МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

А.А. Демидов

ПРОБЛЕМЫ КОНТРОЛЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОБЪЕКТАХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ОРГАНОВ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Учебное пособие

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург

2015

А. А. Демидов **Проблемы контроля безопасности информации на объектах телекоммуникационных систем органов государственного управления: учебное пособие.** — СПб: Университет ИТМО, 2015. — 70 с.

Данное пособие отражает современные тенденции в предметной области и может быть полезно специалистам в области защиты информации. В представленных материалах, в частности, рассматриваются следующие вопросы: условия, определяющие характер функционирования телекоммуникационных систем органов государственного управления; анализ объектов защиты информации; анализ угроз безопасности информации; современное состояние проблемы контроля безопасности информации в телекоммуникационных системах органов государственного управления; обоснование структуры системы комплексного контроля безопасности информации.

Издание адресовано студентам магистерской программы «Управление государственными информационными системами» и слушателям дополнительной образовательной программы повышения квалификации «Электронное правительство и инновационные технологии управления», реализуемой Центром технологий электронного правительства Университета ИТМО.

Рекомендовано к печати учёным советом Факультета технологического менеджмента и инноваций.

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий и один из немногих российских вузов, получивших в 2009 г. статус национального исследовательского университета. С 2013 г. Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

Оглавление

Введение

Современный период развития социально-экономических и политических процессов в России сопровождается развитием информационных ресурсов. В этих условиях существенно повышается роль информации и актуализируется проблема формирования единого информационного пространства страны и перехода от индустриального к информационному обществу. Необходимым условием решения этой проблемы является совершенствование информационного обеспечения деятельности органов государственного управления, научных, промышленных, банковских и других структур на основе предоставления достоверной, своевременной, полной, системно организованной и безопасной информации как основы эффективного управления, безопасности личности, общества и государства.

Решение этих вопросов неразрывно связано с созданием уникальных телекоммуникационных систем и обеспечением их безопасности в условиях широкого использования новых информационных технологий и воздействия внутренних и внешних угроз информационной безопасности. Ярким проявлением таких угроз являются широкомасштабные «информационные войны», несанкционированный доступ к защищаемым информационным ресурсам, недостаточная информированность должностных лиц органов государственного управления при анализе социально–экономических, политических, военных, экологических и других ситуаций.

С учетом этого обеспечение информационной безопасности предполагает наличие эффективной системы администрирования и контроля безопасности информации на телекоммуникационных объектах, по результатам функционирования которой реализуется комплекс адекватных методов устойчивой защиты от угроз, неразрывно связанных с использованием результатов глубоких исследований фундаментальных аспектов информационной безопасности, разработкой научно обоснованных методов обеспечения защиты информации в условиях неопределенности, риска, внешних воздействий и динамичных внутренних изменений объектов деятельности.

В настоящее время известно значительное количество работ, посвященных отдельным, частным аспектам рассматриваемой проблемы. Однако большинство авторов основное внимание уделяли вопросам создания технических средств, систем обработки, защиты информации и, в меньшей степени, вопросам, проблемам теоретического и системного плана, в основе которых лежат управленческие аспекты обеспечения безопасности информации.

Данная брошюра отражает современные тенденции в предметной области и может быть полезна специалистам в области защиты информации, а также аспирантам и студентам вузов по профильным специальностям.

Глава 1.
Условия, определяющие характер функционирования телекоммуникационных систем органов государственного управления

Современный этап развития России характеризуется возрастающей ролью информационной сферы, представляющей совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Материальной основой информационной сферы является единое информационно-телекоммуникационное пространство страны как база решения задач социально-экономического, политического, военного, научного и культурного развития страны и обеспечения ее безопасности. Кроме этого, современный период развития России происходит в условиях перехода к рыночным экономическим отношениям, опасных воздействий окружающей среды, средств вооруженной борьбы и информационных войн и сопровождается:

- интенсивным формированием и совершенствованием государственных структур управления, переустройством экономики, военными реформами, направленными на реализацию военной оборонительной доктрины, ведущей к поэтапному сокращению ассигнований программ, численности войск и вооружений, расширения международных контактов и, с другой стороны, ослаблением (после распада СССР и Варшавского договора) боевой мощи ВС России;
- усложнением социально-экономических процессов, обострением межнациональных отношений, возникновением региональных военных конфликтов внутри страны и в приграничных районах, ростом экстремизма и преступности, периодическими экологическими катастрофами и стихийными бедствиями.

В этих условиях особенно остро встали проблемы совершенствования информационного обеспечения деятельности органов государственного управления (ОГУ). Их решение требует дальнейшего развития систем управления и их материальной основы – современных систем обработки информации. Это в полной мере относится к информационно-телекоммуникационным системам (ТКС) ОГУ, в т.ч. специального

назначения, и их компонентам, телекоммуникационной системе конфиденциальной связи, информационной и системе информационной безопасности. Особенностью функционирования таких систем является «производство» информации не только особого качества, но и информации, обладающей соответствующим правовым статусом. Такая правовая информация (ПрИн), в отличие от других видов информации, имеет свои особенности. Будучи включенной в контур управления социально-экономическими, политическими, военными и другими системами, она имеет ряд особенностей: предполагает обязательность исполнения и ответственность за неисполнение; отсутствие или неадекватность ПрИн при выработке, принятии или реализации решений, как и неисполнение предписаний даже адекватной ПрИн, влекут за собой тяжелые последствия и снижение эффективности процессов управления. Это, по сути, и обусловливает появление проблемы обеспечения комплексного контроля информационной безопасности информационных систем различных классов.

Сущность и содержание современного понятия информационной безопасности находится в центре внимания исследователей уже несколько десятков лет. До недавнего времени оно ассоциировалось, как правило, с рядом проблем защиты информации в автоматизированных системах обработки данных (АСОД), автоматизированных системах обработки информации и управления, электронно-вычислительных машинах, их системах и сетях, технических средствах обработки информации (ТСОИ) и других, направленной на скрытие содержания информации, обрабатываемой в этих системах.

В силу исторически сложившихся обстоятельств рассматриваемое понятие появилось и приобрело определенное содержание в связи с возникновением, созданием и развитием автоматизированных систем обработки информации, автоматизированных систем управления различных классов и предназначения.

В дальнейшем, применительно к той же АСОД, ранее предложенное определение было сформулировано несколько по-другому.

Защита информации – это применение в системах ее обработки методов ($П_м$) и средств ($П_с$), а также осуществление мероприятий ($О_м$) с целью ($Ц$) поддержания в заданных пределах существенно значимых характеристик ($П_х$) защищаемой информации и установленного статуса обращения ($П_{ус}$) с нею:

$$ЗИ = \{П_м, П_с, О_м\}; \quad Ц = \{П_х, П_{ус}\} \qquad (1.1)$$

Нетрудно видеть, что содержания последних определений защиты информации адекватны и отличаются степенью общности формулировок, диапазоном интерпретации.

В «Положении о государственном лицензировании в области защиты информации», утвержденном решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. № 10 дано следующее определение.

Безопасность информации (БИ) – состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных).

Это определение дополняется понятием *защиты информации*.

Защита информации – комплекс мероприятий ($К_м$), проводимых с целью предотвращения утечки ($П_{ут}$), хищения ($П_х$), утраты ($П_у$), несанкционированного уничтожения ($П_{нсу}$), искажения ($П_{нси}$), модификации (подделки) ($П_{нсм}$), несанкционированного копирования ($П_{нск}$), блокирования информации ($П_{нсб}$) и т. п.:

$$ЗИ = \{К_м\}; \quad Ц = \{П_{ут}, П_х, П_у, П_{нсу}, П_{нси}, П_{нсм}, П_{нск}, П_{нсб}\} \qquad (1.2)$$

По мнению авторов, кроме детализации содержания этого определения по целям защиты, оно отражает задачи защиты информации в информационных системах, и, в определенной степени, может быть использовано для определения понятия информационной безопасности и формулировки задач ее контроля. Однако в указанном Положении не определено и не раскрыто содержание понятий «информация», «информационные ресурсы», «информационная система», что затрудняет однозначное понимание объекта контроля.

Анализ содержания норм закона «Об информации, информатизации и защите информации» позволил выявить следующее: несмотря на отсутствие самой дефиниции понятия «защита информации», «безопасность информации», «информационная безопасность», представленное содержание целей контроля защиты информации (предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение угроз безопасности личности, общества и государства; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию, информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством; обеспечение прав субъектов в информационных

процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения), по существу отражает современное понимание информационной безопасности; детальное представление целей защиты позволяет раскрыть содержание понятия и определить задачи защиты и ее контроля, которые затрагивают не только понятие БИ, но и информационной безопасности.

Важным в процессе формирования исследуемого понятия является появление в стране нормативных правовых актов, таких как законы «О безопасности», «Об участии в международном информационном обмене». Основой существующих понятий информационной безопасности является известное понятие безопасности, приведенное в Законе РФ «О безопасности».

Основными объектами этой безопасности являются права и свободы личности, духовные материальные ценности общества, конституционный строй, суверенитет и территориальная целостность государства.

С учетом этого общего понятия безопасности, а также рассмотренных ранее определений безопасности и целей защиты информации можно считать, что наиболее полным будет определение информационной безопасности, приведенное в Федеральном законе Российской Федерации «Об участии в международном информационном обмене» № 85–ФЗ от 4 июля 1996 г.

Содержание определения безопасности рассматривает состояние защищенности среды от воздействия на нее внутренних и внешних угроз. Вполне очевидно, что и состояние защищенности информационной среды различных сфер деятельности, личности общества и государства также зависит от угроз, источником которых могут быть информация, информационные процессы, технологии и системы. Информация, информационные процессы, технологии и системы в то же время являются и объектами защиты как составляющие информационной среды.

Одной из конкретных форм проявлений угроз информационной безопасности является канал несанкционированного получения информации (КНПИ). С учетом этого в наиболее общем виде понятие канала угроз может быть определено как организованная часть пространства (функционального, материального, логического) для передачи либо получения чего-либо. Здесь можно говорить о санкционированных, несанкционированных, выявленных, не выявленных, скрытых, открытых и других каналах угроз.

В силу известных традиций развития АСОД для них дается понятие угроз информации с позиций рассмотренного ранее требования ее безопасности [9, 10].

Останавливаясь на приведенном выше обобщенном понятии информационной безопасности, можно говорить о сложности и многоаспектности подходов формирования понятия информационной безопасности, что обусловливает необходимость дальнейших исследований комплекса вопросов, включая понятийный аппарат, основные объекты информационной безопасности – информацию, информационные системы и процессы.

Решение проблем развития и совершенствования информационного обеспечения деятельности высших органов государственной власти, крупных организационно-технических, промышленных, банковских и других структур неразрывно связано не только с практическим созданием, обеспечением и функционированием уникальных ТКС и их компонентов, но и с обеспечением их информационной безопасности в условиях «информационной войны».

Телекоммуникационный компонент ОГУ как подсистема представляет интегрированную государственную систему конфиденциальной связи (ИСКС) страны, призванную обеспечивать широкий спектр коммуникационных услуг. Основное ее назначение – создание единого коммуникационного пространства в интересах государственных органов власти, которое будет использоваться в условиях как стабильного, устойчивого развития, так и неустойчивого развития государства (переходный период, особый период и т.д.).

Основными требованиями к ТКС ОГУ являются

- непрерывность, устойчивость и оперативность процессов государственного управления и информационного обеспечения органов власти в условиях мирного времени, особого периода, а также при чрезвычайных ситуациях и происшествиях;
- предоставление пользователям (абонентам, должностным лицам систем управления органов государственной власти) возможностей одновременной передачи различных видов информации и расширенного перечня информационных и телекоммуникационных услуг связи, соответствующего требованиям современных информационных технологий;
- широкий охват органов управления цифровыми магистральными трактами через электронные автоматические междугородные и международные центры страны;
- обеспечение возможности выхода абонентов России на страны ближнего и дальнего зарубежья;
- гарантированную защиту информации, информационных систем с использованием криптографических, алгоритмических,

организационно-технических мер и других средств на всех участках обработки информации;

- унификацию технических средств, алгоритмов и протоколов на основе использования международного и отечественного опыта по совершенствованию ТКС;
- максимальное использование ресурсов действующих сетей и систем органов государственной власти и, в первую очередь, силовых ведомств и министерств, занимающих ведущую роль в формировании и реализации научно-технической политики и использовании научно-технических достижений в области построения цифровых сетей интегрального обслуживания.

Особое значение приобретает обеспечение телекоммуникационной поддержки управления государством в условиях неустойчивого развития, характеризующегося наличием особых, экстремальных ситуаций, связанных с проведением глобальных общественно-политических преобразований и экономических реформ, возникновением крупных природных и техногенных аварий и катастроф, обострением внутренней и международной обстановки, появлением вероятности военного конфликта и переходом государства в период военных действий. В этот период большое значение в обеспечении информационного обмена, несомненно, будут играть мобильные элементы ТКС ОГУ, представляемые совокупностью подвижных и полевых систем засекреченной связи, в т.ч. правительственной связи, засекреченной связи Министерства обороны, Федеральной службы безопасности, Федеральной пограничной службы, Министерства внутренних дел и других ведомств.

Кроме того, к основным характерным особенностям создания основных компонент и ТКС ОГУ в целом можно отнести

- обеспечение управления социально-экономическими процессами и вооруженными силами высшим руководством страны;
- обработка компонентной конфиденциальной связи (свыше 30%), циркулирующей в системах специальной связи информационной нагрузки;
- способность функционирования с учетом распределения полномочий между различными уровнями управления страной, организации руководства исполнительными органами власти и особенностями информационного взаимодействия как на каждом уровне, так и между ними;
- обеспечение непрерывности, устойчивости и оперативности процессов государственного управления и информационного

обеспечения органов власти в условиях мирного времени, особого периода, а также при чрезвычайных ситуациях и происшествиях;

- предоставление пользователям возможности одновременной передачи различных видов информации и расширенного перечня услуг связи, соответствующих требованиям современных информационных технологии;
- гарантированность заданного уровня информационной безопасности, в т.ч. высокую гарантированную защищенность информации с использованием криптографических, алгоритмических и организационно-технических мер и средств на всех участках ее передачи, обработки и хранения;
- унификация математического, программного, лингвистического, технического обеспечения с учетом использования международного и отечественного опыта разработки и совершенствования ТКС ОГУ и ее компонентов;
- максимальное использование ресурсов действующих сетей и систем министерств и ведомств, в т.ч. специального назначения, а также научно-технических достижений в области построения цифровых сетей интегрального обслуживания;
- минимизации затрат на всех этапах жизненного цикла ТКС ОГУ и ее компонентов.

