УДК 004.9 + 353.5

В.М. Клецов
([1]Академия ГПС МЧС России, [2]Префектура Западного административного округа г. Москвы;
e-mail: sednev70@yandex.ru)

ПУТИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДОЛЖНОСТНЫХ ЛИЦ ТЕРРИТОРИАЛЬНЫХ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

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

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

V.M. Kletsov

WAYS TO IMPROVE THE EFFICIENCY OF DECISION SUPPORT OFFICIALS TERRITORIAL EXECUTIVE AUTHORITIES

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

Key words: territorial executive authorities, decision support, hardware and software platform.

Специфика деятельности ***территориальных органов исполнительной власти (ТОИВ)***, характер их взаимодействия с другими органами исполнительной власти, населением и хозяйствующими субъектами обуславливает разнородность решаемых задач, выполняемых функций и сложность обрабатываемой информации. К одним из основных задач ТОИВ относятся: создание территориального звена городской территориальной подсистемы ***Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС)***; координация деятельности и взаимодействия с территориальными органами федеральных органов государственной власти по проблемам обеспечения комплексной безопасности и др. При этом основными приоритетами Российской Федерации на период до 2020 г. являются создание и дальнейшее развитие информационного общества и совершенствование системы государственного управления на основе внедрения новейших ***информационно-коммуникационных технологий (ИКТ)***. Государственное регулирование в сфере применения ***информационных технологий (ИТ)*** предусматривает регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации.

Например, основным назначением информатизации задач управления ***административного округа (АО)*** Москвы является обеспечение ТОИВ оперативной, аналитической и прогнозной информацией для поддержки принятия решений в сфере управления округом и районом. В направлении информатизации управления АО можно выделить развитие средств совместной работы ***должностных лиц (ДЛ)*** ТОИВ на основе ***информационного ресурса (ИР)*** округа.

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

Проведенный анализ показал: при создании ИС не решаются вопросы интеграции, стандартизации, унификации и обеспечения совместимости информации, отсутствуют механизмы контроля за использованием ИР, обеспечением их полноты и достоверности; требуется создание эффективного механизма эксплуатации имеющихся ИС и ресурсов, при этом ряд ИС не соответствует требованиям по полноте, доступности, целостности и конфиденциальности имеющейся в них информации, а держатели ИР часто не заинтересованы в том, чтобы их ***базы данных (БД)*** могли использоваться другими подразделениями или хозяйствующими субъектами; в отраслевых и ведомственных системах не учитываются потребности округов, за исключением возможностей просмотра информации и получения некоторых форм отчётности, а округа при решении задач информатизации пытаются эти задачи решать самостоятельно, не опираясь на общегородские проекты.

Анализ ПО и ИТ, применяемых ДЛ ТОИВ, позволил выявить типовые элементы инфраструктуры ИТ: системное ПО основано на решениях Microsoft, как правило, имеется сервер для хранения неструктурированной информации; используются антивирусное ПО, прикладные системы (документооборота, электронной почты, бухгалтерского и кадрового учёта, геоинформационные); инженерная инфраструктура серверных помещений, телекоммуникационная инфраструктура.

В связи с необходимостью развития территориального звена Московской городской территориальной подсистемы РСЧС и для повышения эффективности управления территориями АО, на которых сосредоточены огромные социальные и материальные ресурсы, требуется разработка ***программно-аппаратной платформы (ПАП)***, позволяющей руководителю ТОИВ получать необхо-

димую информацию из прикладных программ, которые функционируют независимо и являются специфичными для каждой сферы деятельности подразделений префектуры, подведомственных организаций и учреждений.

Создание ПАП предполагает реализацию принципов системности (целостность отдельных систем и взаимодействие с другими системами); открытости (расширение функций); совместимости (взаимодействие с другими системами); стандартизации (применение типовых элементов).

