ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИРЕКТОР ФГУП «НИИ АВТОМАТИКИ», ДОКТОР ТЕХНИЧЕСКИХ НАУК, ПРОФЕССОР
Сергей Анатольевич Букашкин

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ РОССИИ

Среднесрочная стратегия социально-экономического развития страны, принятая Правительством Российской Федерации, предусматривает приоритетное развитие информатизации как процесса движения к информационному обществу от общества индустриального. Одним из факторов этого процесса является стремительное развитие информационных и телекоммуникационных технологий. Возрастают значимость и удельный вес отраслей, обеспечивающих создание, передачу и использование информации. Информация становится основным ресурсом и движущей силой социально-экономического, оборонного, научного, политического и культурного развития государства. Поэтому в настоящее время возрастает потребность органов государственного управления различных уровней в объективной, достоверной и своевременной информации о реальной обстановке в округах, регионах и отдельных городах Российской Федерации, в различных отраслях и ведомствах, секторах экономики.

Применение современных телекоммуникационных и информационных технологий является в настоящее время обязательным условием эффективного функционирования органов государственной власти. Методы управления экономикой страны, социальными процессами и обеспечение безопасности государства предусматривают использование и анализ значительных объемов информации при выработке и реализации управленческих решений, оперативном и перспективном прогнозировании ситуации, контроле за исполнением на местах тех решений, которые приняты органами федеральной власти.

Совокупность этих показателей, различающихся источниками информации, способами представления и формами ее отображения, образует консолидированный информационный ресурс государства, на основе которого принимаются решения по проблемам отдельных регионов, отраслей и страны в целом.

Единое информационное пространство, формируемое на федеральном уровне в процессе реализации Федеральной целевой программы «Электронная Россия» на 2002–2010 годы, должно поднять уровень информационного обеспечения органов государственной власти на качественно новую ступень. При этом важнейшим условием его создания является разработка и развертывание защищенной информационно-телекоммуникационной системы (ИТС), обслуживающей органы государственной власти и местного самоуправления, бюджетные и внебюджетные фонды и организации. Защищенная ИТС предназначена для обеспечения технологически эффективной поддержки процедур государственного управления. Это необходимо в интересах обеспечения безопасности государства, экономического роста и социальной стабильности в Российской Федерации, обеспечения конституционных прав граждан.

Развертывание защищенной ИТС должно предусматривать создание новых и интеграцию существующих региональных информационных и телекоммуникационных систем в современную, защищенную от утечек, перехвата и разрушений интегрированную технологическую систему информационного обеспечения, для упра-

вления регионами и страной в целом. Система должна предоставлять абонентам комплекс современных защищенных информационных и телекоммуникационных услуг. Она должна иметь возможность доступа к государственным информационным ресурсам, а также к ресурсам (к сетям связи и базам данных) различной ведомственной принадлежности, при условии реализации принципа гарантированного разграничения доступа.

Технические решения, реализованные в защищенной ИТС для органов государственной власти различных уровней, предоставят возможность субъектам структур государственного управления связывать множество приложений и платформ в режиме реального времени. Технологии, лежащие в основе данных решений, упрощают распространение информации и интеграцию информационных процессов путем привязки каждого приложения к общему информационному пространству, вместо связывания приложений друг с другом напрямую. Комплекс базовых технологий, заложенных в ИТС, дает возможность пользователям органов государственной власти автоматически передавать, получать, сортировать и персонализировать цифровую информацию в режиме реального времени.

Интеграция и централизация информационных ресурсов, необходимая для обеспечения устойчивого управления государством и экономикой на всех административных уровнях, в различные периоды эксплуатации, а также при чрезвычайных ситуациях, может быть обеспечена только за счет создания и развития информационной инфраструктуры органов государственной власти и управления страной. Указанная инфраструктура должна быть основана на современных информационных технологиях, защищенной телекоммуникационной среде, мощных межведомственных центрах обработки и анализа информации, в интересах федеральных и региональных органов государственной власти. Общая организационная структура защищенной ИТС должна быть иерархической и отражать сложившиеся уровни административного государственного управления и информационного взаимодействия.