Анализ организационно-технической базы и научно-технического потенциала страны, а также различных подходов и концепций построения компонентов и в целом ТКС ОГУ позволил выделить следующие основные принципы их создания

- поэтапное формирование ТКС путем объединения основных наиболее разветвленных сетей и систем телефонной и документальной связи, с осуществлением постепенной модернизации используемых и вводом новых средств, обеспечивающих переход к международным стандартам, улучшение качественных и количественных показателей связи, расширение предоставляемых пользователям услуг;
- внедрение новых средств осуществляется на базе имеющихся организационно-технических структур, основу которых составляют центры правительственной связи, размещенные во всех краевых, областных центрах и столицах автономных республик;
- обеспечение безопасности связи на основе применения абонентского принципа шифрования, обеспечивающего

гарантированную защиту передаваемой информации во всем тракте ее прохождения от абонента до абонента;

- обеспечение приоритетности обслуживания и разграничения абонентов по возможности доступа в соответствии с предоставленным им статусом и правами, идентификация абонентов, контроль целостности данных пользователей;
- переход на цифровые магистральные каналы путем преимущественного использования оптоволоконных, спутниковых и радиорелейных систем связи.

К перечисленным выше особенностям и принципам создания ТКС ОГУ актуальность обеспечения надежной защиты информации подчеркивается рядом особенностей подсистем обеспечения безопасности, распределенной обработки информации и предназначением составных частей ТКС ОГУ

- использование большинства подсистем ТКС для обеспечения управления высшего военно-политического руководства страны;
- возрастание объема, сложности и новизны мероприятий по управлению страной и ее вооруженными силами в условиях формирования;
- большие объемы конфиденциальной информации, обрабатываемой в телефонной засекреченной сети, требующей строгого поддержания установленного для нее статуса;
- высокие требования абонентов по обеспечению безопасности информации;
- массовый доступ пользователей, что, с одной стороны, увеличивает вероятность злоумышленных действий, с другой – создает предпосылки для непреднамеренного нарушения целостности информации;
- большая вероятность нарушений безопасности информации, в т.ч. нарушения физической и логической целостности, искажение или уничтожение данных и информации, связей между их компонентами, несанкционированная модификация получения, размножения, присвоения права собственности на информацию, приводящие к огромным потерям (экономическому ущербу, потере приоритетных прав, разглашению государственной, военной тайны и т.д.);
- усложнение организационно-технического построения и функционирования систем конфиденциальной связи как в особый

период, так и в различных условиях внутри страны, например при возникновении межнациональных конфликтов;

- возрастание объема и сложности и новизны мероприятий по управлению подсистемами и элементами ТКС ОГУ в условиях формирования новой государственности;
- расширение сети совместных предприятий и учреждений (с наличием российских и зарубежных партнеров), участвующих в управлении экономикой страны, создающей благоприятные условия для широкого использования как технических средств передачи, обработки и хранения информации, так и технических средств разведки;
- повышение значения факторов времени, высокой оперативности, скрытности управления, обоснованности принимаемых решений при организации связи и обеспечении обработки и защиты информации;
- расширение круга лиц, участвующих в обработке информации, и существенное повышение вероятности угроз со стороны обслуживающего персонала;
- необходимость улучшения централизованного использования всех ресурсов ТКС ОГУ и ее подсистем, в т.ч. обеспечивающих безопасность информации;
- наличие объективных недостатков, в частности демаскирующих признаков, значительных стоимостных, временных, массогабаритных затрат, чувствительностью к различным воздействиям средств поражения и технических средств разведки вероятного противника (ТСР).

Важно отметить те специфические демаскирующие признаки ТКС ОГУ, которые снижают как защищенность сведений о самой системе, так и защищенность информации, циркулирующей в ней. К ним относятся

- принципы организации конфиденциальной связи, и особенно засекречивающей специального назначения, отражающие особенности структурного построения органов управления, которые обеспечиваются связью;
- использование на всех линиях специальных подсистем ТКС ОГУ аппаратуры засекречивания (АЗ) гарантированной стойкости, различной по техническим характеристикам почти для каждого из министерств (ведомств);
- использование в подсистемах связи и обработки информации специального назначения нетиповых средств;

- организация засекреченной связи во всех звеньях управления с использованием радиоизлучающих средств;
- отличие в принципах использования АЗ на линиях специальных систем обработки информации и системы связи Министерства обороны;
- использование на начальном этапе создания ТКС ОГУ разнотипных, в зависимости от ведомственной принадлежности, средств обработки, обладающих различными скоростями передачи информации;
- применение на центрах и узлах связи специфических средств активной некриптографической защиты линий связи и др.

Следовательно можно сделать вывод, что при функционировании ТКС ОГУ и ее компонентов резко возрастает вероятность случайного или злоумышленного воздействия на обрабатываемую информацию и саму систему. Это обусловлено, с одной стороны, возрастанием количества вероятных КНПИ, а с другой – возрастанием интереса к обрабатываемой информации с целью нанесения экономического или иного ущерба, получения информации по приоритетным научным разработкам, перспективам экономического и военного развития страны и др.

Приведенные результаты анализа качественных изменений и особенностей создания и развития ТКС ОГУ требуют дополнительного решения проблемы обеспечения и контроля информационной безопасности на всех этапах жизненного цикла как самой системы в целом, так и ее подсистем (отдельных элементов в частности) на качественно новом уровне. При этом новые тенденции в построении информационно-телекоммуникационных систем и их компонентов в значительной мере определяют большое разнообразие проблем и специфику обеспечения информационной безопасности. С учетом больших масштабов использования ТКС ОГУ в социально-экономических процессах страны даже незначительное повышение эффективности решения отдельных вопросов защиты информации в элементах информационной системы даст значительный народнохозяйственный эффект.

Анализ существующих взглядов, подходов, концепций обеспечения достоверного, своевременного и полного контроля информационной безопасности позволил выявить неоднозначность как самого понимания проблемы, так и недостаточную полноту их теоретической проработки, систематизации знаний по вопросам комплексного контроля безопасности информации в рамках телекоммуникационных систем органов государственного управления.

В качестве первоочередного этапа на пути разработки методов комплексного контроля безопасности информационной предполагается проведение анализа объектов защиты информации и современного состояния проблем контроля информационной безопасности ТКС ОГУ.

Глава 2.
Объекты защиты информации в телекоммуникационных системах органов государственного управления. Анализ основных закономерностей

Важной составляющей проведения анализа объектов защиты информации является выявление объективных условий, закономерностей процесса функционирования подсистемы управления ТКС ОГУ и ее компонентами в условиях воздействия различных угроз, в т.ч. ТСР. Это позволит в дальнейшем определить возможности угроз информационной безопасности, в т.ч. воздействий ТСР по добыванию информации, циркулирующей ТКС ОГУ, и осуществить анализ направлений обеспечения её информационной безопасности.

Рассмотренные в предыдущем параграфе особенности построения и функционирования ТКС ОГУ и ее компонентов, позволяют сделать вывод об их определяющем значении для формирования информационной сферы, а также основных направлений и видов информационной деятельности личности, общества и государства.

Наряду с выполнением основной функции – обеспечения доставки информации с заданным качеством должностным лицам органов государственной власти, ТКС ОГУ должны будут обеспечивать предоставление услуг служб электросвязи для различных категорий пользователей, в т.ч. коммерческих и других предпринимательских структур, а также обеспечение информационного взаимодействия с должностными и другими лицами за пределами страны, в т.ч. через сеть Internet. Это предполагает установки дополнительных технических средств и систем обработки информации, что, в свою очередь, повлечет дополнительные затраты ресурсов, поэтому возникает задача оценки эффективности представления различных услуг ТКС.

В силу этого развитие и совершенствование ТКС ОГУ является сложной системной задачей, решение которой будет определяться выделенными материальными, энергетическими и информационными ресурсами, что требует оценки их распределения между отдельными отраслями в государстве. Это предполагает рассмотрение ТКС ОГУ и ее компонентов как подсистемы управления социально-экономическими процессами, военными, техническими системами в стране. С учетом этого вполне обосновано применение системных методов в рамках сферы и направлений применения ТКС ОГУ. При этом целесообразно выделить прогнозирование развития, перспективное планирование, проектирование и принятие управленческих решений. Выделение этих сфер условно, т.к. в общем случае принятие решения охватывает и прогнозирование, и

планирование, и техническое проектирование на уровне разработки крупномасштабных проектов. Однако возрастание в настоящее время значимости прогнозирования и перспективного планирования, необходимость непрерывного проведения работ, обеспечивающих уточнение прогнозов и перспективных планов развития ТКС ОГУ на различные периоды, приводит к целесообразности выделения проблем прогнозирования и перспективного планирования в отдельную сферу.

Известно, что наиболее явное применение системных методов проявляется в сфере управленческих решений. Так, рост объемов управленческой информации привел к поиску новых методов и средств управления. Научно-технический прогресс и связанный с ним рост новых информационных технологий обеспечивает расширение межотраслевых связей, увеличение сложности выпускаемых изделий, быструю смену оборудования и технологий. Все это в совокупности с требованиями получения максимального экономического эффекта приводит к тому, что часть задач управления не всегда решается с достаточно глубокой проработкой, а часть задач не успевают поставить. Это происходит потому, что сама постановка задачи требует привлечения большого числа специалистов различных предметных областей знаний, между которыми должно быть организовано взаимодействие и взаимопонимание. Организация такого взаимодействия, понимания и принятия решения невозможна без применения методов системного анализа, без разработки и применения систем сбора, первичной обработки и хранения информации на основе использования новых информационных технологий (НИТ).

Кроме того, необходимость использования системных методов при создании, разработке модернизации комплексов технических средств обработки и защиты информации обусловлена внедрением новых материалов, микропроцессорных технологий, принципов построения систем передачи и обработки информации. Это увеличивает число возможных вариантов реализации как отдельных элементов и устройств, так компонентов ТКС ОГУ в целом, что требует больших затрат времени и людских ресурсов на проработку проектных решений и работ, выдвигает необходимость решения задачи автоматизации проектирования и модернизации. Последняя задача связана с формализацией процесса проектирования и разработки технических комплексов, выработкой научно обоснованных способов организации связи.

В рамках рассмотрения основных задач системного подхода в исследовании проблемы и задач разработки методов комплексного контроля безопасности информации систематизируем и сформируем основной понятийный аппарат, относящийся к ТКС ОГУ.

Для рассмотрения основных задач системного подхода введем определения и понятия, которые необходимы при рассмотрении системы управления. При этом центральное место в общей теории систем уделяется выявлению природы систем, т. е. информации, сведениям о ее структуре, функциях и свойствах.

Проанализируем известные определения «системы» с целью выбора наиболее адекватного по содержанию для ТКС ОГУ.

Определение 1. Система есть нечто целое и выражает факт существования, целостность, а двоичное суждение, $H(1, 0)$, отображает наличие или отсутствие этих качеств, $S = H(1, 0)$.

Определение 2. Система есть организационное множество: S = (ОРГ, М), где М – множество; ОРГ – оператор организации.

Определение 3. Система есть множество вещей, свойств и отношений между ними: $S = (\{m\}, \{n\}, \{r\})$.

Определение 4. Система есть множество элементов e, образующих структуру *ST* и обеспечивающих определенное поведение *BE* и в условиях окружающей среды *E*: $S = (e, ST, BE, E)$.

Определение 5. Система есть множество входов *X*, множество выходов *G*, множество состояний *s*, характеризуемых функцией переходов *d* и функцией выходов *L*: $S = (X, G, s, d, L)$.

Определение 6. Система – это многочленное определение, оперирует понятиями модели *F*, связи *SC*, пересчета *R*, самообучения *FL*, самоорганизации *FO*, проводимости связей *CO* и возбуждения моделей *IN*: $S = (F,SC,R,FL,FO,CO,IN)$

Определение 7. Система есть множество входов, множество выходов, множество состояний, характеризуемых функцией переходов и функцией выходов с учетом факторов времени и функциональных связей: $S = (T, X, G, s, f, V, n, \varphi)$, где T – время; X – входы; G – выходы; s – состояния; f – класс функций на выходе; V – значения функций на выходе; n – функциональная связь в уравнении $q(t_2) = n[x(t_1), s(t_1), t_2]$; φ – функциональная связь в уравнении $s(t_2) = \varphi[x(t_1), s(t_1), t_2]$.

Определение 8. Система есть множество, учитывающее цели и планы *PL*, ресурсы внешние *RO* и ресурсы внутренние *RI*, исполнителей *EX*, процесс *PR*, помехи *DT*, контроль *SV*, управление *RD*, эффект *EF*:

$$S = (PL, RO, RI, EX, PR, DT, SV, RG, EF).$$

Анализ этих определений системы позволяет заключить, что на разных этапах жизненного цикла ТКС ОГУ применимы различные определения. Так, определения 5 и 7 можно использовать в теории автоматического управления, в т.ч. и для рассмотрения

автоматизированных систем управления ТКС ОГУ. Наиболее удобным для организационных систем, в т.ч. для ТКС ОГУ, является определение 8, однако на различных этапах функционирования ТКС ОГУ это определение может изменяться.

В ходе создания, исследования и развития ТКС необходимо выделить ряд существенных факторов: наличие реальной цели по обеспечению конфиденциальной связи и информации заданного качества; реальные запросы пользователей на обеспечение конфиденциальной связи и информации (КСИ) и возможности ТКС; качество подготовки обслуживающего персонала, процесса организации КСИ и обеспечения ее безопасности; внешние воздействия ТСР и различных помех; влияние контроля на качество КСИ, управления процессом организации, обеспечения КСИ и защищенности информации ИСКС; учет затрат ресурса в соответствии с требуемой степенью информационной безопасности.

Определение ТКС ОГУ как системы, раскрывающее представление о системе, характеризующее её строение и особенности функционирования, по нашему мнению, наиболее удачно с точки зрения обобщенной системы.

