.2.2. Лицензирование деятельности

К лицензируемым видам деятельности при создании АИС ОБЖ относятся виды деятельности, осуществление которых может повлечь за собой нанесение ущерба правам, законным интересам, здоровью граждан, обороне и безопасности государства, культурному наследию народов Российской Федерации и регулирование которых не может осуществляться иными методами, кроме как лицензированием.

При создании АИС ОБЖ лицензированию, в соответствии с Федеральным [законом](#) "О лицензировании отдельных видов деятельности", подлежат:

деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;

деятельность по разработке и(или) производству средств защиты конфиденциальной информации;

деятельность по технической защите конфиденциальной информации.

Организации, участвующие в выполнении вышеуказанных видов деятельности при создании АИС ОБЖ, должны иметь соответствующие лицензии.

Подлежит обязательному лицензированию деятельность негосударственных организаций и частных лиц, связанная с обработкой и предоставлением персональных данных.

Абзац утратил силу. - [Постановление](#) Правительства Санкт-Петербурга от 29.06.2007 N 716.

#### 6.3. Организационные меры и этапы создания АИС ОБЖ

Комитет по информатизации и связи осуществляет функции заказчика АИС ОБЖ и обеспечивает подготовку и проведение конкурсов, заключение контрактов и координацию выполнения мероприятий по созданию АИС ОБЖ, рассмотрение, согласование и утверждение технических заданий и проектно-сметной документации на реализацию отдельных элементов АИС ОБЖ и принимает решения о сдаче-приемке результатов.

(в ред. Постановлений Правительства Санкт-Петербурга от 30.03.2011 [N 381](#), от 12.05.2012 [N 453](#))

Комитет по информатизации и связи назначает подведомственную государственную организацию генеральным конструктором АИС ОБЖ, которая отвечает за:  
(в ред. Постановлений Правительства Санкт-Петербурга от 30.03.2011 N 381, от 12.05.2012 N 453)

разработку регламентов и правил межведомственного и межсистемного взаимодействия;

разработку и внедрение в отраслевых системах единых информационных и телекоммуникационных стандартов;

поддержание системного взаимодействия с информационными проектами федерального уровня;

создание и эксплуатацию подсистем АИС ОБЖ;

контроль качества исполнения.

При создании АИС ОБЖ используется ГОСТ 34.601-90, который имеет следующие этапы разработки:

формирование требований к АИС ОБЖ;

разработка концепции;

разработка технического задания;

разработка эскизного проекта;

разработка технического проекта;

разработка рабочей документации;

опытная эксплуатация;

промышленная эксплуатация.

С учетом изложенных выше факторов представляется целесообразным следующий порядок разработки и внедрения АИС ОБЖ:

выполнение работ по ранним стадиям создания автоматизированных систем (исследования, концептуальное обоснование, эскизное и техническое проектирование) с учетом особенностей уже действующих элементов АИС ОБЖ;

разработка стандартов в области обмена между элементами АИС ОБЖ данными различной структуры: видео, аудио, текстовые и т.п.;

внедрение вновь создаваемых компонентов и узлов АИС ОБЖ в соответствии с документами, указанными в пункте 1.2 настоящей Концепции;

развитие и наращивание существующих элементов АИС ОБЖ в соответствии с документами, указанными в пункте 1.2 настоящей Концепции.

Такой подход к разработке АИС ОБЖ позволит органично объединить существующий технический потенциал и минимизировать затраты на реализацию новых систем, входящих в АИС ОБЖ.

7. Ожидаемый эффект от внедрения АИС ОБЖ

Планируется следующий эффект от использования АИС ОБЖ:

повышение уровня безопасности жизнедеятельности и объектов инфраструктуры Санкт-Петербурга;

стабильное социально-экономическое развитие Санкт-Петербурга;

повышение качества жизни населения Санкт-Петербурга;

повышение эффективности контроля за объектами инфраструктуры Санкт-Петербурга и населением;

повышение эффективности решения задач территориальными подразделениями силовых структур;

недопущение и предотвращение чрезвычайных ситуаций техногенного характера;

повышение эффективности мероприятий по ликвидации последствий природных и техногенных катастроф;

обеспечение развития российских передовых технологий.

Количественную оценку эффекта от внедрения АИС ОБЖ можно сделать лишь на стадии проектирования, однако уже сегодня имеются сведения об эффекте, который получен от внедрения автоматизированных информационных и технологических систем, которые в перспективе могут войти в состав АИС ОБЖ.