Основными технологическими функциями и задачами ИТС органов государственной власти являются:

– обеспечение информационно-аналитической поддержки управленческой деятельности органов государственной власти на основе интеграции информационных фондов и базовых информационных технологий, с реализацией системного подхода к предоставлению, развитию и централизации комплекса информационных и телекоммуникационных услуг;
– обеспечение органов государственной власти комплексом современных телекоммуникационных услуг на основе интеграции технических возможностей сетей связи и передачи данных, входящих в систему, создание единой транспортной среды для взаимодействия различных объектов в структуре ИТС, унификации технических решений и средств на базе применения перспективных телекоммуникационных технологий;
– обеспечение гарантированного уровня информационной безопасности в ИТС органов государственной власти на основе комплексной системной интеграции методов и средств обеспечения информационной безопасности;
– реализация методов и средств обеспечения устойчивости и живучести ИТС органов государственной власти в условиях преднамеренных или случайных воздействий на их информационные ресурсы.

Для технологического достижения указанных целей в состав технической структуры защищенной ИТС на каждом организационном уровне административного управления должны быть включены:

– система интегрированных официальных информационных ресурсов ИТС;
– телекоммуникационная система для обеспечения взаимодействия информационных объектов ИТС;
– система обеспечения безопасности информации как составная часть всех других компонентов системы в целом.

Материально-технической основой консолидированного информационного ресурса должна стать составляющая интегрированных официальных информационных ресурсов (ИИР) ИТС. Она предназначена для поддержки процессов принятия решений высшими органами государственной власти, обеспечения информационного обслуживания и информационного взаимодействия федеральных и региональных органов исполнительной власти, решения задач информационно-аналитического обслуживания и оперативного информирования органов государственной власти РФ различных уровней и других абонентов, использующих ресурсы ИТС.

Подсистема ИИР ИТС реализуется аппаратно-программными средствами ситуационных, административных, аналитических и информационных центров, а также систем информационного обеспечения органов государственной власти, относящихся к федеральному, региональному, ведомственному или территориальному уровням, а также их технологическими телекоммуникационными средствами.

Информационно-аналитические объекты в составе подсистемы ИИР защищенной ИТС должны подключаться и взаимодействовать с другими средствами ИТС (в том числе телекоммуникационными). Это может быть сделано через унифицированные интерфейсы, реализованные на базе стандартных аппаратно-программных средств, образующих типовые интерфейсные коммуникационные узлы, входящие в состав каждого объекта.

Создание и внедрение в деятельность органов государственной власти Российской Федерации системы электронного документооборота, обеспечение информационного взаимодействия органов государственной власти, обеспечение их доступа к централизованным информационным ресурсам (в том числе к базам данных правовой информации) являются приоритетными направлениями развертывания ИИР ИТС.

Одной из основных задач межведомственного электронного документооборота в подсистеме ИИР защищенной ИТС является обеспечение контроля целостности пе-

редаваемых электронных образов документов, их аутентификация, а также предоставление возможности получения надежных реквизитов (цифровых сертификатов) всеми участниками электронного документооборота. В зависимости от типа решаемых задач и возникающих ситуаций техническими средствами информационных центров и объектов должны поддерживаться различные виды информационной обработки и обмена, включая организацию циркулярной и конференц-связи (речевой и видео).

Поддержка указанных режимов может привести к возникновению различных требований к вероятностно-временным характеристикам информационного обмена в контуре защищенной ИТС, включая требование на обработку информации, в различных ситуациях в реальном масштабе времени.