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

Рис. 1. Требования к программно-аппаратной платформе

Основные требования к ПАП:

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

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

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

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

Требования к функциям (задачам) следующих подсистем:

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

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

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

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

Основные требования к видам обеспечения:

- информационное обеспечение должно быть реализовано в виде комплексов информационных средств и обеспечивать полноту отображения предметной области, многократное использование данных при однократном вводе; информационную совместимость между частями системы; разграничение доступа к данным в соответствии с обязанностями ДЛ; используемые ***системы управления базами данных (СУБД)*** должны иметь интерфейсы с языками программирования высокого уровня;

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

- техническое обеспечение должно включать средства сбора, обработки и отображения информации; средства обмена информацией между АРМ ДЛ; средства связи и обмена данными с взаимодействующими объектами; аппаратно-программные ***средства защиты информации (СЗИ)***; необходимые контрольно-измерительные приборы;

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

управления данными, расчётные и графические модули, позволяющей реализовать модульность построения системы, использовать открытые промышленные стандарты, обеспечивающие интеграцию различных АС, и системный подход к деятельности ТОИВ.

Конечной целью создания ПАП является повышение эффективности деятельности ТОИВ и качества принимаемых его ДЛ управленческих решений. На её основе обеспечивается информационно-аналитическая поддержка процессов анализа, моделирования и прогнозирования развития ситуации и выработки эффективных решений по направлениям деятельности ТОИВ.

Архитектура ПАП включает в себя: IBM-совместимый компьютер; операционную систему семейства Windows, MS Office 2003, 2007, Visual Studio 2010, Mathcad 14, Adobe Flash CS3; базу данных (рис. 2), состоящую из трёх функциональных модулей (СУБД, коррекции, банка данных) и четырёх программных генераторов (стохастизма, транзактов, динамики, расчётно-графического).

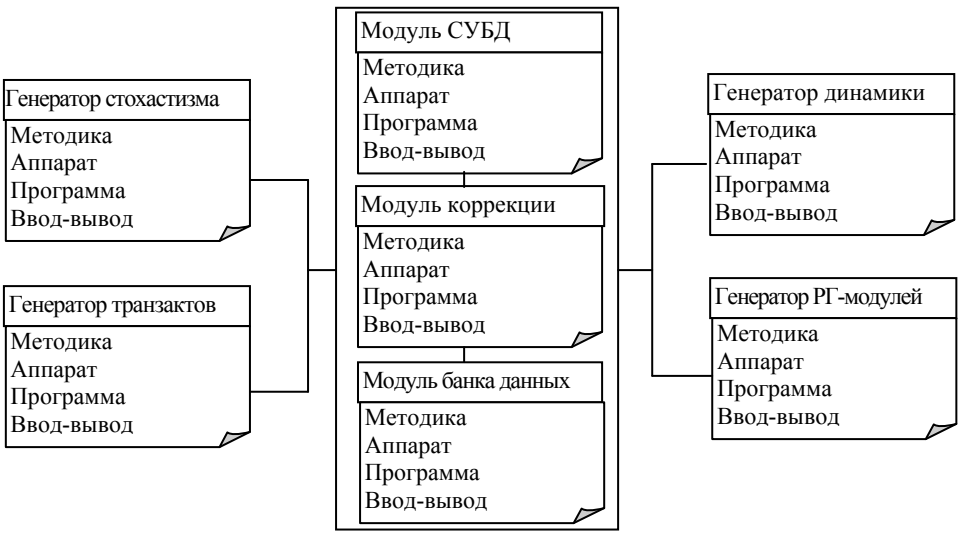

Рис. 2. Структура базы данных

Модуль коррекции БД предназначен для реализации динамических обратных связей, изменяющих банк данных (рис. 3). Функционирование модуля обеспечивается программными генераторами [1] стохастизма, транзактов, динамики, расчётно-графическим. Генераторы являются посредниками между БД и виртуальной оболочкой платформы и расчётно-графическими модулями и обеспечивают: стохастизма – реализацию случайных процессов, приводящих к изменению БД; транзактов – функции источника и поглотителя событий, требующих коррекции БД; динамики – устойчивость вектора модельного времени; расчётно-графический – связь БД с расчётно-графическими модулями платформы.