Так, внедрение только одной составляющей АИС ОБЖ, а именно системы передачи информации о группировке сил и средств в режиме реального времени непосредственно в районные отделы внутренних дел, значительно повысило эффективность оперативного реагирования на тревожные сигналы с объектов. Например, время доведения сигнала об изменении состояния контролируемого объекта до групп задержания сократилось на 25-40 процентов, время прибытия групп задержания на объекты после оповещения сократилось на 25-50 процентов. Кроме того, отмечается повышение организованности и дисциплины личного состава нарядов при выполнении служебных обязанностей по патрулированию, практическое отсутствие случаев отклонения от заданных маршрутов патрулирования.

При оценке эффективности ЕМТС органов государственной власти Санкт-Петербурга, которая может стать составляющей транспортной сети АИС ОБЖ, были получены следующие результаты:

При завершении строительства в 2005 году ЕМТС исполнительных органов государственной власти Санкт-Петербурга объединит в единую сеть все органы государственной власти Санкт-Петербурга. При этом они получат возможность пользоваться услугами качественной связи и широким спектром услуг современных информационных технологий. Проект окупится в течение четырех последующих лет.

ПРИЛОЖЕНИЕ 2  
к постановлению  
Правительства Санкт-Петербурга  
от 04.10.2005 N 1505

**ПЛАН**

**МЕРОПРИЯТИЙ НА 2005-2006 ГОДЫ ПО РЕАЛИЗАЦИИ КОНЦЕПЦИИ  
АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ  
БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ САНКТ-ПЕТЕРБУРГА**

N п/п	Наименование мероприятий	Срок исполнения	Ответственные исполнители
1	2	3	4
1. Проведение исследовательских работ и мероприятий			
1.1	Обобщение опыта внедрения компонентов и подсистем АИС ОБЖ в других регионах Российской Федерации, а также зарубежного опыта	IV квартал 2005 г.	КИС
1.2	Определение функциональных возможностей интеграции городских и ведомственных систем в рамках АИС ОБЖ	IV квартал 2005 г.	КИС
1.3	Выявление информационных потребностей субъектов взаимодействия в рамках АИС ОБЖ	IV квартал 2005 г.	КИС
1.4	Формирование перечня городских объектов, подлежащих техническому оснащению и включению в состав АИС ОБЖ	IV квартал 2005 г.	КИС, КЗПБ
1.5	Выработка рекомендаций по разработке стандартов и регламентов межведомственного и межсистемного информационного взаимодействия	IV квартал 2005 г.	КИС

КонсультантПлюс: примечание.

Временный перечень стандартов проживания в Санкт-Петербурге на 2005-2008 годы, утвержденный постановлением Правительства Санкт-Петербурга от 19.04.2005 N 474, утратил силу в связи с изданием [постановления](#) Правительства Санкт-Петербурга от 29.08.2006 N 1051, утвердившего [Перечень](#) стандартов проживания в Санкт-Петербурге на 2006-2008 годы.

2. Разработка и утверждение регламентов и стандартов для АИС ОБЖ			
2.1	Корректировка отраслевого стандарта проживания в Санкт-Петербурге "Обеспечение личной и общественной безопасности" в соответствии с <a href="#">постановлением</a> Правительства Санкт-Петербурга от 19.04.2005 N 474 "О Программе социально-экономического развития Санкт-Петербурга на 2005-2008 годы"	IV квартал 2005 г.	КЗПБ, КИС
2.2	Корректировка стандарта общественной эффективности отрасли в соответствии с <a href="#">постановлением</a> Правительства Санкт-Петербурга	IV квартал 2005 г.	КЗПБ, КИС