Взаимодействие информационных объектов и абонентов ИТС должно осуществляться с помощью средств телекоммуникационной подсистемы защищенной ИТС. Она обеспечивает формирование единого информационного пространства органов государственной власти путем интеграции ресурсов информационных фондов коллективного пользования. Важнейшей функциональной задачей телекоммуникационной подсистемы ИТС является создание взаимосвязанного федерального комплекса систем, средств и комплексов связи Российской Федерации. Данный комплекс обеспечивает системно-техническую интеграцию информационных и телекоммуникационных ресурсов, систем различного назначения, включая действующие системы правительственной связи, взаимоувязанную сеть связи России (ВСС), а также ФЦП «Электронная Россия».

Эффективное решение задач информационного обслуживания абонентов, интеграции технических возможностей существующих и перспективных сетей связи и передачи данных, взаимодействия ведомственных и региональных баз и банков данных требует разработки и создания телекоммуникационной составляющей защищенной ИТС. Она является интегрированной телекоммуникационной средой всей системы государственного управления, обеспечивающей федеральные органы государственной власти и органы власти субъектов РФ современными телекоммуникационными услугами, а также конфиденциальность информации при ее передаче и обработке.

Создание телекоммуникационной и информационной составляющей ИТС должно опираться на приоритетное использование технических средств и технологий, разрабатываемых и поставляемых отечественными предприятиями.

Построение телекоммуникационной подсистемы ИТС, образующей единую интегрированную телекоммуникационную среду на базе использования цифровых методов передачи и обработки информации, должно обеспечивать решение задач по эффективной организации телекоммуникационного обмена с целью предоставления пользователям услуг по поддержке процедур государственного управления, включая:

– передачу различных видов информации, в том числе речи, данных, графики, видео- и мультимедийной информации в реальном масштабе времени с высоким качеством предоставляемой связи;
– автоматизацию процессов обмена информацией и установления соединения;
– улучшение вероятностно-временных характеристик информационного обмена, его надежности и устойчивости;
– обеспечение эффективного управления информационными процессами в телекоммуникационной компоненте системы;
– повышение эффективности использования канального ресурса телекоммуникационной компоненты системы и снижения расходов на аренду каналов связи;
– повышение безопасности информационного взаимодействия и обмена информацией между компонентами системы;
– информационную и телекоммуникационную совместимость, сопряжение и интеграцию телекоммуникационной компоненты ИТС с действующими, а также перспективными системами правительственной связи, включая цифровую сеть интегрального обслуживания органов государственной власти, и системами, создаваемыми в рамках ФЦП «Электронная Россия»;
– эволюционное развитие существующих областных и региональных систем связи с поэтапным улучшением их тактико-технических характеристик на базе интеграции технических возможностей и ресурсов систем связи и передачи данных, входящих в структуру ИТС, с унификацией технических решений, применяемых аппаратно-программных средств и протоколов информационного взаимодействия, за счет использования перспективных телекоммуникационных технологий.

Увеличение объемов и видов информации, передаваемой разнотипными источниками в ИТС, увеличение (преобладание) данных и видеоинформации в общей структуре трафика, поддержка технологии передачи и обработки речевой, текстовой, картографической и мультимедийной информации, в том числе в реальном масштабе времени, предполагает необходимость ориентации на принципы интеграции услуг, служб и информационных ресурсов при создании и развертывании телекоммуникационной компоненты защищенной системы управления. При построении различных элементов подсистемы передачи информации в составе ИТС, ориентированных на решение задач каждого уровня, могут применяться различные сетевые решения. Это связано с тем, что системы связи на каждом уровне отличаются по функциям, параметрам информационного обмена, ведомственной принадлежностью и, как следствие, располагаемыми для их создания ресурсами. Однако, несмотря на принципиальную возможность применения на каждом уровне различных телекоммуникационных технологий и собственных принципов построения, общая идеология организации телекоммуникационной компоненты системы управления должна обеспечивать «сквозное» взаимодействие всех пользователей системы. Должен быть обеспечен регламентированный доступ абонентов к различным объектам ИТС независимо от особенностей и принципов их организации.

ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИТС

Эффективная поддержка процессов государственного управления с использованием средств и ресурсов ИИР возможна только в том случае, если система будет обладать свойством «защищенности». Оно обеспечивается реализацией комплексной системы защиты информации, включающей базовые компоненты защиты – систему управления доступом на объекты ИТС, систему видеонаблюдения и систему безопасности информации.

Ключевым звеном комплексной защиты является система безопасности информации, концептуальные положения которой вытекают из особенностей построения системы и составляющих ее подсистем. Понятие «защищенной» системы, может быть сформулировано следующим образом:

Защищенная ИТС – информационно-телекоммуникационная система, обеспечивающая устойчивое выполнение целевой функции в рамках заданного перечня угроз безопасности и модели действий нарушителя.

Перечень угроз безопасности и модель действий нарушителя определяются широким спектром факторов, включающих эксплуатационный процесс ИТС, возможные ошибочные и несанкционированные действия обслуживающего персонала и пользователей, отказы и сбои оборудования, пассивные и активные действия нарушителей.

При построении ИТС органов государственной власти целесообразно рассматривать три базовые категории угроз безопасности информации, которые могут привести к нарушению выполнения основной целевой функции системы – эффективной поддержки процессов государственного управления:

– отказы и сбои в аппаратных средствах системы, аварийные ситуации и другие события без участия человека;
– ошибочные действия и непреднамеренные действия обслуживающего персонала и абонентов системы;
– несанкционированные действия (пассивные и активные) нарушителей.

Несанкционированные действия нарушителя могут относиться к пассивным (перехват информации в канале связи, перехват информации в технических каналах утечки) и активным действиям (перехват информации с носителей информации с явным нарушением правил доступа к информационным ресурсам, искажение информации в канале связи, искажение, включая уничтожение, информации на носителях информации с явным нарушением правил доступа к информационным ресурсам, введение дезинформации).

Со стороны нарушителя могут осуществляться также активные действия, направленные на анализ и преодоление системы защиты информации. Данный тип действий целесообразно выделить в отдельную группу, поскольку, преодолев систему защиты, нарушитель может выполнять действия без явного нарушения правил доступа к информационным ресурсам. В указанном типе действий целесообразно выделить возможные действия, направленные на внедрение аппаратно-программных закладок в оборудование ИТС, что в первую очередь определяется использованием зарубежного оборудования, элементной базы и программного обеспечения.

На основе анализа архитектуры ИТС и угроз может быть сформирована общая архитектура системы безопасности информации, включающая следующие основные подсистемы:

– подсистему управления системой безопасности информации;
– подсистему безопасности в информационной подсистеме;
– подсистему безопасности в телекоммуникационной подсистеме;
– подсистему безопасности при межсетевом взаимодействии;
– подсистему выявления и противодействия активным действиям нарушителей;
– подсистему выявления и противодействия возможным аппаратно-программным закладкам.

Последние три подсистемы являются компонентами второй и третьей подсистем, но с учетом сформулированных выше особенностей их целесообразно рассматривать как отдельные подсистемы.

Основой системы безопасности информации в ИТС и каждой из ее подсистем является политика безопасности в ИТС и ее подсистемах. Ее ключевыми положениями являются требования использования следующих базовых механизмов и средств обеспечения безопасности информации:

– идентификация и аутентификация абонентов ИТС, оборудования ИТС, обрабатываемой информации;
– контроль информационных потоков и жизненного цикла информации на базе меток безопасности;
– управление доступом к ресурсам ИТС на основе сочетания дискреционной, мандатной и ролевой политик и межсетевого экранирования;
– криптографическая защита информации;
– технические средства защиты;
– организационные и режимные меры.

Данный перечень механизмов защиты определяется целями системы защиты информации в ИТС, среди которых выделяются пять основных:

– управление доступом к информационным ресурсам ИТС;
– обеспечение конфиденциальности защищаемой информации;
– контроль целостности защищаемой информации;
– доступ к информационным ресурсам;
– готовность информационных ресурсов.

Реализация указанных механизмов и средств защиты базируется на интеграции аппаратно-программных средств защиты в аппаратно-программные средства ИТС и обрабатываемую информацию.