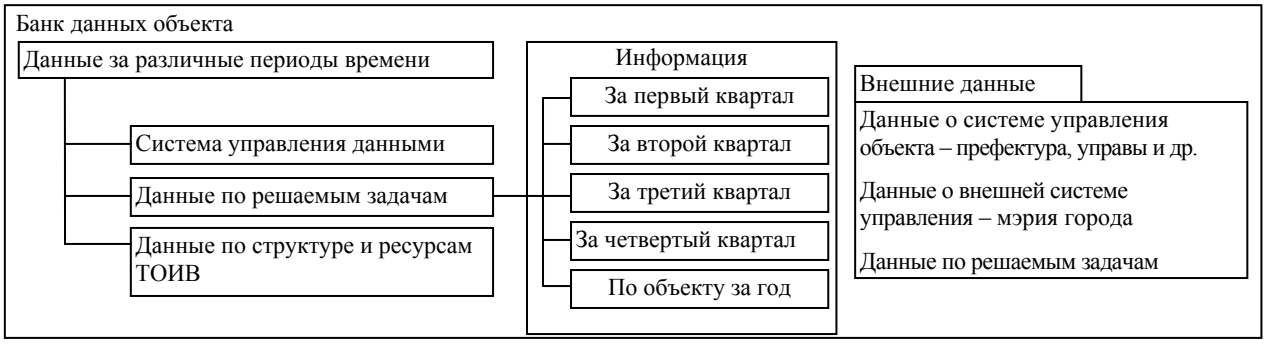

Рис. 3. Состав банка данных

Банк данных должен включать структурированную, иерархически построенную, именованную совокупность данных ТОИВ, состоящих из внутренней и внешней частей: внутренняя формируется из системы управления и данных по задачам и структуре объекта; внешняя должна содержать динамическую информацию о системе управления префектуры и подчиненного объекта. При этом возможно два варианта использования ПАП: в одном случае она рассматривается как инструмент управления ТОИВ, во втором применяется для анализа и прогнозирования его показателей.

Основные уровни ПАП ТОИВ (рис. 4) [1]: уровень первичной обработки данных включает объектно-ориентированный интерфейс прикладного программирования и интерфейс объектного языка запросов – SQL-язык; уровень поставщика данных представлен СУБД Microsoft SQL Server 2008; уровень предметной обработки данных, предполагающий разработку решений на основе результатов решения задач, полученных от сервера БД и уровня первичной обработки данных; уровень взаимодействия ДЛ с ПАП отвечает за ввод/вывод информации, получение отчётов, визуализацию результатов.

Рис. 4. Порядок обработки и учёта данных

В качестве системы управления в ПАП предлагается использовать плагинную архитектуру, предполагающую наличие менеджера плагинов, самих плагинов, взаимозаменяемого модуля, программно-завершённого модуля, что позволяет обеспечить инкапсуляцию данных и функций, наследование и полиморфизм. Главное окно ПАП должно включать панели управления внутренней и внешней средой. Все элементы управления и дизайн окна предлагается выполнять с помощью VSM-конструктора – совокупности скриптов и плагинов, разработанных в среде Visual Studio 2010, предназначенных для визуального и интерактивного отображения данных в Microsoft SQL Server 2008 R2. Для разработки панелей управления и согласованной работы плагинов оболочки и программных модулей предлагается использовать OLAP-технологию, основанную на аналитической обработке данных в режиме реального времени, позволяющую извлекать информацию из БД, структурировать, дополнять, обрабатывать данные, подготавливать их для расчётно-графических модулей, обновлять БД на основе полученных расчётов, осуществлять визуализацию результатов.

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

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

Система хранения информации должна обеспечивать хранение разнородных данных с консолидированием поступающей информации в нескольких БД и представлять собой программно-аппаратное решение по организации надёжного хранения ИР и предоставлению гарантированного доступа к ним. В БД должна также сохраняться информация: об особенностях (типе) каждой подсистемы управления; о типах взаимоотношений между ними; о типах и количестве ТС подсистем; о типах ресурсов, потребляемых подсистемами; о величине потребления ресурса; о фактах перемещений ТС.

Большинство задач ДЛ ТОИВ относится к классу информационно-аналитических, что требует соответствующего информационного обеспечения, которое не может быть реализовано классическими БД, так как они являются временным срезом и не предполагают изменения состояния объектов. Устранить этот недостаток могут информационные хранилища, строящиеся как многомерные структурированные совокупности данных, ориентированные на решение задач, связанных с анализом и прогнозом различных процессов.