Система есть множество элементов (вещей), свойств и отношений между ними: $S = (\{m\}, \{n\}, \{r\})$.

Использование этого определения позволяет описать процессы функционирования ТКС ОГУ как сложных систем, в т.ч. систем управления процессами обработки информации и обеспечения информационной безопасности на различных этапах жизненного цикла в зависимости от их внутреннего состояния, внешних воздействий, выделить такие характерные свойства и закономерности, как устойчивость, поведение, равновесие, целостность, бесконечность, интегративность, иерархичность, коммуникативность и др.

С учетом рассмотренных характеристик и свойств ТКС ОГУ можно сделать вывод, что ТКС ОГУ и ее компоненты, представляющие совокупность взаимосвязанных и взаимодействующих элементов, выполняющих определенные функции, объединенных единой целью, являются системой в силу соответствия следующим основным признакам:

- наличие цели функционирования, определяющей назначение ТКС ОГУ;
- устойчивость, непрерывность, оперативность и разведзащищенность управления ТКС ОГУ, представляющей систему организационно-технического, социально-экономического типа;

- наличие управления как особого вида деятельности, заключающегося в воздействии на систему в соответствии с поставленными целями и обстановкой;
- наличие потоков информации управления и состояний;
- наличие большого количества взаимосвязанных и взаимодействующих элементов;
- взаимодействие с внешней средой;
- иерархичность структуры (первичные сети связи, подсистемы радио-, радиорелейной, проводной, конфиденциальной связи и др.);
- динамичность системы – непрерывное изменение состояний и количества элементов.

Анализ рассмотренных свойств ТКС ОГУ позволяет заключить, что она обладает всеми чертами, позволяющими отнести ее к классу больших и сложных систем [11, 12]. В качестве формальных признаков сложной системы используются число взаимосвязанных элементов; отсутствие формальной математической модели функционирования; способы описания. Понятие больших систем в значительной степени перекликается с понятием сложной системы.

Исходя из этого, российский ученый Г.Н. Пивоваров выделяет (в зависимости от количества элементов) четыре класса систем: *малые* — 10–10^4 элементов; *сложные* — 10^4–10^7 элементов; *ультрасложные* — 10^7–10^{30} элементов; *суперсистемы* — 10^{30}–10^{200} элементов. В силу того, что понятие элемента системы определяется относительно задач и целей исследования, определение сложности является понятием относительным.

Согласно точке зрения английского кибернетика С. Бера простые и сложные системы определяются способом описания: детерминированный или теоретико-вероятностный. Российский ученый А.И. Берг определяет сложную систему как ту, которую можно описать не менее чем на двух математических языках.

Наиболее приемлемым определением сложной системы для исследуемой предметной области является определение, учитывающее следующие признаки:

- наличие большого количества взаимосвязанных и взаимодействующих между собой элементов;
- сложность функции, выполняемой системой и направленной на достижение заданной цели функционирования;

– возможность разбиения системы на подсистемы, цели которых подчинены общей цели системы;

– наличие управления, разветвленной информационной сети и интенсивных потоков информации;

– наличие взаимодействия с внешней средой и функционирования в условиях воздействия случайных факторов.

Такая же ситуация имеет место и в определении понятия большой системы. С появлением и развитием автоматизированных систем управления (АСУ) под понятием большой системы предложено понимать совокупность материальных и человеческих ресурсов; средств преобразования, передачи и обработки информации; операторов, занятых в обслуживании этих средств; руководителей, наделенных правами и ответственностью принимать решения, объединенных с помощью некоторой системы взаимосвязей для достижения общей цели или группы целей.

Однако такой подход в определении значительно сужает класс больших систем, исключая транспортные, телефонные сети большой емкости и др., поэтому (в силу отсутствия четкого определения) отнесение системы к разряду больших является в значительной мере условным и связано в основном с ролью комплексных общесистемных вопросов. Это обстоятельство зависит как от свойства самих систем, так и от тех задач, ради решения которых разрабатывается система.

Анализ свойств больших и сложных систем, понятий, характеризующих их строение и функционирование, позволяет утверждать, что ТКС ОГУ и такой ее компонент как система администрирования и контроля БИ, являются сложными системами. Доказательство – характерные признаки, свойства и закономерности функционирования ТКС и ее составных частей.

Во-первых, сложность ТКС является свойством системы (сложность системы), а во-вторых – свойством системных задач (сложность задач, вычислительная сложность). При этом независимо от типа сложности можно выделить два принципа оценки сложности ТКС.

Первый принцип оценки сложности системы. Сложность системы управления пропорциональна объему синтаксической информации, необходимой для описания этой системы.

Одним из способов описания такой дескриптивной сложности является оценка числа элементов, входящих в систему (переменных, состояний, компонентов), разнообразия взаимоотношений между элементами, свойств, характеризующих сложность системы. И одним из способов описания такой дескриптивной сложности является оценка числа

элементов, входящих в систему (переменных, состояний, компонентов) и разнообразия взаимоотношений между ними.

Тогда, если X – множество всех систем определенного эпистемологического уровня, $P(X)$ мощность множества X, а C_x – мера дескриптивной сложности на множестве X, то C_x – это функция

$$C_x: P(X) \to R, \qquad (1.3)$$

обладающая следующими свойствами: **C1**, если $C_x(0) = 0$; **C2**, если $A < B$, то $C_x(A) < C_x(B)$; **C3**, если A – гомоморфный образ B, то $C_x(A) \subseteq C_x(B)$; **C4**, если A изоморфно B, то $C_x(A) = C_x(B)$; **C5**, если $A\ B$=0, 2) A и B не взаимодействуют друг с другом, A и B не являются гомоморфными образами друг друга, то $C_x(A \cup B) = C_x(A) + C_x(B)$.

Из свойств С1 и С2 следует, что сложность ТКС характеризуется неотрицательным числом. Свойства С2 и С3 связаны с монотонностью системы, которая подтверждает, что сложность ТКС не должна возрастать при сокращении множества систем и элементов ТКС или менее детальном их рассмотрении. Условие С4 показывает, что сложность системы не изменяется, если переобозначить некоторые произвольные элементы заданных систем, а все остальные не изменять. Свойство аддитивности С5 подтверждает, что суммарная сложность равна сумме сложностей при объединении двух множеств систем, не имеющих никаких общих компонентов.

Второй принцип оценки сложности системы. Сложность ТКС ОГУ и ее компонентов пропорциональна объему синтаксической информации, необходимой для разрешения любой нечеткости системы. В данном случае имеется в виду оценка количества синтаксической информации, основанной на вероятностной мере нечеткости, называемой шенноновской энтропией: $H(X) = -\sum_{i=1}^{N} p_i \log p_i$, где N – мощность множества событий X, связанных с нечеткостью системы; p_i – вероятности наступления событий множества X.

К свойствам, характеризующим сложность системы, относятся неотрицательность числа элементов; монотонность системы, которая подтверждает, что сложность системы управления не должна возрастать при сокращении множества систем и элементов системы или менее детальном их рассмотрении; неизменность сложности системы при переобозначении некоторых произвольных элементов заданных систем без изменения всех остальных; аддитивность, подтверждающая, что суммарная сложность равна сумме сложностей при объединении двух множеств систем, не имеющих никаких общих компонентов.

Результаты проведенного анализа предназначения ТКС ОГУ и ее компонентов, а также характеристик, требований и показателей эффективности функционирования подтверждают сложность исследуемой ТКС ОГУ. Они позволяют уточнить структуру элементов, способы организации, выявить наиболее существенные пассивные и активные воздействия. К ним относятся климатические, гидрометеорологические, физико-географические условия; активные, целенаправленные воздействия на ТКС, оказываемые взаимодействующими и противоборствующими системами; складывающаяся электромагнитная обстановка (ЭМО); наличие собственных сетей связи для организации взаимообмена каналами и потоками сообщений, информацией, сигналами оповещения и др.; обработка исходных данных, их передача (прием) для совместного планирования связи.

Особое внимание при решении вопросов обеспечения информационной безопасности — на активное воздействие на ТКС ОГУ противоборствующих систем за счет применения различных видов поражения, средств радиоэлектронного подавления (РЭП).

Обоснованным подтверждением сложности ТКС ОГУ является анализ закономерностей построения и функционирования системы управления ТКС по обеспечению информационной безопасности.

Очевидно, что эффективность исследуемой системы определяется качеством управления, которое может быть обеспечено современными средствами автоматизации.

Понимая под управлением целенаправленный процесс обработки информации с целью обеспечения заданного ее качества, в т.ч. обеспечения информационной безопасности [13-15], можно выделить тройку, внутри которой образуется процесс управления: объект *Y*, среда *K*, субъект *X*. (рис. 1).

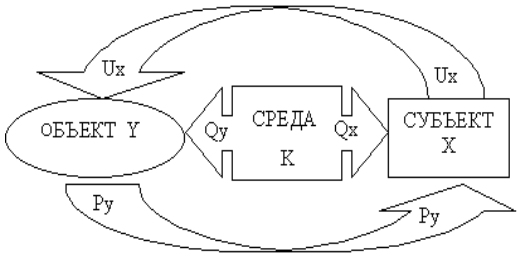

Рис.1. Структура процесса управления

Здесь на субъект *X* воздействует среда *K* и объект *Y*, а управление представляет организованное воздействие субъекта U_x на объект с учетом воздействия на него среды Q_x и объекта P_y, а также воздействия среды на объект Q_y. Управление строит субъект на оптимизации своих потребностей $A = (a_1, a_2, \ldots, a_i)$, где a_i – состояние i-й потребности субъекта, которая выражается неотрицательным числом, характеризующим насущность, актуальность этой потребности. В ходе управления субъект решает задачу многокритериальной оптимизации своих потребностей при условиях минимизации имеющегося у него ресурса и максимальном учете информации о воздействиях J_{Qx}, J_{Qy}, J_{Ux}, J_{Py}, среды, субъекта и объекта, соответственно, а также информации о состоянии объекта J_y и субъекта J_x:

$$\text{opt } a_i(X, U) \rightarrow \min_{r \in R} (i = 1, 2, ..., k), \mid \max J_{Qx}, J_{Qy}, J_{Ux}, J_{Py}, J_K, J_y, J_x, \qquad (1.4)$$

где *R* – информационные ресурсы субъекта.

Рассмотренная зависимость выражает неизвестную, но существующую связь потребностей с состоянием среды *X* и поведением *U* субъекта и зависимость эффективности управления от информации.

Если считать, что U_X – решение задачи, то способ решения задачи, позволяющий получить это решение, будет называться алгоритмом управления $U_X = f(A_t, X)$, где *f* – алгоритм синтеза управления по состоянию среды *X* и потребностей A_t, которые изменяются как под влиянием среды и объекта, так и самостоятельно, в ходе жизнедеятельности субъекта. Эффективность функционирования субъекта в конкретной среде определяется алгоритмом управления *f*, который имеет рекуррентный характер: $U_{N+1} = f(U_N, A_t, X)$, т. е. позволяет улучшать управление на каждом шаге, уменьшая уровень своих потребностей $U_{N+1} = f(U_N, A_t, X)$, $A_t(X, U_{N+1}) < A_t(X, U_N)$. Рассмотрение процесса управления как организации целенаправленного осознанного воздействия на объект, обеспечивающего удовлетворение потребностей субъекта, требует разделения алгоритма управления на два этапа:

этап 1 – формулировка, выбор цели управления, осуществляемой человеком на интуитивном уровне, $Z = f_1(X, A_t)$, где f_1 – алгоритм синтеза цели *Z* по потребностям субъекта A_t и состоянию среды *X*;

этап 2 – определение управляющего воздействия, реализация которого обеспечивает достижение цели, приводящей к удовлетворению потребностей субъекта, $U_x = f_2(Z, X)$, где f_2 – алгоритм определения и реализации управляющего воздействия.

Тогда в общем виде управление будет представлять собой изменение состояния объекта, системы или процесса, ведущее к достижению поставленных целей. Разделение процесса управления на два этапа и выделение двух различных функций позволяет выделить и различные

структурные элементы управления, реализующие эти функции. Первую функцию выполняет субъект, а вторую – управляющее устройство. Управляющее устройство и объект представляют систему управления, выполняющую функцию реализации целей управления, формируемых субъектом (рис. 2).

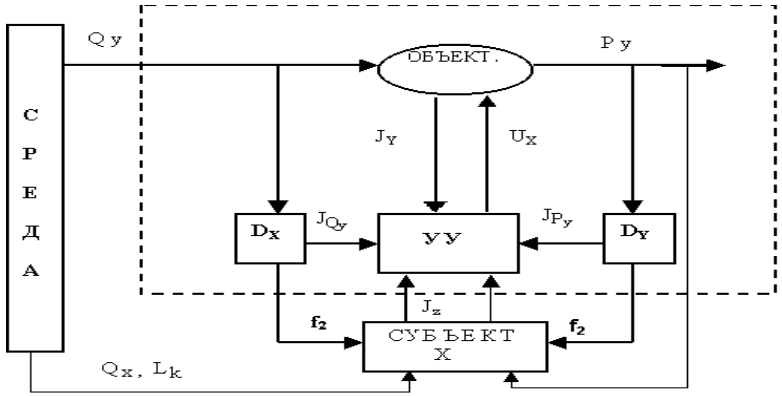

Рис. 2. Структура системы управления

Рассматриваемая структурная схема системы управления наглядно демонстрирует информационный характер управления. Здесь выработка команды управления осуществляется на основе исходной информации J, формируемой из данных о состоянии среды и объекта, $J = \{X', Y'\}$, а сама команда управления U, вырабатываемая устройством управления, представляет не что иное, как информацию о том, в какое положение должны быть приведены управляемые входы объекта. Очевидно, управление U есть результат работы алгоритма $U = f_2 (J, Z)$. Управление (в широком смысле) может быть представлено множеством $\{Z, J, U, f_2\}$.

В общем виде процесс управления будет включать следующие этапы: получение информации о задачах управления, формируемых на основании целей субъекта (J_z); получение информации о результатах управления, представляющих характеристику поведения объекта управления (J_y); получение информации о состоянии среды (J_k); анализ информации и выработка решения ($J = \{J_{Qy}, J_{Py}, J_K, J_y, J_x, J_z\}$); осуществление управляющих воздействий (исполнение решения) (U_x).