Под термином «информация» в ИТС понимаются следующие виды информации:

– пользовательская информация (информация, необходимая для управления и принятия решений);

– служебная информация (информация, обеспечивающая управление оборудованием ИТС);
– специальная информация (информация, обеспечивающая управление и работу средств защиты);
– технологическая информация (информация, обеспечивающая реализацию всех технологий обработки информации в ИТС).

При этом защите подлежат все перечисленные виды информации.

Без применения автоматизированных средств управления системой безопасности информации невозможно обеспечить устойчивую работу системы безопасности в территориально распределенной системе обработки информации, взаимодействующей как с защищенными, так и незащищенными системами в контуре ИТС и обрабатывающей информацию различного уровня конфиденциальности.

Основными целями подсистемы управления безопасностью информации являются:
– формирование, распределение и учет специальной информации, используемой в подсистемах защиты (ключевая информация, парольная информация, метки безопасности, права доступа к информационным ресурсам);
– конфигурирование и управление средствами обеспечения безопасности информации;
– согласование политики безопасности во взаимодействующих системах, включая специальную информацию;
– мониторинг системы безопасности;
– актуализация политики безопасности в ИТС с учетом различных периодов эксплуатации, внедрения в ИТС новых технологий обработки информации.

Реализация подсистемы управления безопасностью информации требует создания единого центра управления, взаимодействующего с локальными центрами управления безопасностью телекоммуникационной и информационной подсистемами ИТС, центрами управления безопасностью информации во взаимодействующих сетях и агентами безопасности информации на объектах системы.

Архитектура системы управления безопасностью информации должна быть фактически идентична архитектуре самой ИТС, а с точки зрения ее реализации должны выполняться следующие принципы:
– центр управления безопасностью информации и локальные центры управления должны реализовываться на выделенных аппаратно-программных средствах с использованием отечественных средств;
– агенты управления безопасностью должны интегрироваться в аппаратно-программные средства рабочих мест системы с возможностью независимого от них управления со стороны центра и локальных центров.

Подсистема безопасности информации в информационной подсистеме ИТС – одна из наиболее сложных подсистем как с точки зрения механизмов защиты, так и их реализации. Сложность этой подсистемы определяется тем, что именно в данной подсистеме выполняется основной объем обработки информации, при этом в ней сосредоточены основные ресурсы по доступу к информации абонентов системы – абоненты непосредственно имеют санкционированный доступ как к информации, так и к функциям ее обработки. Именно поэтому основу данной подсистемы составляет система управления доступом к информации и функциям ее обработки.

Базовым механизмом реализации санкционированного доступа к информации и функциям ее обработки является механизм защиты информационных ресурсов от несанкционированных действий, основными компонентами которого являются:
– организационно-технические средства управления доступом к объектам системы, информации и функциям ее обработки;
– система регистрации и учета работы системы и абонентов системы;
– подсистема обеспечения целостности;
– криптографическая подсистема.

Основой реализации отмеченной защиты является архитектурное построение информационной составляющей ИТС – создание логически и информационно выделенных объектов информационного компонента ИТС (банки данных, информационно-справочные комплексы, ситуационные центры). Это позволит реализовать криптографически независимые изолированные объекты, функционирующие по технологии клиент–сервер и не предоставляющие непосредственного доступа к хранилищам информации и функциям ее обработки, – вся обработка производится по санкционированному запросу пользователей на базе предоставленных им полномочий.

Для санкционированного предоставления информационных ресурсов абонентам применяются следующие методы и механизмы:
– метки безопасности информации;
– идентификация и аутентификация абонентов и оборудования системы;
– криптографическая защита информации при хранении;
– криптографический контроль целостности информации при хранении.

При реализации *подсистемы безопасности в телекоммуникационном компоненте ИТС* необходимо учитывать наличие каналов связи как на контролируемой, так и на неконтролируемой территории.