Объединение требований к динамике и разнообразию типов информационных потоков ПАП позволяет дать характеристику технологий, формирующих архитектуру БД [1]: компонентная технология проектирования и перекомплектации предметно-ориентированных БД; расширенная технология хранилища различных данных, включающая средства оперативной аналитической обработки данных; открытость БД для включения в нее и получения из нее информации с использованием глобальной информационной магистрали. Предлагаемая структура БД позволяет хранить информацию об особенностях каждого объекта ТОИВ, при этом предполагается в качестве системы управления данными использовать MS SQL Server 2008 R2, графические и аналитические модули реализовывать в программной среде Mathcad, что повысит эффективность деятельности ДЛ ТОИВ. Разработанная ПАП позволяет реализовать механизм информационного обмена с использованием ИС и ресурсов АО посредством их интеграции, консолидации и унификации при обеспечении требований по полноте, доступности и целостности.

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

Для обеспечения конфиденциальности и безопасности обрабатываемой в ПАП информации разработана ***система информационной безопасности (СИБ)*** ТОИВ. Создание СИБ основывается на выявленных моделях угроз и модели нарушителя для ИС АО и учитывает категорирование информации, обращающейся в системе, и систем, её обрабатывающих. Объектами защиты являются прикладные системы, ***локальные вычислительные сети (ЛВС)***, телекоммуникационные компоненты, ИР, вычислительная техника. При этом реализуется комплекс защиты информации, обеспечивающий этапы её передачи, обработки и хранения.

В целом СИБ должна включать средства защиты от несанкционированного доступа, антивирусную защиту и защиту от вредоносного содержимого, систему обнаружения и предотвращения вторжений; комплекс механизмов и СЗИ, средств разграничения и контроля доступа, обеспечения целостности информации, протоколирования и аудита; систему обеспечения безопасности, включающую систему мониторинга и управления СЗИ, систему управления рисками и др.

Определены основные требования к элементам СИБ:

- структура СИБ должна состоять из двух уровней: по защите ИР, осуществляющих обработку, передачу и хранение конфиденциальной информации, и по защите остальных ИР, компонент ИС, не обрабатывающих конфиденциальную информацию. СИБ должна включать следующие технические решения: инфраструктуру сетевой безопасности, разграничения доступа и мониторинга сетевых активностей, обнаружения и предотвращения сетевых атак; систему безопасности узлов, приложений и БД, обеспечения информационной безопасности и мониторинга БД, ОИБ серверов; средства управления доступом в сети и в прикладных системах, идентификации и аутентификации ДЛ в ЛВС, идентификации ДЛ для систем, обрабатывающих конфиденциальную информацию; систему противодействия вредоносному содержимому, защиты от вредоносного содержимого электронной почты, антивирусной защиты на файловых серверах; систему обеспечения непрерывности предоставления информационных
услуг (IT-услуг); аналитические средства. Архитектура СИБ должна предполагать многослойность, модульность и возможность адаптации системы к различным организационным и техническим условиям; независимость функционирования каждой из подсистем;

- система должна функционировать в следующих режимах: штатном (7 дней в неделю); сервисном (для проведения ТО); аварийном (в случае возникновения нештатных ситуаций);

- компоненты СИБ должны обеспечивать расширение круга защищаемых ресурсов, добавление или удаление объектов защиты, изменение времени хранения и накопления хранимой информации; технические решения должны обеспечить масштабируемость производительности и объёма хранения данных при увеличении количества пользователей, узлов и компонент ИС.

Требования к функциям СИБ:

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

- единая система идентификации, аутентификации и управления ДЛ и правами их доступа к сетевым и информационным ресурсам должна обеспечить механизмы разграничения доступа к узлам и ресурсам ИС АО на основании матрицы доступа;

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

- планирование аварийного восстановления должно обеспечивать непрерывность предоставления IT-услуг, поддерживать разработку планов аварийного восстановления для систем ТОИВ, включение в их состав схем, графиков, инструкций и других документов в общеупотребительных форматах;

- АРМ ДЛ и информация на них должны быть защищены от угроз, связанных с поступлением вредоносного содержимого, с сетевыми атаками, подключением внешних устройств и средств хранения информации. Для этого комплекс ТС должен включать системы антивирусной защиты, системы персонального межсетевого экранирования, системы контроля за действиями ДЛ.

В целом СИБ должна выполнять задачи контроля прав доступа ДЛ к ресурсам ИС, контроля текущего уровня защищенности, протоколирования и аудита; оповещения администратора о сбоях в работе серверов, рабочих станций и средств защиты, о фактах вирусного заражения.