Таким образом, содержание рассмотренных этапов показывает, что процесс управления имеет информационный характер и представляет целенаправленный процесс переработки информации, т. е. информационный процесс. Его содержание включает сбор информации о

ходе процесса, передачу информации в пункты накопления и переработки, анализ поступающей, накопленной и справочной информации, принятие решения на основе результатов анализа информации, выработку соответствующего управляющего воздействия и доведение его до объекта управления. Эти фазы управления протекают во взаимодействии с окружающей средой при воздействии различных помех. При этом цели, принципы и границы такого процесса управления зависят от сущности решаемой задачи. В общем виде информационный характер управления можно представить этапами информационного процесса управления (табл. 1). Здесь необходимо отметить, что рассматриваемому информационному процессу, как и любому процессу управления, присущ ряд углубляющих его содержание определений.

Таблица 1. Этапы информационного процесса управления

Этапы управления	Этапы информационного обеспечения		
	Сбор информации	*Анализ и синтез*	*Выбор критериев, оценка альтернатив*
Подготовка к принятию решения	Поиск и отбор информации	Формулировака задач, выделение путей решения	Формирование дерева целей объекта и субъекта управления
Принятие решения	Оценка информации и ее аналитическая обработка	Формирование множества альтернатив	Определение ограничений, выбор критериев, оценка альтернатив
Организация исполнения, контроль результатов	Поиск дополнительной информации и ее оценка	Создание моделей решения задач управления	Оценка стратегий и условий реализации практических решений

Цели (задачи управления):

- поддержание некоторого желаемого состояния объекта (системы) при воздействии на него различного рода возмущающих воздействий;
- поддержание заданной степени материального или духовного комфорта членов общества при решении задач развития его экономики и культуры;

– определение такого режима работы предприятия, организации и других систем организационно-технического типа, при котором достигается максимум выпускаемой им продукции (или минимум себестоимости этой продукции и т. д.).

Важной составляющей процесса управления в системах организационно-технического типа является принятие решения. Проблема принятия решения возникает только тогда, когда существует затруднение в достижении какой-либо цели. В ходе решения задач управления проблемы могут изменяться: терять свою актуальность и сложность или прекращать свое существование; простые вопросы и задачи, вызывая определенные сложности в их решении, становятся проблемами, требующими решения; решение задач в условиях возникновения особых внешних воздействий и обстоятельств, изменений ситуаций во внешней среде приводит к возникновению актуальной проблемы; наличие ряда разнообразных проблем приводит к возникновению проблемы или необходимости решения задачи выбора из различных возможностей, направленных на достижение желаемой цели.

Таким образом, желание или необходимость достижения определенной цели может либо привести к проблеме, либо нет. В таких случаях принято считать: проблемы нет, когда достижение цели осуществляется вполне очевидными для данных условий действиями и не вызывает никаких затруднений; проблема есть, когда для достижения цели необходимо преодолеть определенные затруднения или решить задачи выбора или нахождения наилучшего действия из всех возможных; решить проблему – значит найти средство и методы, обеспечивающие реализацию различных управляющих воздействий для достижения заданной цели.

Процесс (объект) называется управляемым, если среди множества воздействий на него имеется такое, которое позволяет добиться поставленной цели.

В развернутом виде содержание управления включает следующие этапы: определение объекта управления; формирование целей; структурный синтез модели управления: определение внешней структуры, декомпозиция и определение внутренней структуры модели; идентификация параметров модели объекта – определение числовых значений параметров системы в режиме нормального функционирования объекта; планирование эксперимента, синтез плана эксперимента, позволяющего с максимальной эффективностью определить искомые параметры модели объекта управления; синтез управления – принятие решения о выборе способов решения задачи оптимального управления; реализация управления или отработка в объекте оптимального решения

полученного на предыдущем этапе; адаптация – коррекция, связанная с подстройкой этапов.

В зависимости от выбора этапа коррекции бывают различные виды управления: *адаптивное* – коррекция параметров модели; *дуальное* – применение специальных мер планирования эксперимента путем добавления специальных тестовых сигналов (осуществляется при невозможности управления обеспечить необходимое разнообразие входа объекта для эффективной коррекции параметров модели); *эволюционное* – коррекция структуры модели в соответствии с новой информацией, коррекция границ раздела объекта и среды; *целевое* – коррекция всего множества целей управления.

Система управления представляет собой совокупность взаимодействующих между собой объекта управления (ОУ) и управляющего органа (УО) соответствующей иерархической или иной структуры, соединенных прямыми и обратными связями для достижения заданной цели управления.

С учетом этого в более общем виде система управления может решать следующие задачи: стабилизации системы – поддержание выходных величин системы управления вблизи некоторых заданных значений в условиях воздействия помех; выполнения программы – реализация изменений во времени заданных значений управляемых величин в соответствии с заранее известным способом; слежения – реализация заранее неизвестных изменений заданных значений управляемых величин в зависимости от значений других величин; оптимизации управления – выполнение наилучшим образом поставленной перед системой задачи при заданных реальных условиях и ограничениях.

Как и любая система, исследуемая система управления может функционировать в условиях внешних антагонистических воздействий, физико-географических воздействий окружающей среды и взаимодействующих систем. Реализация цели управления заключается в поддержании заданного состояния ОУ и выполнения им определенной программы по изменению состояния самих УО или внешней среды при ее постоянном воздействии на систему.

Цикл управления характеризуется временными интервалами информационных процессов управления по следующим этапам:

этап 1 – время сбора, выработки информации (И) о состояния ОУ, $t_{вн}$;

этап 2 – время передачи информации в УО по системам коммуникаций организационного (человек–человек), организационно-технического (человек–машина) и технического (машина–машина) типа (в т.ч. телекоммуникаций), $t_{пи}$;

этап 3 – время сбора и обработки информации УО о состоянии ОУ, $t_{сб}$;

этап 4 – время принятия решения, выработка информации управления, $t_{пр}$;

этап 5 – время доведения информации управления в виде приказа, команды, директивы до ОУ, $t_{пз}$;

этап 6 – время перехода ОУ в новые состояния, $t_{пнс}$.

Таким образом, возникают два встречных потока информации состояний и управления, передаваемых системой коммуникации.

В цикле управления объект управления, находящийся в различных ситуациях, является источником информации о своем состоянии, производительность которого может быть выражена через число состояний (N), принимаемых объектом в единицу времени, $H_{max} = \log N$. Эта информация через систему коммуникации передается в УО для обработки и принятия решения. Результатом сбора и обработки информации о состоянии объекта управления является решение лица, принимающего решение, проявляющееся в виде потока информации управления, $H_{my} = \log N$, зависящего от числа состояний (N'), принимаемых УО в единицу времени.

Для функционирования системы управления требуется минимально необходимое количество информации, $H_{кр}$. Однако в процессе ее передачи и обработки в системе коммуникации всегда существуют условия, приводящие к потере некоторого количества информации (h_y) за счет отказов средств, помех, потерь, утечки и т. д. Информация в процессе управления должна быть передана за время меньшее, чем время ее старения, $t_{пер} < t_{стар}$. Тогда условия функционирования системы управления можно представить через потоки информации в контуре управления:

$H \geq H_{кр}$ – система управления функционирует нормально;

$H < H_{кр}$ – система управления перестает функционировать.

Величина h_y не должна превышать некоторой доступной величины $h_{доп}$. Тогда большая эффективность будет у той системы управления, в которой система коммуникации имеет меньше h_y.

Таким образом, можно сделать следующие выводы:

- системы управления и их системы коммуникации, в т.ч. ТКС ОГУ, являются информационными системами;
- система коммуникации является составной частью системы ОГУ, ее материально-технической частью;

- для нормального функционирования системы управления необходимо выполнить следующие условия:

$$\begin{cases} H \geq H_{кр} \\ t_{пер} < t_{стар} \\ h_y < h_{доп} \end{cases} \quad (1.5)$$

- эффективность системы коммуникации как составной части системы управления определяется свойствами системы коммуникации, обеспечивающей передачу необходимого количества информации в заданное время.

ТКС ОГУ и ее компоненты являются наиболее уязвимыми звеньями в системах управления социально-экономическими, политическими, военными и другими процессами, так как через них наносится ущерб. Учитывая рассмотренные особенности управления, можно заключить, что специфика ТКС и обеспечение ее информационной безопасности будет зависеть от внутреннего строения, природы образующих элементов и компонентов, характера их взаимодействия.

К основным задачам, решаемым органами управления ТКС по обеспечению информационной безопасности, можно отнести:

- планирование и организация комплексной защиты;
- выявление и устранение демаскирующих признаков ТКС ОГУ, нарушений безопасности информации при организации связи, эксплуатации средств связи и ЭВТ, проведении испытаний новых технических средств передачи, обработки и хранения информации;
- сбор, обработка и хранение информации по выявлению демаскирующих признаков и нарушений информационной безопасности и ее составляющих, выдача этой информации по запросам должностных лиц;
- предотвращение вероятных угроз и закрытие возможных каналов утечки информации, обрабатываемой в ТКС ОГУ;
- организацию взаимодействия с оперативными подразделениями органов безопасности, вооруженных сил, Министерства внутренних дел по обеспечению информационной безопасности;
- разработку предложений по совершенствованию системы комплексной защиты ТКС ОГУ и повышению степени их информационной безопасности;

– обеспечение комплекса организационных и технических мероприятий по обеспечению информационной безопасности;
– контроль обеспечения информационной безопасности и др.

Глава 3.
Анализ угроз безопасности информации в телекоммуникационных системах органов государственного управления

3.1. Анализ закономерностей функционирования телекоммуникационных систем органов государственного управления и их компонентов, обусловливающих угрозы безопасности информации

Основными особенностями и условиями функционирования ТКС ОГУ являются следующие:

– функционирование и развитие современных информационных систем различных классов (в т.ч. ТКС ОГУ и ее компонентов) требует организации и обеспечения сложного организационно-технический механизма;
– на всех этапах жизненного цикла ТКС ОГУ функционируют на значительной территории, в различных физико-географических условиях, постоянных и стохастических, естественных и искусственных, преднамеренных и непреднамеренных внешних, внутренних воздействиях и факторах, в чрезвычайных условиях и ситуациях внутри страны, которые могут привести к угрозе информационной безопасности самой ТКС ОГУ и обрабатываемой в ней конфиденциальной информации;
– внутренние воздействия, обусловлены рядом особенностей функционирования системы, в т.ч. надежностью ее элементов, воздействием обслуживающего персонала, внешние – физико-географическими условиями, взаимодействующими системами, а также противодействующими системами;
– противодействующие системы представляют воздействия злоумышленников, преследующих цель воздействия на ТКС ОГУ и информацию в ней для получения конфиденциальных сведений или их изменения (в т.ч. уничтожения) любыми способами и средствами. Рассматриваемые воздействия могут быть пассивного или активного характера;
– наиболее существенными пассивными воздействиями, определяющими особенность структурно-функционального построения ТКС ОГУ, являются климатические, гидрометеорологические, а также физико-географические условия;

– к отрицательным воздействиям взаимодействующих систем можно отнести взаимные помехи и некачественное планирование вопросов обеспечения электромагнитной совместимости радиоэлектронных средств; некачественный обмен сигналами взаимодействия; большие потоки взаимной информации; некачественное использование систем и средств обеспечения телекоммуникациями; нескоординированные виды деятельности и др.;

Рис. 3. Модель функционирования телекоммуникационной системы органа государственного управления в условиях воздействия угроз

– активное, целенаправленное воздействие на ТКС ОГУ оказывают противоборствующие системы, к которым можно отнести оружие массового поражения (ОМП); высокоточное оружие (ВТО); разведывательные ударные комплексы (РУК); средства радиоэлектронной борьбы (РЭБ), радиоэлектронного подавления (РЭП), технической разведки (ТСР); обычное вооружение; другие виды деятельности противоборствующих систем.

Таким образом, в наиболее общем виде функционирование ТКС ОГУ с учетом активных воздействий можно представить моделью (рис. 3).

3.2. Особенности сигналов, обрабатываемых на объектах телекоммуникационных систем органов государственного управления

Функциональное предназначение, особенности и несовершенство технологии разработки комплексов ТСОИ ТКС ОГУ, отдельных их образцов и элементной базы определяют особенности сигналов, циркулирующих в технических средствах. Основу большинства ТСОИ составляет радиоэлектронная аппаратура, физическими носителями информации в которой являются электрические сигналы различной формы и параметров (дискретные и непрерывные, детерминированные и случайные, широкополосные и узкополосные, и т.д.), изменение которых во времени соответствует переданному сообщению. Особенностью этих сигналов является то, что они обеспечивают перехват и обработку различных видов конфиденциальной информации и сведений непосредственно от источников без дополнительных сложных преобразований и в реальном масштабе времени. К таким видам информации относятся речевая, телеграфная, телекодовая, телевизионная, факсимильная и др. Исходя из этого, формируются и единые критерии защищенности, методы передачи, обработки, хранения информации. Анализ характеристик и показателей таких видов информации и их сигналов [16–18] позволил выделить наиболее значимые и выявить ряд их особенностей:

– в силу своей физической сущности речевые сигналы являются многопараметрическими, что обусловливает относительную простоту их преобразования в электромагнитные сигналы, которые отражают как содержание конфиденциальной информации, так и факт ее обработки, являясь демаскирующими признаками;

– обусловливает доступность электрических сигналов техническим средствам перехвата, в т.ч. радио- и радиотехнической разведкой (РРТР);

- относительная простота формирования телеграфных сигналов, обусловливающая их перехват ТСР;
- зависимость перехватываемых телеграфных сигналов (длительность, амплитуда, ширина спектра сигнала) от формы сигнала, вида модуляции, вида кода, скорости передачи информации и элементной базы аппаратуры;
- широкочастотная полоса телевизионного сигнала обусловливает ряд гармоник строчной частоты, каждая из которых имеет симметричные боковые полосы, формирующие побочные излучения, а использование высокочастотного оборудования в устройствах обработки сигнала усугубляет паразитные побочные излучения;
- последовательное построчное преобразование в передающем устройстве оптического сигнала в видеосигнал обусловливает наличие демаскирующего признака, содержащего признак начала или конца строки, позволяющего правильно восстанавливать изображение приемным устройством.