Обоснованным способом защиты информации в каналах связи является криптографическая защита информации в каналах связи на неконтролируемой территории в сочетании с организационно-техническими средствами защиты информации в каналах связи на контролируемой территории, с перспективой перехода на криптографическую защиту информации во всех каналах связи ИТС, в том числе *с использованием методов технологии VPN*. Ресурсом защиты информации в телекоммуникационной подсистеме (с учетом наличия нарушителей с легальным доступом к телекоммуникационным ресурсам) является разграничение доступа

к телекоммуникационным ресурсам с регистрацией потоков информации и регламента работы абонентов.

Типовым решением защиты информации в каналах связи является применение абонентского и линейного контуров защиты в сочетании с алгоритмическими и техническими средствами защиты, обеспечивающих (как напрямую, так и косвенно), следующие механизмы защиты:

– защита от утечки информации в каналы связи и в технические каналы;
– контроль сохранности информации при передаче по каналам связи;
– защита от возможных атак нарушителя по каналам связи;
– идентификация и аутентификация абонентов;
– управление доступом к ресурсам системы.

Подсистема безопасности при межсетевом обмене в ИТС основывается на следующих механизмах безопасности:

– управлении доступом к ресурсам межсетевого обмена (межсетевое экранирование);
– идентификации и аутентификации абонентов (включая криптографические способы аутентификации);
– идентификации и аутентификации информации;
– криптографической защите информации в каналах связи на неконтролируемой территории, а в перспективе – во всех каналах связи;
– криптографической изоляции взаимодействующих систем.

Важное значение в рассматриваемой подсистеме имеет реализация технологии виртуальных частных сетей (VPN), свойства которых во многом решают вопросы как защиты информации в каналах связи, так и противодействия атакам нарушителей со стороны каналов связи.

Существенным также для данной подсистемы является реализация механизмов идентификации и аутентификации информации и абонентов, основным средством которой является цифровая подпись, что объясняется следующими факторами:

– одной из функций ИТС является принятие решений по управлению как отдельными ведомствами и предприятиями, так и государством в целом на основе аналитической обработки информации;
– не исключается существование нарушителей среди абонентов, взаимодействующих с ИТС систем.

Подсистема выявления и противодействия активным действиям нарушителя реализуется на двух основных компонентах: аппаратно-программных средствах выявления и противодействия возможным атакам нарушителей по каналам связи и архитектуре защищенной сети.

Первый компонент – компонент выявления возможных атак, предназначен для защиты в тех подсистемах ИТС, в которых принципиально возможны действия нарушителя в части атак на информационные ресурсы и оборудование ИТС, второй компонент – предназначен для исключения таких действий или существенного их затруднения.

Основными средствами второго компонента являются аппаратно-программные средства, обеспечивающие реализацию методов защиты в соответствии с технологией виртуальных частных сетей (VPN) как при взаимодействии различных объектов ИТС в соответствии с их структурой, так и внутри отдельных объектов и подсетей на базе межсетевых экранов или межсетевых экранов со встроенными средствами криптографической защиты.

Подчеркнем, что наиболее эффективное противодействие возможным атакам обеспечивают криптографические средства линейного контура защиты и межсетевого криптографического шлюза для внешних нарушителей и средства управления доступом к информационным ресурсам для легальных пользователей, относящихся к категории нарушителя.

Подсистема выявления и противодействия возможным аппаратно-программным закладкам реализуется комплексом организационно-технических мероприятий при изготовлении и эксплуатации оборудования ИТС, включающем следующие основные мероприятия:

– специальную проверку оборудования и элементной базы зарубежного производства;
– эталонирование программного обеспечения;
– проверку свойств элементной базы, влияющих на эффективность системы защиты;
– проверку целостности программного обеспечения с использованием криптографических алгоритмов.

Одновременно с другими задачами вопрос противодействия возможным аппаратно-программным закладкам обеспечивают и другие средства защиты:

– линейный контур криптографической защиты, обеспечивающий защиту от активизации возможных программных закладок по каналам связи;
– архивирование информации;
– резервирование (дублирование аппаратных средств).