Создана ***система защиты персональных данных (СЗПДн)***. Перечень объектов защиты определялся по результатам обследования префектуры ЗАО г. Москвы [2, 3] и они включали: обрабатываемую информацию – персональные данные субъектов ПДн и сотрудников префектуры; технологическую информацию; программно-технические средства обработки; средства защиты; каналы информационного обмена; помещения, где размещены компоненты ***информационной системы ПДн (ИСПДн)***.

Персональные данные субъектов ПДн (гостей) и сотрудников префектуры включают более 70 категорий, в частности: фамилию, имя, отчество; место, год и дату рождения; гражданство; телефон; паспортные данные; фотографию; информацию о пребывании за границей и др. Технологическая информация включает: управляющую информацию (конфигурационные файлы, и пр.); информацию средств доступа к системам управления; информацию на съемных носителях информации, содержащих информацию системы управления ресурсами или средств доступа к ней; информацию о СЗПДн, их составе и структуре, технических решениях защиты; ИР, содержащие информацию о информационно-телекоммуникационных системах, о планах обеспечения бесперебойной работы; служебные данные, и др.

Суть организационных мер состоит в следующем – резервное копирование и хранение данных необходимо осуществлять на периодической основе: для обрабатываемых ПДн – не реже раза в неделю; для технологической информации – не реже раза в месяц; копий ПО (ОС, программные средства защиты), – не реже раза в месяц и каждый раз при внесении изменений в эталонные копии. Разработан план мероприятий по обеспечению защиты ПДн (табл. 1), содержащий организационные, технические и контролирующие мероприятия.

Таблица 1

План мероприятий по обеспечению безопасности ПДн

Мероприятие	Периодичность и исполнитель
Организационные	
Проведение обследования; определение обрабатываемых ПДн и объектов защиты; определение лиц, участвующих в обработке ПДн, и их ответственности; определение прав разграничения пользователей; организация порядка резервного копирования защищаемой информации на твёрдые носители и восстановления работоспособности ТС, ПО, БД и подсистем СЗИ ПДн; разработка инструкций о порядке обработки ПДн и обеспечения режима защиты; о действиях в случае возникновения внештатных ситуаций; разработка журнала учёта обращений субъектов ПДн	Разовое / обслуживающая организация. Сроки устанавливаются отдельно
Назначение ответственного за безопасность ПДн; введение режима защиты ПДн; собрание коллегиального органа по классификации ИСПДн; классификация ИСПДн; выбор помещений для установки аппаратных средств ИСПДн; организация контроля доступа в помещения, в которых установлены аппаратные средства; введение в действие инструкции по порядку формирования, распределения и применения паролей; организация учёта технических средств защиты и документации к ним	Разовое / территориальный орган исполнительной власти. Сроки устанавливаются отдельно
Технические (аппаратные и программные)	
Внедрение: хранилища зарегистрированных действий пользователей с ПДн; подсистемы: управления доступом, регистрации и учёта; обеспечения целостности; антивирусной защиты	Разовое / обслуживающая организация. Сроки устанавливаются отдельно
Контролирующие	
Создание журнала внутренних проверок	Разовое / обслуживающая организация. Сроки устанавливаются отдельно
Поддержание журнала внутренних проверок в актуальном состоянии	Ежемесячно / ТОИВ
Контроль: над соблюдением режима обработки ПДн; над выполнением антивирусной защиты; за обновлениями и единообразием применяемого ПО	Еженедельно / администратор безопасности
Контроль над соблюдением режима защиты	Ежедневно / администратор безопасности
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно / администратор безопасности
Контроль за обеспечением резервного копирования	Ежемесячно / администратор безопасности
Контроль за разработкой и внесением изменений в ПО собственной разработки или штатное ПО, дорабатываемое собственными разработчиками или сторонними организациями	Ежемесячно / администратор безопасности ИСПДн

Литература

1. ***Разработка*** требований и методов оценки качества энергосбережения и теплоснабжения населения и их влияние на риски чрезвычайных ситуаций: Отчёт о НИР / ОАО "Средства спасения", ООО "КИЦ "Техноценоз"". М., Калининград, 2011. 454 с.

2. ***Подсистема*** информационной безопасности. Отчёт о предпроектном обследовании: Отчёт по НИР / ЗАО г. Москвы, Управление корпоративных сетей и администрирования информационных ресурсов ОАО "ГУП Экономика". М., 2011. 200 с.

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

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

Статья опубликована 19 декабря 2012 г.