Рассмотренные особенности сигналов позволяют системно представить не только процессы преобразования, обработки, передачи информации, но и пути утечки, содержание каналов утечки информации.

Глава 4.
Современное состояние проблемы контроля безопасности информации в телекоммуникационных системах органов государственного управления

С учетом проведенного анализа особенностей, принципов построения и функционирования ТКС и их компонентов, а также в рамках подхода комплексной защиты информации ТКС ОГУ была проведена систематизация проблем обеспечения БИ и выделены те из них, которые (с точки зрения обеспечения комплексного контроля БИ) требуют решения.

4.1. Проблема разграничения доступа и защиты от несанкционированного доступа

Построение и развитие телекоммуникационного компонента ТКС ОГУ базируется на обособленной сети передачи данных первичной сети связи, в т.ч. телефонных сетей, образованных за счет объединения существующих сетей конфиденциальной связи силовых министерств (ведомств) и выделенного ресурса действующей сети Министерства связи России. Кроме этого, предполагается работа системы в многопользовательском режиме. Это обусловливает возникновение проблемы разграничения доступа к общим информационно-вычислительным и другим ресурсам и несанкционированного доступа (НСД) к информации как различных пользователей (абонентов) одного ведомства, так и абонентов разной ведомственной принадлежности, а также обслуживающего персонала. По этой причине задачи обеспечения физической, логической целостности информации, предупреждения несанкционированной модификации, несанкционированного получения и размножения информации остаются актуальными, а с учетом широкого использования новых информационных технологий, требуют (как и сама проблема) дальнейшего решения.

Решение рассмотренных задач может быть выполнено как с учетом традиционных способов повышения достоверности передачи информации в транспортной системе (уменьшение канальных помех, помехоустойчивое блочное кодирование, решающая обратная связь и т.д.), так и нетрадиционными методами комплексной защиты информации (КЗИ) (кодовое зашумление, преобразования Уолша, Радемахера и т.д.). При этом необходимо обеспечить комплексную защиту от всех способов НСД, которые могут осуществляться следующими путями:

- непосредственным обращением к объектам доступа;
- созданием программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

- модификацией средств защиты, позволяющей осуществить НСД;
- внедрением в технические средства вычислительной техники или автоматизированных систем программных или технических механизмов, позволяющих осуществить НСД и др.

Комплексная защита информации от НСД должна включать защиту технических и программных средств от действий субъектов доступа, направленных на ознакомление с информацией, к которой они не имеют права доступа, на её изменение или уничтожение; на дезорганизацию связи; нарушение топологии сети; нарушение штатного набора программных и технических средств и их функций.

При этом должны выполняться следующие требования по КЗИ от НСД:

- управление доступом;
- регистрация и учет всех действий, критичных для БИ в системе и ее компонентах;
- наличие криптоподсистемы, совмещенной с операциями доступа к разным объектам системы, с индивидуальными параметрами доступа субъектов в качестве ключей;
- осуществление контроля целостности программного обеспечения и программных средств с периодическим тестированием алгоритмов функционирования средств восстановления целостности.

Для КЗИ от НСД необходимы также организационные и технические меры:

- физическая охрана средств обработки информации и администрирование системы;
- меры по ограничению доступа в помещения расположения системы;
- комплекс мер по защите помещений пользователей (абонентов).

4.2. Проблема обеспечения информационной безопасности в территориально распределенной системе

Учитывая, что ТКС ОГУ является распределенной системой, размещенной на большой территории и имеющей большое количество пользователей, проблема обеспечения комплексного контроля безопасности БИ в такой сети обусловлена следующими факторами:

- сети связи и включенные в них технические средства доступны большому количеству потенциальных нарушителей;

- сети распределенных вычислительных систем общего пользования отличаются большой динамичностью; кроме того, в них используются различные протоколы связи, позволяющие реализовать различные архитектуры;
- в распределенных сетях вычислительных систем трудно обеспечить четкое управление защитой информации (особенно оперативное) из-за необходимости своевременной обработки огромных потоков быстро меняющейся информации, поступающей от большого количества точек потенциально возможных нарушений;
- действующие сети расширяются недостаточно скоординировано при присоединении к ним новых сетей;
- в силу специфики внутримашинного представления и организации обработки информации в современных ЭВМ возникают сугубо специфические проблемы защиты информации, находящейся на машинных носителях и обрабатываемой средствами ЭВМ;
- широкое использование НИТ в рамках некоторой организационной структуры предопределяет необходимость решения задач правового обеспечения БИ;
- в связи с массовым распространением малых и особенно персональных ЭВМ принципиально меняется содержание технологии обработки информации: если до недавнего времени практически параллельно и в значительной мере автономно существовали традиционная и автоматизированная технологии, то в последнее время обе технологии все органичней сливаются в единую, причем доля безбумажных процессов циркуляции и обработки информации неуклонно возрастает.

4.3. Проблема обеспечения безопасности информации при реализации нетрадиционных для ТКС ОГУ видов информационных услуг

В ТКС ОГУ в ближайшей перспективе, кроме традиционной телефонной, телеграфной и факсимильной связи, планируется реализовать такие формы обслуживания, как передача видеоинформации, теледоступ к банкам данных, высокоскоростная передача файлов и т.д. Отсюда вытекает проблема обеспечения КЗИ по всем видам передаваемых сигналов, что выражается в расширении диапазона побочных электромагнитных излучений и наводок (ПЭМИН) для разноскоростных потоков информации и определяет различие методов шифрования и некриптографической

защиты информации (НКЗИ), а применение абонентского способа шифрования обеспечивает достаточно надежную защиту информации только в линиях связи и не решает проблем защиты связанных, например, с побочными каналами утечки информации (ПКУИ) и НСД на конечных абонентских пунктах. В связи с этим естественно остается проблема их инженерно-технической защиты.

4.4. Проблема специальных исследований на предмет наличия аппаратных и программных закладок

Крупной проблемой при обеспечении информационной безопасности является предполагаемое массовое использование в оборудования иностранного производства [например, АТС «Hicom 3000» (США)] коммутаторов пакетов фирмы «Siemens»(ФРГ), создающее благоприятные условия для злоумышленных действий вероятного противника (например, установки закладных устройств различного типа [19–20]). Контроль наличия таких устройств методом анализа функциональной необходимости элемента в устройстве для таких сложных устройств, как электронная АТС или коммутатор пакетов, представляет собой довольно трудный, а зачастую и нереализуемый процесс из-за возможностей интеграции закладных устройств в современные специализированные большие интегральные микросхемы. Кроме того, современные закладные устройства могут снабжаться механизмом предотвращения срабатывания на контрольные воздействия (счетчиком контрольных воздействий), что существенно затрудняет выявление наличия таких устройств в системах и средствах обработки информации при специальной проверке в процессе сертификации. При этом значительное повышение защищенности информации в пунктах транзита, достигаемое с помощью абонентского шифрования, не исключает такого нежелательного явления, как анализ трафика с помощью закладок, так как при передаче шифротекста адрес может быть открыт в шлюзе или пункте транзита. Перехваты и анализ трафика могут привести к нарушениям в криптосистеме, включая вставки, уничтожение и изменение, воспроизведение адекватного шифротекста и подлог (имитоввод). Все это определяет необходимость применения АЗ, использующей механизм противодействия всем видам имитоввода.

Кроме этого, возможна установка в импортируемых устройствах закладных устройств, ориентированных не на классическую передачу конфиденциальной информации посредством ее записи с последующим излучением (или путем непосредственного излучения), а на создание в сети различных аварийных ситуаций (изменение информации или состояния системы, преднамеренное искажение таблицы маршрутизации в определенные моменты времени). Предварительное выявление закладных устройств такого типа до проявления их действия практически

невозможно, а выявление их после срабатывания уже неэффективно, т.к. даже в единичном случае возможно причинение большого ущерба в зависимости от важности и сложности сложившейся на момент аварии ситуации. Использование импортного программного обеспечения также обусловливает необходимость специальной проверки на отсутствие программных закладок и скрытых функциональных возможностей, но это практически невозможно, т.к. по сложности и трудоемкости такая проверка сравнима с разработкой собственного оригинального программного обеспечения.

4.5. Проблема интегральной оценки защищенности информации при использовании различных средств комплексной зашиты информации

Обеспечение гарантированной защиты информации с использованием всех криптографических, алгоритмических, организационно-технических мер и средств на всех участках ее передачи, обработки и хранения требует проведения научных исследований для установления степени, уровня защищенности информации в системе, разработку критериев и методик оценки защищенности с учетом всех дестабилизирующих факторов.

4.6. Проблема разведзащищенности системы (защиты от демаскирования)

Для передачи основных потоков информации планируется преимущественное использование космических и радиорелейных линий связи, поэтому остро встает проблема радиоперехвата передаваемой информации и разведзащищенности самой сети в целом. При этом возникают сложности в решении задачи сокрытия наличия или отсутствия передачи данных и их характеристик, а также обеспечения требования к ТКС по «защите структуры системы» (обеспечения «скрытого трафика»). С учетом этого стоит задача путем группового шифрования обеспечить сокрытие только технических демаскирующих признаков. Однако при этом не обеспечивается полное сокрытие оперативно–тактических признаков (способов организации радиосвязи, состава радиосети, режимов работы радиолиний).

4.7. Проблема комплексной защиты информации по всем компонентам ТКС ОГУ

В силу многокомпонентности как самой ТКС ОГУ, так и ее составных частей, необходимо комплексное решение вопросов защиты по каждой компоненте в отдельности и по всей системе, т.к. недостаточная проработка проблем защиты в одном из компонентов существенно снижает эффективность защиты системы в целом. Так, в связи с

происходящими в стране изменениями, в процессе которых, во-первых, появляется много небольших объектов негосударственной принадлежности: кооперативов, фирм, компаний, обществ и т.п., а во-вторых, актуальной становится защита негосударственных форм секретов: промышленных, коммерческих, банковских и т.п. В сложившейся системе различные виды защиты осуществлялись практически независимо один от другого. Такое положение было оправдано при независимом существовании традиционной и автоматизированной технологий обработки информации и при сравнительно небольших объемах работ по защите, но в современных условиях в силу отмечавшихся выше изменений, произошедших в последнее время, независимая защита различных видов становится все менее эффективной как по чисто техническим, так и по экономическим показателям.

Разработка стратегий защиты для каждой из подсистем должна базироваться на той посылке, что мероприятия по защите информации (методы контроля доступа, способы физической охраны и т.д.) будут существенно различаться в каждом из компонентов.

4.8. Проблема ЗИ при выходе на международные сети, подключении пользователей (абонентов) негосударственных структур

Обеспечение защиты информации при выходе абонентов ИСКС на международные сети и подключении абонентов негосударственных структур включает несколько частных проблем:

- организации рациональных ключевых структур;
- техническую, обусловленную трудностями унификации отечественных и зарубежных аппаратных средств, средств и мер защиты, протоколов обмена данными, стандартов и параметров шифрования, сложностями распределения ключевых документов;
- нормативно-правовую, обусловленную недостаточной согласованностью существующей отечественной и зарубежной законодательной правовой базы по международному информационному обмену.

4.9. Проблема разработки оптимальных ключевых структур

При обеспечении требований к ТКС ОГУ в плане обеспечения гарантированной защиты информации с использованием криптографических средств остро встает проблема разработки оптимальных ключевых структур. Её возникновение обусловлено рядом факторов.

Ключевая система должна обеспечивать многорубежную защиту от явной и неявной компрометации ключевой информации, разделение абонентов шифрованной связи по уровням обеспечения защиты и зонам взаимодействия между собой и с абонентами других уровней. Кроме того, ключевая система должна обеспечивать и удовлетворять следующим требованиям:

- долговременный ключ со значительным периодом смены (более 1 года);
- достаточную устойчивость к числу компрометаций (не менее нескольких десятков) в каждой ключевой зоне;
- иметь аварийную систему открытого ключа или открытого распределения ключей;
- компрометация шифроключей аппаратуры низшего уровня не должна приводить к компрометации шифроключей аппаратуры более высоких уровней;
- абоненты стран СНГ должны быть выделены в отдельные ключевые зоны, а их выход в сети России должен осуществляться через специальные шлюзы с использованием ключей взаимодействия;
- для сохранения возможностей обеспечения связи абонентов России с абонентами СНГ должна быть предусмотрена модификация аппаратуры для стран СНГ, отличающейся по криптоалгоритму, но обеспечивающей возможность совместной работы с перспективной шифроаппаратурой абонентов России. При этом связь может быть организована с перешифрованием на узлах нашей страны с помощью аппаратуры, имеющей общегосударственную схему;
- для обеспечения возможности абонентского шифрования на межгосударственном уровне необходима модификация аппаратуры, которая будет содержать два криптоалгоритма: национальный (может быть индивидуальный для каждой страны) и межгосударственный (общий для всех стран), и использовать соответственно два ключа, которыми оснащаются все или выборочно абоненты сети.

4.10. Проблема организации управления защитой информации

Рассматриваемые и решаемые задачи управления защитой информации [21–23] представляют собой далеко не полный их перечень. Кроме этого, они недостаточно четко структурированы. Необходимо разработать полный перечень и произвести систематизацию задач

управления защитой информации, в т.ч. и по этапам его осуществления (функциям управления защитой информации), которые включают планирование, оперативно-диспетчерское управление, календарно-плановое руководство и обеспечение повседневной деятельности системы управления защитой информации. Наряду с перечисленным, требует дальнейшего развития и решения задача совершенствования оперативно-диспетчерского управления защитой информации. В то же время предполагаемые высокоскоростные потоки данных большого объема требуют четкого оперативно-диспетчерского управления (ОДУ) защитой информации и, прежде всего, для обеспечения требуемого (или максимально возможного в данных условиях) уровня защищенности информации при возникновении нештатных ситуаций. Несвоевременное принятие мер по пресечению нарушений и ликвидации последствий может привести к большому ущербу, т.к. при возникновении нарушения в системе защиты существует возможность утечки большого количества информации за сравнительно небольшой промежуток времени. Решение проблемы ОДУ возможно за счет имеющихся служб защиты информации, либо путем создания специально выделенной службы ОДУ защитой информации в масштабе всей сети.