	от 19.04.2005 N 474 "О Программе социально-экономического развития Санкт-Петербурга на 2005-2006 годы"		
2.3	Корректировка инфраструктурного стандарта в соответствии с постановлением Правительства Санкт-Петербурга от 19.04.2005 N 474 "О Программе социально-экономического развития Санкт-Петербурга на 2005-2008 годы"	IV квартал 2005 г.	КЗПБ, КИС
2.4	Разработка стандарта качества в соответствии с постановлением Правительства Санкт-Петербурга от 19.04.2005 N 474 "О Программе социально-экономического развития Санкт-Петербурга на 2005-2008 годы"	IV квартал 2005 г.	КЗПБ, КИС
2.5	Разработка и утверждение проектов межведомственных регламентов взаимодействия в сфере инфокоммуникационных технологий (в том числе инфокоммуникационных систем, видеосистем, автоматизированных систем управления и мониторинга, систем управления доступом и др.)	IV квартал 2005 г. - I квартал 2006 г.	КИС, КЗПБ
2.6	Разработка и утверждение проектов стандартов межсистемного взаимодействия в сфере инфокоммуникационных технологий (в том числе инфокоммуникационных систем, видеосистем, автоматизированных систем управления и мониторинга, систем управления доступом и др.)	IV квартал 2005 г. - I квартал 2006 г.	КИС, КЗПБ
2.7	Формирование и представление в Комитет экономического развития, промышленной политики и торговли предложений по реализации постановления Правительства Санкт-Петербурга от 19.04.2005 N 474 "О Программе социально-экономического развития Санкт-Петербурга на 2005-2008 годы"	IV квартал 2005 г.	КИС, КЗПБ
3. Проектирование, разработка и внедрение базовых компонентов АИС ОБЖ			
3.1	Проектирование центра управления доступом	IV квартал 2005 г.	КИС
3.2	Проектирование системы защиты информации	IV квартал 2005 г.	КИС
3.3	Технологическое обновление существующих элементов системы	IV квартал 2005 г.	КИС

	защиты информации		
3.4	Проектирование, разработка и внедрение удостоверяющего центра городского уровня	IV квартал 2005 г.	КИС
3.5	Проектирование, разработка и внедрение макета межведомственной системы видеонаблюдения	IV квартал 2005 г.	КИС, ГУВД (по согласованию)
3.6	Разработка, внедрение центра управления доступом	I-IV кварталы 2006 г.	КИС
3.7	Создание и внедрение системы защиты информации	I-IV кварталы 2006 г.	КИС
3.8	Развитие Единой мультисервисной телекоммуникационной сети в рамках реализации АИС ОБЖ	I-IV кварталы 2006 г.	КИС
3.9	Создание ситуационного центра Санкт-Петербурга	I-IV кварталы 2006 г.	КИС, ГУВД (по согласованию)
3.9.1	Проектирование, создание и внедрение Центра управления нарядами милиции общественной безопасности ГУВД в рамках локального узла системы мониторинга объектов	IV квартал 2005 г. - II квартал 2006 г.	КИС, ГУВД (по согласованию)
3.9.2	Проектирование ситуационного центра Санкт-Петербурга	I квартал 2006 г.	КИС, ГУВД (по согласованию)
3.9.3	Построение базовой инфраструктуры ситуационного центра Санкт-Петербурга	I-II кварталы 2006 г.	КИС, ГУВД (по согласованию)
3.9.4	Организация оперативной селекторной связи и системы оперативного управления	I-IV кварталы 2006 г.	КИС, ГУВД (по согласованию)
3.10	Создание типовых локальных узлов видеомониторинга, центра мониторинга объектов, систем информационного обеспечения	I-IV кварталы 2006 г.	КИС, ГУВД (по согласованию)
3.11	Разработка и создание информационных сервисов для внешних пользователей, а также автоматизированных рабочих мест должностных лиц	I-IV кварталы 2006 г.	КИС
4. Интеграция существующих систем в рамках АИС ОБЖ			
4.1	Внедрение межведомственной системы видеонаблюдения на выбранной территории	I-III кварталы 2006 г.	КИС
4.2	Организация взаимодействия с информационными системами ГУВД	I-IV кварталы	КИС, ГУВД (по

		2006 г.	согласованию)
4.3	Организация взаимодействия с информационными системами администраций районов Санкт-Петербурга	I-IV кварталы 2006 г.	КИС, ГУВД (по согласованию), администрации районов Санкт-Петербурга
4.4	Организация взаимодействия с информационными системами органов государственной власти Санкт-Петербурга	I-IV кварталы 2006 г.	КИС

АИС ОБЖ - автоматизированная информационная система обеспечения безопасности жизнедеятельности Санкт-Петербурга

ГУВД - Главное управление внутренних дел Санкт-Петербурга и Ленинградской области

КЗПБ - Комитет по вопросам законности, правопорядка и безопасности

КИС - Комитет по информатизации и связи

---