Средствами ИТС на различных объектах системы пользователям органов государственной власти могут предоставляться различные услуги по передаче информации и информационному обслуживанию, включая:

– защищенную подсистему документооборота;
– удостоверяющие центры;
– защищенную подсистему передачи телефонной информации, данных и организации видеоконференции;
– защищенную подсистему официального информирования, включая создание и обслуживание официальных сайтов руководителей федерального и регионального уровней.

Защищенная подсистема документооборота жестко связана с удостоверяющими центрами, обеспечивающими реализацию механизма цифровой подписи.

Рассмотрим более подробно интеграцию средств обеспечения безопасности информации в систему электронного документооборота, в подсистему передачи телефонной информации, подсистему официального информирования и официальный сайт руководителей различного уровня.

Базовым механизмом защиты информации в системе электронного документооборота является

электронная цифровая подпись, обеспечивающая идентификацию и аутентификацию документов и абонентов, а также контроль их целостности.

Поскольку особенности системы документооборота ИТС определяются наличием информационного обмена между различными объектами и ведомствами (включая возможный информационный обмен между защищенными и незащищенными системами), а также использованием различных технологий обработки документов в различных ведомствах, то реализация защищенного документооборота с учетом сформулированных факторов требует выполнения следующих мероприятий:

– унификации формата документов в различных ведомствах;
– согласования политик безопасности в различных ведомствах.

Отмеченные требования могут быть решены частично с использованием шлюзов между взаимодействующими системами.

Удостоверяющие центры по своей сути представляют собой распределенную базу данных, обеспечивающих реализацию цифровой подписи в системе документооборота. Несанкционированный доступ к информационным ресурсам этой базы данных полностью разрушает свойство защищенности электронного документооборота. Отсюда вытекают основные особенности системы защиты информации на удостоверяющих центрах:

– управление доступом к ресурсам базы данных удостоверяющих центров (защита от НСД к ресурсам);
– обеспечение устойчивой работы удостоверяющих центров в условиях возможных отказов и сбоев, аварийных ситуациях (защита от разрушения информации баз данных).

Реализация указанных механизмов может быть выполнена в два этапа: на первом этапе механизмы защиты реализуются с использованием организационно-технических мер защиты и режимных мероприятий, включая использование отечественной сертифицированной операционной системы, а на втором – производится интеграция криптографических способов защиты в аппаратно-программные средства при хранении и обработке информации на удостоверяющих центрах.

Особенности защиты трафика различного вида, передаваемого в ИТС (телефонного трафика, данных и трафика видеоконференцсвязи), можно разделить на два класса:

1) особенности защиты абонентского оборудования, которые определяются необходимостью защиты информации различного типа (видеоинформация и речь, а возможно, и данные), а также необходимостью защиты информации различного типа от утечки в технические каналы;
2) особенности защиты оборудования системы передачи информации определенного вида, которые определяются необходимостью защиты от несанкционированного доступа к услугам телефонной связи, передачи данных, конференц-связи и ее ресурсам.

Для указанных классов базовыми механизмами защиты являются:

– технические средства защиты информации от утечки в технические каналы, реализуемые стандартными средствами;
– управление доступом к ресурсам, обеспечивающим организацию связи различных видов, в основе которого лежит идентификация и аутентификация возможных подключений различных пользователей и оборудования к оборудованию связи.

Особенностью защищенной подсистемы официального информирования является наличие потоков информации в двух направлениях – от ИТС к внешним системам, включая отдельных граждан страны, а также от внешних систем к ИТС (информационный обмен с незащищенными объектами).