4.11. Проблема построения защищенной системы на основе принципиально открытой модели

В основу архитектурного построения ТКС ОГУ положена так называемая *семиуровневая эталонная модель взаимодействия открытых систем* (ЭМВОС). При этом широко используются открытые конфигурации. Применяются стандартизованные взаимосовместимые технические и программные средства, не требующие доработки при эксплуатации в составе системы и соответствующие рекомендациям ISO 7498–2(Х–800 МККТТ) по защите информации открытых систем связи. Это обеспечивает большую гибкость, но увеличение стандартизации способствует упрощению НСД к оборудованию систем. Концептуальная посылка построения сети конфиденциальной связи на основе принципиально открытой модели создает множество возможностей нарушения установленного статуса информации на каждом из ее уровней. При этом шифрование данных на одном из уровней не снимает проблемы в целом. Сложность решения данной проблемы определяется следующими факторами:

- во-первых, реализация мероприятий (служб) безопасности на всех уровнях ЭМВОС связана с большими затратами и трудностями;
- во-вторых, в связи с необходимостью сохранения совместимости систем в них следует внедрять службы безопасности на одном и том же уровне;

- в-третьих, отсутствие общих подходов к решению проблем безопасности может породить трудности при выходе абонентов ИСКС на международные сети.

4.12. Проблема аутентификации абонентов и абонентских установок

При вводе ключевой информации в оперативное запоминающее устройство АЗ планируется использование индивидуальных специальных абонентских карточек. Данная карточка становится еще одним объектом защиты, наряду с ключевыми документами.

Необходимо предусмотреть возможность установления подлинности абонента, осуществляющего ввод ключевых данных и проводящего сеанс связи, с помощью интеллектуальных карт с личными данными пользователя (Ф.И.О., ведомство, должность), передаваемых по каналу связи с использованием криптозащиты. Должна быть исключена возможность подделки карточек или несанкционированного пользования подлинными карточками субъектом, не имеющим на это полномочий. Другими словами, необходимо проведение аутентификации как абонентских установок, так и абонентов.

Кроме того, необходимо обеспечить защиту от отказа отправителя или получателя от переданной или принятой документальной информации посредством применения цифровой подписи.

4.13. Проблема защиты от преднамеренной перегрузки ресурсов системы и переадресации информации

Предполагается создание и эксплуатация ТКС ОГУ несколькими ведомствами, а также коллективное использование ресурсов этой системы. В связи с этим возникает дополнительная возможность для злоумышленника, маскируясь под санкционированного пользователя другого ведомства, искусственно занимать ресурсы и перегружать линии передачи с целью блокировки возможностей использования этих ресурсов санкционированными пользователями и передачи их конфиденциальной информации. В связи с этим необходимо предусмотреть систему управления прохождением и обработкой информации, а также предоставлением ресурсов сети для абонентов различного приоритета.

Кроме того, должны быть приняты меры, предотвращающие переадресацию информации за счет сбоев и неисправностей в технических средствах, ошибок абонентов и обслуживающего персонала.

Анализ приведенных проблем подтверждает актуальность решения проблемы КЗИ, требует более углубленных исследований, предполагающих первоочередных разработку теоретических основ БИ в ТКС ОГУ, формирование полного множества задач их КЗИ, разработку

моделей систем КЗИ и обоснование выбора методов обеспечения информационной безопасности, разработку способов реализации систем КЗИ в ТКС ОГУ.

Решению рассмотренных выше проблем и задач обеспечения информационной безопасности (как в целом, так и по ее составляющим) посвящены работы теоретического и прикладного характера как отечественных [24–27], так и зарубежных ученых [28–39]. Значительное место в этих работах уделено исследованию вопросов защиты информации в системах связи специального назначения, АСОД, электронно-вычислительной технике (ЭВТ), построению моделей безопасности и разработкам методик оценки частных показателей защищенности информации в АСОД и системах связи [79–81,85]. Достаточно глубоко исследованы вопросы повышения разведзащищенности систем связи и защищенности информации в АСОД и ЭВТ.

Вместе с тем решение проблемы повышения эффективности системы обеспечения информационной безопасности ТКС ОГУ требует, прежде всего, наличия единого методологического базиса и инструментария для решения задач анализа, синтеза систем и процессов защиты, учитывающих наиболее полное множество показателей и параметров ТКС ОГУ, требований к качеству обрабатываемой в ней информации, различные угрозы информации и возможности ТСР, а также особенности системы комплексного противодействия ТСР (ПД ТСР) и обеспечения БИ.

Недостаточность разработки актуальных проблем обеспечения информационной безопасности, в т.ч. и качественной ее оценки, в настоящее время ограничивается рядом факторов.

1. К более значимым следует отнести недостаточную проработку, неадекватность существующего понятийного аппарата реальным запросам теории и практики информационной безопасности. Подтверждением этого является тот факт, что на протяжении длительного времени отсутствовало однозначное понимание учеными и специалистами понятия информационной безопасности и некоторых его составляющих (безопасности информации, безопасности связи, компьютерной безопасности и др.), что подтверждается результатами анализа выше приведенных источников, а также ряда нормативных правовых актов [1, 3, 36, 37]. Положительное значение для решения вопроса развития понятийного аппарата информационной безопасности сыграли впервые появившееся в 1995 г. понятие информационной безопасности [11–12], а также фактическое принятие понятия информационной безопасности на уровне доктрины [4], что в целом подтверждает не только важность самой проблемы, но и очевидную актуальность, и первоочередность уточнения и развития понятийного аппарата информационной безопасности.

2. Недостаточная разработанность существующих адекватных моделей систем и процессов обеспечения информационной безопасности, анализа, синтеза систем и процессов комплексной защиты, а также методов и методик оценки. Проведенный анализ существующих моделей систем защиты информации позволил выявить следующее:

- большинство моделей только описывают в общем виде состав средств защиты, не позволяя описать и объяснить отношения между объектами и элементами защиты. Эти модели не позволяют осуществлять прогнозирование класса проблем обеспечения информационной безопасности;
- в большинстве случаев существующие обобщенные модели защиты информации и обеспечения безопасности связи сводятся к частным моделям, позволяющим выйти на оценку одной из компонент: степени криптографической, некриптографической, программной, организационной защиты информации, без учета взаимных влияний на информационную безопасность уровней этих составляющих;
- ряд моделей системы защиты информации сведен к моделям защиты системы связи от демаскирования и воздействия различных средств поражения;
- в большинстве моделей систем защиты и оценки информации недостаточно учитываются взаимосвязи состояний системы защиты от качества их обслуживания, взаимосвязи воздействий ТСР и принятых мер защиты, взаимосвязи информационных потоков в ТКС ОГУ и СЗИ, взаимосвязи затрат ресурса и достаточности мер защиты;
- большинство существующих моделей составлено без учета содержания понятия информационной безопасности и ее компонентов: компьютерной безопасности, безопасности информации и связи, разведзащищенности системы, защищенности от разрушающих воздействий информации и др., и это при том, что существующие определения имеют неоднозначное содержание. В таких моделях не всегда отражены требования пользователей и самих ТКС к информационной безопасности;
- разработанные модели не всегда позволяют проанализировать и произвести выбор структурных показателей построения систем КЗИ, сформировать показатели их эффективности и обеспечения требуемой информационной безопасности, исследовать характеристики и взаимосвязи элементов объектов обеспечения

информационной безопасности, в т.ч. информации, информационных процессов и компонент ТКС ОГУ.

Рассмотренные недостатки обусловлены рядом причин, среди которых можно выделить то, что разработка моделей систем КЗИ ТКС ОГУ усложняется:

- многокритериальным характером функционирования системы защиты в условиях неопределенности факторов внешнего воздействия;
- отсутствием адекватных моделей воздействия угроз, в т.ч. ТСР на ТКС ОГУ и ее подсистемы;
- недостаточностью формальных способов представления информации о состоянии ТКС ОГУ и системах обеспечения информационной безопасности, в т.ч. комплексного противодействия ТСР, обеспечения БИ, противодействия разрушающим воздействиям информации, информационных систем и ресурсов на должностных лиц, человека и в целом на ТКС ОГУ.

3. В свою очередь недостаточная формализация способов представления информации не позволяет использовать ЭВТ для обработки результатов контроля и оценки информационной безопасности. Кроме этого, отсутствие единых аналитических, математических и логических моделей анализа и синтеза систем и процессов защиты затрудняет разработку соответствующих методик для получения количественных, интегральных значений информационной безопасности и ее составляющих.

Отсутствует единый подход к интегральной количественной оценке эффективности обеспечения БИ действующими и развивающимися системами комплексной защиты ТКС ОГУ. В рамках такой оценки не в полной мере решены задачи количественного учета влияния характеристик элементов ИНКС, информационных процессов в ней, методов и способов КЗИ от воздействия угроз, в т.ч. ТСР противника, на информационную безопасность и безопасность защищаемой информации. С учетом этого можно сделать вывод о недостаточной проработке не только адекватных моделей комплексной защиты, но и методов выбора, анализа эффективности функционирования систем КЗИ, необходимых для объективной оценки степени обеспечения информационной безопасности. Такое положение дел, в свою очередь, затрудняет обоснованный выбор рациональных структур ТКС ОГУ и подсистем их комплексной защиты как в ходе планирования, эксплуатации действующих, так и при проектировании, разработке перспективных, модернизации существующих ТКС ОГУ и их компонентов на различных этапах жизненного цикла. Это в конечном итоге приводит к неэффективному использованию ТКС ОГУ, ее

подсистемы обеспечения безопасности информации и снижению безопасности обрабатываемой в ней информации.

4. Руководство организацией и обеспечением информационной безопасности является одной из важнейших функций подсистемы управления ТКС ОГУ. Целью обеспечения информационной безопасности является недопущение прямой утечки содержания передаваемой информации за счет различных угроз и дестабилизирующих факторов, а также защиту сведений о самой системе обработки информации в силу косвенной утечки конфиденциальных сведений за счет структурной, функциональной и признаковой доступности ТКС ОГУ, обеспечение заданной семантической доступности информации ЛПР за счет исключения разрушающих воздействий, в т.ч. ввода ложной информации и другой деструктивной информации в системы, средства и комплексы по различным каналам и через программно-аппаратные компоненты ТКС ОГУ.

И, наконец, анализ существующих методик оценки информационной безопасности, рассматриваемых в ряде указанных выше работ, а также в нормативных правовых актах [7, 8, 36], проведенный авторами, позволил выявить ряд недостатков, затрудняющих ее оценку:

- большинство из существующих методик ориентировано на оценку частных показателей защищенности информации, не позволяющих получить интегральную оценку;
- в ряде случаев количественная оценка информационной безопасности сводится в основном к частным оценкам разведзащищенности систем, криптостойкости систем засекречивания, криптоживучести ключевых структур действующих сетей конфиденциальной связи, надежности защитных свойств программного обеспечения;
- многие методики ориентированы на оценку защищенности только аналоговых сигналов;
- большинство методик являются графоаналитическими, требуют громоздких расчетов и больших затрат времени, что снижает оперативность и своевременность оценки информационной безопасности или ее составляющих в динамике функционирования ТКС ОГУ и ее компонентов;
- используемые в методиках показатели носят субъективный характер и зачастую большую степень неопределенности;
- применяемые методики, как правило, ориентированы на апостериорные данные, что не позволяет получить прогнозную оценку безопасности связи;

- отсутствие учета влияния на конечную оценку случайных факторов внешнего воздействия окружающей среды, средств поражения, ТСР, а также влияния реальной надежности элементов ТКС ОГУ и ее подсистемы обеспечения информационной безопасности;
- недостаточная точность методик, ориентированных на получение качественных оценок, не дающих адекватного представления о реальном состоянии информационной безопасности ТКС ОГУ;
- большинство методик требует сложных, дорогостоящих приборов и не учитывает сложности проведения инструментального контроля и обработки результатов в полевых условиях;
- многие методики не учитывают возможности автоматизированной обработки результатов контроля и оценки БПС в рамках развития автоматизированных систем управления самой ТКС ОГУ и др.

Глава 5.
Обоснование структуры системы комплексного контроля безопасности информации

Рассматривая вопрос о разработке структуры *комплексного контроля безопасности информации* (ККБИ), необходимо учитывать существующий опыт направлений формирования основных естественнонаучных теорий и сформулированный взгляд на понятие, содержание ККБИ, подход и модели формирования структуры ККБИ, а также известные взгляды о сложности и противоречивости процесса решения данной задачи.

Это позволит сформировать в обобщенном виде макроструктуру ККБИ, представляющую собой некую методологическую схему (рис. 4), которая не только отражает существующие взгляды на содержание ККБИ, но и представляет содержание этапов ее синтеза. Представляется, что структуру ККБИ должны составлять

- исследование и систематизация проблем, взглядов, концепций построения информационных систем (ИС) различных классов (ТКС ОГУ, АСОД и др.);
- рассмотрение содержания сущности, систематизация и определение проблем обеспечения БИ ТКС ОГУ и ее компонентов, направлений формирования полных и систематизированных знаний о происхождении и содержании проблем и вопросов комплексной защиты информации и обеспечения информационной безопасности ТКС ОГУ, комплексной защиты информации в системах специальной связи, автоматизированных системах обработки информации и (на их основе) формирование задач обеспечения информационной безопасности, а также оценки предпосылок их решения;
- научно-обоснованная постановка проблемы реализации комплексной защиты информации, обеспечивающей заданный уровень информационной безопасности ТКС ОГУ, адекватно учитывающей потребности личности, общества, государства в защите информации, в т.ч. в защите содержания информации пользователей (ИП), защите информации, сведений о системах ее обработки (ИС), защите от разрушающих воздействий информации, объективные предпосылки удовлетворения этих потребностей, действующие и перспективные концепции построения информационных систем и подсистем обеспечения их ИБ;

– систематизация требований к обеспечению информационной безопасности и организации комплексной защиты информации, учитывающая все многообразие потенциально возможных условий функционирования систем обработки и защиты информации;

– исследование и систематизация содержания теоретических аспектов, результатов анализа, направлений развития теоретических исследований и опыта практического решения задач обеспечения информационной безопасности ИС различных классов;

– систематизация принципов, подходов, направлений, моделей разработки ККБИ;

– рассмотрение направлений развития понятийного аппарата ККБИ;

– формирование методологических принципов ККБИ;

– разработка концепции обеспечения БИ ТКС ОГУ.

Систематизация и формирование:

– задач обеспечения информационной безопасности как содержащих необходимые методы и инструментальные средства эффективного решения наиболее полного множества задач защиты, а также общеметодологические подходы и конкретные прикладные методы их решения для любых условий;

– математических моделей обеспечения информационной безопасности и ее оценки в ТКС ОГУ;

– методов решения задач и моделирования систем и процессов защиты информации и оценки ее безопасности в информационных телекоммуникационных системах, сетях конфиденциальной связи и ее элементах;

– основ методологии анализа и синтеза эффективных систем защиты, представляющей структуру способов, методов, логической организации средств защиты, контроля и оценки защищенности информации информационных телекоммуникационных системах и в интегрированных системах конфиденциальной связи;

– инструментария решения задач защиты и контроля, включающего

  – методики выбора показателей информационной безопасности;

– методики оценки эффективности многоуровневой системы защиты информации, оценки компрометации шифров и криптоживучести ключевых структур;

– организационно-технических рекомендаций и предложений по реализации эффективной систем защиты информации, циркулирующей в телекоммуникационной системе и ее элементах;

– прогнозную оценку перспективных направлений развития методологии и практики контроля безопасности информации.

Рис. 4. Обобщенная структура методологических основ комплексного контроля безопасности информации

Таким образом, исходя из вышеизложенного можно сформулировать некоторые выводы.

Многообразие и разнообразие существующих взглядов, подходов, концепций, неоднозначность понимания вопросов обеспечения информационной безопасности, а также противоречия одновременного совершенствования информационного обеспечения видов деятельности и развития систем и средств информационного противоборства в условиях формирования нового информационного общества и широкого использования новых информационных технологий обусловили несоответствие между существующей, традиционной системой знаний предметной области и изменившимся содержанием процесса информационного обеспечения деятельности личности общества и государства, необходимость формирования требуемой полноты теоретической проработки, систематизации знаний по широкому спектру вопросов комплексной защиты информации и обеспечения информационной безопасности.

Основными факторами, определяющими направления и пути развития информационной безопасности, являются возрастающая роль НИТ и обеспечение на их основе технотизированной интеллектуализации общества; процессы формирования единого информационного пространства, динамического возобновляемого ресурса развития страны, мирового сообщества и в целом цивилизации. От уровня и качества информации и информационного ресурса зависит эффективность принимаемых решений, формирование государственной информационной политики, отражающих национальные интересы России в информационной сфере, стратегических направлений, задач, способов мер их достижения и реализации. Решение этих вопросов неразрывно связано с системами управления и их материальной основой – современными системами обработки информации, представляющими информационные телекоммуникационные системы, в т.ч. специального назначения. Закономерности их развития обусловливают причинно-следственные связи, относящиеся к информационной безопасности.

Особенностью функционирования ТКС ОГУ является обработка и доставка информации не только особого качества, но обладающей соответствующим правовым статусом, своими особенностями: включенность в контур управления социально–экономическими, политическими, военными и другими системами; обязательность исполнения и ответственность за неисполнение; тяжесть последствий, снижение эффективности управления при неадекватности и низком качестве. Это обусловливает актуализацию проблемы комплексного контроля и обеспечения безопасности информации в ТКС ОГУ.

Особенности построения и функционирования ТКС ОГУ обусловливают в целом проблему обеспечения ее информационной безопасности и определяют пути формирования информационной сферы, основные направления, виды информационной деятельности должностных лиц ОГУ. Это предполагает решение следующих задач: расширение существующих телекоммуникационных сетей с глобальным охватом территорий, значительным числом пользователей различных органов государственной власти, государственных и общественных организаций с различными формами собственности; совершенствование качества представления телематических услуг и обслуживания; развитие новых видов телекоммуникации и различных услуг в рамках как существующих, так и вновь создаваемых систем; интеграция видов связи, информации систем и сетей телекоммуникации на различных уровнях систем управления; использование новых информационных технологий; повышение качества представляемой пользователям информации при минимальных затратах ресурса.

Анализ особенностей, принципов построения и функционирования информационных телекоммуникационных систем их компонент позволяет

- доказать, что ТКС ОГУ и система ее информационной безопасности обладают всеми чертами, позволяющими отнести их к классу больших и сложных систем в силу их свойств как системы и по сложности решаемых задач (вычислительная сложность), что обосновывает применение системного подхода в решении поставленной проблемы;
- выявить и систематизировать проблемы обеспечения информационной безопасности в распределенной ТКС ОГУ при предоставлении всех видов услуг, формирования методического инструментария интегральной оценки качества использования новых информационных технологий и средств комплексной зашиты информации, совершенствования комплексов технических средств обработки конфиденциальной информации, развития управления подсистемой контроля и защиты информации, нормативного правового базиса обеспечения контроля безопасности информации и др.;
- выявить и систематизировать неопределенности воздействий внешних факторов и внутренних взаимосвязей, снижающие уровень безопасности информации в ТКС ОГУ;
- доказать, что ТКС ОГУ и ее компоненты являются объектами постоянного воздействия ТСР вероятного противника как в мирное, так и в военное время, и с учетом этого систематизировать ряд основных направлений обеспечения

безопасности информации. При функционировании ТКС ОГУ и ее компонентов резко возрастает вероятность случайного или злоумышленного воздействия на обрабатываемую информацию и саму систему. При этом новые тенденции в построении телекоммуникационных систем в значительной мере определяют большое разнообразие проблем и специфику обеспечения безопасности информации. С учетом больших масштабов использования ТКС ОГУ в социально-экономических процессах страны даже незначительное повышение эффективности решения отдельных вопросов защиты информации в ОГУ даст значительный народно-хозяйственный эффект;

- выявить недостаточность решения актуальных проблем количественной и качественной оценки эффективности систем контроля и обеспечения безопасности информации, проработки, неадекватности существующего понятийного аппарата реальным запросам теории и практики информационной безопасности; недостаточность разработки существующих адекватных моделей систем и процессов контроля и обеспечения безопасности информации, анализа, синтеза систем и процессов комплексной защиты, а также методов и методик оценки; недостаточность формализации способов представления информации.
- выявить обусловленность развития ТКС ОГУ направлениями совершенствования системы обеспечения ее информационной безопасности на основе формирования научно-методологического базиса методологических основ комплексного контроля безопасности информации, создания методического инструментария решения актуальных проблем и задач комплексной защиты информации;
- уточнить важность мобильного компонента ТКС ОГУ, который определяет возможности системы по обеспечению заданного качества информационного обеспечения деятельности в чрезвычайных ситуациях и особенности функционирования ТКС ОГУ в условиях воздействия внешних факторов, в т.ч. технических средств разведки.

Основными результатами сегодняшнего состояния развития методологических основ комплексного контроля безопасности информации можно назвать сформировавшийся предмет защиты информации, который развивается в традиционном русле обеспечения защиты содержания носителей информации в телекоммуникационных и автоматизированных системах, обеспечения безопасности информации и связи на основе известных криптографических и некоторых

некриптографических способов, что и определило приоритет теоретических аспектов в этом направлении; наличие определенного теоретического, научно-методического, учебно-методического потенциала; недостаточность разработанности адекватных моделей, методов и методик решения задач обеспечения и оценки эффективности контроля безопасности информации на соответствующих объектах, которая обусловлена практическим опытом решения задач обеспечения безопасности информации в системах ее обработки классическими методами криптографической и некриптографической защиты; недостаточная разработанность теоретических методов, моделей, методологии оценки безопасности информации в информационных системах, а также представление ряда методик в нормативно–директивной форме не позволяют говорить о завершенности методологии и обусловливает субъективный подход к оценке состояния безопасности информации на объектах ОГУ.

В рамках этих проблем очевидным образом могут быть выявлены конкретные тенденции и закономерности в теории и практике информационной безопасности, обусловливающие их развитие, а также определены проблемы, которые предполагают

- исследование существующих, перспективных направлений и видов деятельности органов управления в области обеспечения информационной безопасности;
- систематизацию существующих и наиболее значимых факторов, определяющих необходимость изменения и развития подходов в области защиты и безопасности информации;
- анализ базовых и выбор адекватной (для развития и решения проблем безопасности) информации;
- обоснование и разработку наиболее приемлемой концепций безопасности информации, учитывающих действующие и перспективные особенности социально-экономического, технического, военного развития страны;
- доказательство необходимости видоизменения и уточнения существующих постановок задач обеспечения безопасности информации в ТКС ОГУ с усилением управленческого компонента;
- формирование теоретических принципов и подходов к решению проблем, связанных с концепциями информационной безопасности;
- развитие существующей правовой базы контроля безопасности информации.

Содержание, выявленные особенности информационных процессов, протекающих в ТКС ОГУ, условия постоянного воздействия на них угроз, а также состояние теоретических основ информационной безопасности обусловливают

- содержание и постановку проблемы комплексного контроля безопасности информации, адекватной современным требованиям обеспечения информационной безопасности, сущность которой заключается в переходе от всеохватывающего календарного контроля безопасности и интегральной защиты, построенных по принципу тотального охвата всего, что имеет прямое или косвенное отношение к охраняемым сведениям, к созданию дифференцированной комплексной системы контроля безопасности и защиты информации, реализующей принцип оптимизации уровня защиты от воздействия различных угроз с учетом деятельности ОГУ и затрат ресурсов, предусматривающих конечный результат, сбалансированное и согласованное развитие ОГУ и его функциональных подсистем;
- исходные посылки для разработки методологических основ комплексного контроля безопасности информационных телекоммуникационных систем.

В заключение следует отметить, что решение проблемы разработки методов комплексного контроля безопасности информации на объектах ТКС ОГУ, отражающих целостную систему взглядов в сфере информационной безопасности, характеризующих логическую зависимость элементов названой сферы, дающих системное представление о содержании задач контроля и обеспечения защиты информации, закономерностях развития безопасности информации, существенных связях с другими отраслями знаний, определяющими направления совершенствования и повышения эффективности контроля безопасности информации в ТКС, является одним из важных направлений развития и повышения эффективности деятельности ОГУ.

Заключение

В рассмотренных выше материалах дается первичный анализ функционирующих в настоящее время в федеральных органах исполнительной власти и в исполнительных органах государственной власти субъектов Российской Федерации, а также подведомственных им учреждений и организаций телекоммуникационных систем органов государственного управления.

Можно сделать вывод, что телекоммуникационные системы органов государственной власти и ее компоненты являются наиболее уязвимыми звеньями в системах управления социально-экономическими, политическими, военными и другими процессами, так как через них в первую очередь возможно нанесение ущерба.

Учитывая рассмотренные особенности управления, можно заключить, что специфика ТКС и обеспечение ее информационной безопасности напрямую зависит от внутреннего строения, природы образующих элементов и компонентов, характера их взаимодействия.

Анализ проблем контроля безопасности информации в телекоммуникационных системах органов государственного управления позволяет сделать вывод о необходимости скорейшего импортозамещения в сфере инфокоммуникационных технологий. Использование импортного программного обеспечения обусловливает необходимость специальной проверки на отсутствие программных закладок и скрытых функциональных возможностей, но это практически невозможно, так как по сложности и трудоемкости такая проверка сравнима с разработкой собственного оригинального программного обеспечения.

Основная цель программы импортозамещения — обеспечение безопасности автоматизированных систем управления военного и специального назначения, а также производственных и технологических процессов.

Термины и определения

Активное (атакующее) оружие — вид информационного оружия, включающий компьютерные вирусы, блокирующие возможность применения информационных систем различного класса и назначения; средства имитации воздействия вирусов на программное обеспечение и сбоев в работе ЭВМ, системы ЭВМ, сети ЭВМ; программные и аппаратные закладные средства, внедряемые в вычислительные системы агентурой техническим методами, при производстве импортируемой техники и поставке программного обеспечения; системы (средства) радиоэлектронного подавления; средства имитоввода, обеспечивающие передачу ложных сообщений, задержку (искажение) информации, предаваемой по каналам связи, нарушение системы адресации и паролирования и в целом управления; комплексные средства защиты.

Безопасность — состояние защищенности жизненно важных интересов личности общества и государства от внутренних и внешних угроз.

Вспомогательные технические средства и системы — технические средства обработки информации, не предназначенные для обработки конфиденциальной информации, но на них во время их работы могут воздействовать электрические, магнитные электромагнитные или акустические поля источников опасных сигналов.

Графическое изображение (процесс) — вид выражения (воплощения) воспринятого образа графическими средствами (точки, линии, светотень, цвет, тон, штрихи и т.д.) и методами (методы их объединения, масштабирования, сочетания, проекции, стереоэффекта, мультипликации и т.д.) работы с ними.

Деятельность (процесс) — форма отношений, реализуемых средствами деятельности между объектом и субъектом деятельности, содержание которых составляет целесообразное изменение и преобразование объекта.

Дестабилизирующие факторы — совокупность некоторых явлений, событий, факторов, при которых возможно нежелательное воздействие на информацию.

Демаскирующие признаки средств связи и автоматизации — любая количественная или качественная характеристика полей, которые создаются, отражаются или искажаются средствами связи и автоматизации, если они раскрывают их наличие (отличие друг от друга).

Достоверность — способность контроля объективно отображать действительное техническое состояние изделия (технических средств передачи информации или средств их защиты).

Единое информационное пространство — это форма существования инфокоммуникационной инфраструктуры и технологических процессов, протекающих в ней, в обеспечение должностных лиц органов управления инфокоммуникационными услугами заданного качества в любое время и в любой точке установленного пространства.

Информационная безопасность — состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Информационная сфера (среда) — сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

Инфокоммуникационная сеть (ранее применялись также термины «информационная сеть», «компьютерная сеть») — это технологическая система, которая включает в себя, кроме сети связи, также средства хранения, обработки и поиска информации, и предназначена для обеспечения пользователей электрической связью и доступом к необходимой им информации.

Изображение (процесс) — вид выражения (воплощения) образа в форме, предназначенной для визуального восприятия.

Информационная операция — совокупность согласованных и взаимосвязанных по цели, задачам, месту и времени действий сил и средств информационного противоборства, проводимых одновременно, последовательно, по единому замыслу и плану для решения определенных задач, представляющих противоборство в области систем управления, организацию разведки и предоставление требуемых данных для принятия решений по защите от адекватного воздействия злоумышленника своих информационных ресурсов.