На основе информации, поступающей от внешних систем, вырабатываются решения в интересах как отдельных организаций, ведомств и регионов, так и государства в целом, а от информации, поступающей во внешние системы, зависит исполнение выработанных решений также на всех уровнях государственного управления. Поэтому в первом случае основными требованиями, предъявляемыми к функционированию системы с точки зрения ее безопасности, являются целостность предоставляемой информации, оперативность предоставления информации, включая ее обновление, достоверность источника информации, контроль доведения информации до получателя. Во втором случае – достоверность предоставляемой информации, достоверность источника информации, оперативность доведения информации, а также контроль доведения информации до получателя. В основном перечисленные требования обеспечиваются стандартными механизмами защиты (криптографические способы контроля целостности информации, идентификации и аутентификации абонентов и информации). Отличительной особенностью, характерной для данной подсистемы, является необходимость контроля достоверности информации, поступающей от внешних систем и являющейся исходным материалом для выработки решений, в том числе и в интересах государства. Эта задача решается с использованием аналитических методов контроля достоверности информации, обеспечивающих устойчивость выработанных решений в условиях поступления недостоверной информации, и организационно-технических мер, обеспечивающих подтверждение поступающей информации.

Главными целями системы защиты информации на сайте руководителей федерального и регионального уровней являются исключение попадания на сайт информации, не предназначенной для этого, а также обеспечение целостности информации, представленной на сайте. Базовый механизм защиты, реализованный на сайте, должен обеспечивать управление доступом к сайту со стороны внутренней системы, обеспечивающей предоставление информации на сайт, а также управление доступом со стороны внешних систем к ресурсам сайта. Реализация защиты

основана на создании особой зоны на основе межсетевых экранов (шлюзов), обеспечивающих:

– фильтрацию информации в направлении от внутренней системы к сайту с контролем доступа к сайту со стороны внутренней системы (идентификацией и аутентификацией источника информации) и фильтрацию информации с использованием меток безопасности;
– контроль целостности информационных ресурсов на сайте и обеспечение устойчивой работы сайта в условиях возможных искажений информации;
– контроль доступа со стороны внешних систем к ресурсам сайта;
– фильтрацию запросов, поступающих на сайт со стороны внешних систем.

Одним из важнейших вопросов при решении задач обеспечения безопасности информации является совершенствование нормативной базы в части безопасности информации. Необходимость совершенствования нормативной базы определяется двумя основными факторами – наличием информационного обмена между различными ведомствами, наличием большого количества видов и типов информации, циркулирующей в ИТС.

В части обеспечения безопасности информации в ИТС совершенствование нормативной базы необходимо проводить по следующим направлениям:

– создание единых требований по обеспечению безопасности информации и на их основе единой концепции безопасности, обеспечивающей возможность согласования политик безопасности в различных ведомствах и ИТС в целом, включая различные периоды эксплуатации;
– создание единого стандарта на документальную информацию, обеспечивающего внедрение унифицированных меток безопасности и снижающего затраты на трансляцию документов при межведомственном взаимодействии;
– создание положений межведомственного взаимодействия, обеспечивающих постоянный мониторинг безопасности информации при межведомственном взаимодействии.

В заключение необходимо подчеркнуть, что немаловажной задачей при создании ИТС является процедура эволюционного развития как функциональных возможностей ИТС, так и системы безопасности информации, обеспечивающей заданный уровень безопасности информации.

Выбор базовых программно-технических средств при создании ИТС должен производиться с учетом следующих принципов:

– архитектура ИТС и базовые технологии обработки информации в ИТС должны создаваться с учетом эволюционного перехода на средства отечественной разработки;
– автоматизированные рабочие места ИТС системы безопасности информации должны создаваться на аппаратно-программной платформе отечественного производства (ЭВМ отечественной сборки, отечественная операционная система, отечественные программные средства);
– архитектура ИТС и базовые технологии обработки информации в ИТС должны создаваться с учетом возможности использования на первом этапе действующих аппаратно-программных средств защиты с последующей заменой их на перспективные средства защиты информации.

Выполнение этих требований обеспечит непрерывность и заданную эффективность защиты информации в переходный период от использования в ИТС технологий обработки информации в сочетании с технологиями защиты информации к использованию в ИТС защищенных технологий обработки информации.