Информационное оружие — системы (средства), методы и способы целенаправленного воздействия на все составляющие информационного ресурса противоборствующей стороны.

Инфокоммуникационная инфраструктура — это совокупность устойчивых связей информационных и телекоммуникационных инфраструктур, обеспечивающих ее целостность и тождественность самой себе, т.е. сохранение единой инфокоммуникационной среды и функциональных возможностей при различных внешних воздействующих факторах (например, механических, климатических, специальных).

Информационная технология — это совокупность приемов и способов выполнения функций (технологических операций) сбора, хранения, поиска, обработки и распределения информации с применением средств вычислительной техники.

Информационная инфраструктура — это совокупность информационных ресурсов, технологий и изделий, построенных на базе этих технологий, средств поддержки использования изделий по назначению для обеспечения сбора, хранения, поиска, обработки, распределения информации и доступа пользователей к ней.

Информационный ресурс (информационное обеспечение) — это совокупность хранимой, обрабатываемой и передаваемой информации и реализованных решений по объемам, размещению и формам ее существования.

Информационная технологическая платформа — это совокупность методов, разрешенных (установленных) к применению, в обеспечение сбора, форматирования, формализации, хранения, поддержания идентичности информации и доступа пользователей к ней.

Контролируемая зона — пространство вокруг объекта технических средств обработки информации, исключающее неконтролируемое пребывание посторонних лиц или транспортных средств (посторонними считаются лица или транспортные средства, не имеющие соответствующего разрешения для пребывания на территории (в пространстве) объекта).

Канал нарушения целостности информации — это канал, образованный совокупностью соответствующих дестабилизирующих факторов, источника информации, источника сообщения, злоумышленника и приводящий к логическому искажению (модификации) или полному физическому уничтожению информации.

Канал утечки информации — это канал, образованный совокупностью соответствующих дестабилизирующих факторов, источника информации, источника сообщения, злоумышленника и приводящий к несанкционированному получению информации лицами, не имеющими на это законных полномочий.

Канал несанкционированного доступа — физический путь от источника информации (информации), источника сообщения к злоумышленнику, характеризующийся возможностью несанкционированного воздействия на информацию с целью модификации, искажения, уничтожения, хищения и т.д.

Конфиденциальная информация — вся документированная на различных носителях, а также обрабатываемая в ТСОИ информация, доступ к которой ограждается в соответствии с действующими нормативно-правовыми актами.

Конкретная форма проявления угрозы (дестабилизирующего фактора) относительно атрибута защищенности информации — предупреждения

несанкционированного ее получения лицами или процессами (программами), не имеющими на это полномочий.

Контроль состояния защиты информации от утечки за счет использования специальных электронных закладочных устройств — это проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

Конечное изделие — это изделие, выполняющее функции в полном объеме согласно целевому назначению.

Объект отражения — любой объект действительности, вовлеченный в отражательную деятельность, реализуемую любым средством искусственного или природного происхождения.

Отражение (процесс) — деятельность, реализуемая средством искусственного или природного происхождения с использованием определенных методов по воспроизведению признаков, свойств и отношений отражаемого объекта в его образе.

Образ (продукт) — результат отражения объекта на (или в) некоей форме в некоторой воспринимающей этот образ системе.

Основные технические средства и системы — технические средства обработки информации, предназначенные для обработки конфиденциальной информации.

Опасный сигнал — сигнал, содержащий конфиденциальную информацию. (Степень важности конфиденциальной информации, а, следовательно, и опасного сигнала определяется на основе соответствующих нормативных документов).

Полиструктурность — принцип, в соответствии с которым допускается возможность описания одного и того же объекта (системы) различными структурами, получаемыми комбинированием типов элементов и отношений между ними, а также изменением законов комбинации.

Процесс управления — это процесс сбора информации о ходе управления, передаче ее в пункты накопления и переработки, анализа поступающей, накопленной и справочной информации, принятия решения на основе выполненного анализа, выработки соответствующего управляющего воздействия и доведения его до объекта управления.

Показатель защищенности информации — характеристика, имеющая однозначно интерпретируемое содержание, по значению которой можно судить об уровне защищенности информации.

Пассивные средства — вид информационного оружия, включающий системы технической разведки, обеспечивающие перехват, рассекречивание, анализ и селекцию информации, передаваемой по техническим каналам в системах и на объектах, получение сведений посредством обработки демаскирующих признаков, характеризующих отличительные особенности работы технических средств обработки информации; системы аналитической обработки информации средств массовой информации; средства контроля безопасности информации, циркулирующей в собственные информационных сетях; системы защиты информации и др.

Пользователь — это должностное лицо или техническое средство, являющееся потребителем услуг инфокоммуникационной сети.

Платформа — это совокупность методов или средств (программных, технических, программно-технических модулей), разрешенных (установленных) к применению, для обеспечения создания конечных изделий на их основе. Кроме того, платформа может включать совокупность процедур, правил, норм и др.

Платформа основного назначения — это совокупность программных, технических и/или программно-технических средств (модулей), разрешенных (установленных) к применению, для создания конечных изделий на их основе.

Платформа специализированного назначения — это совокупность общесистемных процедур (процессов), которые выполняются совокупностью конечных изделий инфокоммуникационной инфраструктуры за счет, как правило, частичного использования их ресурса в обеспечение реализации общесистемных функций (операций).

Платформа вспомогательного назначения — это совокупность методов и средств, разрешенных (установленных) к применению, обеспечивающих поддержание изделий в работоспособном (исправном) состоянии и в установленной степени готовности к использованию по назначению.

Платформа безопасности информации — это совокупность методов и средств комплексной защиты информации, разрешенных (установленных) к применению, от заданного множества угроз ее безопасности.

Платформа видов обеспечения — это совокупность видов обеспечения, разрешенных (установленных) к применению, для обеспечения функционирования изделия инфокоммуникационной инфраструктуры по назначению.

Полнота контроля, оцениваемая количественно, — величина, показывающая, в какой мере контроль защищённости объекта по выбранной совокупности параметров отличается от полного, если сама система контроля является идеальной.

Результат деятельности (продукт) — измененный или (и) преобразованный объект, зафиксированный в некоторой форме в некоторой системе.

Сеть связи (или телекоммуникационная сеть) — это технологическая система, которая состоит из линий и каналов связи, узлов, оконечных станций и предназначена для обеспечения пользователей электрической связью с помощью абонентских терминалов, подключаемых к оконечным станциям.

Система защиты информации — совокупность взаимосвязанных средств, методов и мероприятий, направленных на предотвращение уничтожения, искажения, несанкционированного получения конфиденциальных сведений, отображенных физическими полями, электромагнитными, световыми и звуковыми волнами или вещественно—материальными носителями в виде сигналов, образов, символов, технических решений и процессов.

Среда распространения опасного сигнала — эфир, токо-, звуко- и светопроводящие средства коммуникации, различные физические среды, ослабляющие параметры электромагнитных и других физических полей.

Спецнадёжность — это способность объекта или средства выполнять задачи передачи, обработки и хранения информации в определённых условиях функционирования без возникновения отказов, приводящих к утечке информации (спецотказов).

Телекоммуникационный ресурс — это совокупность возможностей телекоммуникационной инфраструктуры по предоставлению пользователям телекоммуникационных услуг заданного качества.

Телекоммуникационная инфраструктура — это совокупность телекоммуникационных технологий и изделий, построенных на базе этих технологий, средств поддержки использования изделий по назначению для обеспечения хранения, преобразования, передачи, переноса (транспортирования), распределения трафика и доступа пользователей к территориально-распределенным информационным ресурсам.

Телекоммуникационная технология — это совокупность приемов и способов выполнения функций (технологических операций) хранения, преобразования, передачи, переноса (транспортирования) трафика с применением телекоммуникационных средств и средств вычислительной техники.

Телекоммуникационная технологическая платформа — это совокупность методов, разрешенных (установленных) к применению, для создания среды переноса (транспортирования) трафика.

Угроза безопасности — совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Угроза информации (дестабилизирующий фактор) — явление (событие, случай), которое может произойти в интересующем интервале времени и следствием которого может быть существенное (имеющее значение) нежелательное воздействие на защищаемую информацию по одному или нескольким аспектам статуса защищенности.

Уязвимость информации — свойство информации, находящейся в системе ее обработки, подвергаться воздействию внутренних или внешних угроз с точки зрения одного или нескольких атрибутов статуса защищенности.

Угроза информационной безопасности ТКС ОГУ — реальные или потенциально возможные действия или условия, приводящие к овладению, хищению, искажению, изменению, уничтожению информации, обрабатываемой в ТКС ОГУ, и сведений о самой системе, а также к прямым материальным убыткам.

Уровень защищенности информации — значения представляющих интерес показателей защищенности, обеспечиваемые в конкретном состоянии системы ее обработки используемыми методами и средствами защиты.

Фасцинация — не содержание, но атрактивность (привлекательность) сообщения, являющаяся свойством формы. Сообщение содержит в себе информацию, но самому сообщению присуща некая атрактивность (привлекательность или, наоборот, не привлекательность), вызывающая готовность (не готовность) адресата воспринимать содержание этого сообщения. Исходя из этого, можно сказать, что в сообщении, представленном графическим изображением, информация рассматривается как форма и как содержание, поэтому использование в системе информационного обеспечении деятельности графических изображений может быть привлекательным с точки зрения фасцинации (информации о форме), однако совершенно бесполезным и более опасным и вредным с точки зрения информации о содержании переданного смысла, т.е. нести разрушающую информационную угрозу.

Цикл управления — процесс сбора данных о состояниях объекта управления, принятия решения, выработки и реализации управляющих воздействий.

Список литературы

Блахнов Л.Л., Лихачев А.М., Масановец В.В. Вопросы обеспечения национальной безопасности при создании глобального информационного пространства // Исследование, разработка и применение высоких технологий в промышленности: сборник трудов. Т.3. СПб: Политехнический университет, 2005. С. 99—113.

ГОСТ Р 50922 — 99 Защита информации. Основные термины и определения.

ГОСТ Р 51275 — 99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию.

Демидов А.А. Проблемы государственного регулирования процессов развития и безопасного функционирования Интернет // Проблемы развития технологических систем государственной охраны, специальной связи и информации: сб. научных трудов. №7. Ч.2 / Под общ. ред. В.В. Мизерова. Орел: Академия ФСО России, 2011. С. 123—125.

Демидов А.А., Никифоров О.Г., Акимов С.В. Автоматизация структурно-параметрического синтеза системных объектов // Вопросы радиоэлектроники. Сер. СОИУ, 2012. Вып. 2. С. 166—181.

Доктрина информационной безопасности. Утверждена Президентом Российской Федерации 9 сентября 2000 г.

Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М.: ГТК, 1997.

Концепция национальной безопасности Российской Федерации // Независимое военное обозрение. № 46. 1999. С. 1—4.

Лопатин В.Н. Концепция развития законодательства в сфере обеспечения информационной безопасности Российской Федерации. М.: Государственная дума, 1998. 128 с.

Масановец В.В. Исследование вопросов моделирования базовых свойств телекоммуникационных систем. Теоретические основы построения ОАЦСС. М.: МО РФ, 2001. С. 239—284.

Масановец В.В. Исследование вопросов моделирования базовых свойств телекоммуникационных систем. М.: МО РФ, 2001. С. 239—284.

Масановец В.В. Основные направления создания информационной инфраструктуры государственного управления РФ // Информация и космос. № 1. 2003. С. 1—2.

Терминологический словарь «Бизнес — безопасность — телекоммуникации»: учебное пособие / Сост.: А.А. Аржанов, Е.Г. Новикова, А.В. Петраков и др. М.: РИО МТУСИ, 2000. 304 с.

Указ Президента РФ №644 от 8.05.1993 «О защите коммуникационных систем и баз данных государственных органов от утечки информации».

Указ Президента РФ от 3 апреля 1995 г. № 334 «О принятии в качестве президентской программы создания и развития информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти».

Федеральная целевая программа создания и развития информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти. М.: ФАПСИ, 1996.

Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ. // Российская газета. 1995. 22 февраля.

Федеральный закон от 4 июля 1996 года № 86-ФЗ «Об участии в международном информационном обмене».

Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб: Наука и техника, 2004. 384 с.

Abelson H., Anderson R., Bellovin S.M. The risks of key recovery, key escrow, and trusted third-party encryption. World Wide Web Journal (Web Security: A Matter of Trust). 2(3) 241-257, Summer 1997. This report was first distributed via the Internet on May 27, 1997.

Amoroso E. Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response. Intrusion. Net Books, 1999.

Forest S. Detecting Intrusions Using System Calls — Alternative Data Models // IEEE Symposium on Security and Privacy, May 1999.

Jantsch S. Risks by using COTS products and commercial ICT services // Proceedings of the NATO Conference on Commercial Off-The-Shelf Products in Defence Applications: The Ruthless Pursuit of COTS, Brussels, Belgium, April 2000. NATO.

Leveson N.G. Using COTS components in safety-critical systems // Proceedings of the NATO Conference on Commercial Off-The-Shelf Products in Defence Applications: The Ruthless Pursuit of COTS, Brussels, Belgium, April 2000. NATO.

NCSC-TG-009. Version-1, Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria.

Schneier B. Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons, 2000.

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

КАФЕДРА УПРАВЛЕНИЯ ГОСУДАРСТВЕННЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

Кафедра УГИС создана в 2011 г., сейчас работает в составе факультета технологического менеджмента и инноваций Университета ИТМО. Обучение по магистерской программе «Управление государственными информационными системами» направлено на приобретение теоретических знаний и практических навыков в сфере создания и развития ИТ-систем для нужд государственной власти и местного самоуправления.

Практическая часть обучения проходит на базе Центра технологий электронного правительства Университета ИТМО, Санкт-Петербургского информационно-аналитического центра и других партнерских структур под руководством опытных экспертов и представителей органов власти.

Демидов Александр Алексеевич

Проблемы контроля безопасности информации на объектах телекоммуникационных систем органов государственного управления

Учебное пособие

В авторской редакции
Дизайн обложки С.Н. Ушаков
Вёрстка Е.Е. Нестерова
Корректор Т.А. Асанович
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж 50 экз.
Отпечатано на ризографе