Раздел II. Анализ защищенности и защита информационных систем и объектов

УДК 004.056.5

И.В. Машкина, А.Ю. Сенцова, Р.М. Гузаиров, В.Е. Кладов

ИСПОЛЬЗОВАНИЕ МЕТОДОВ СИСТЕМНОГО АНАЛИЗА ДЛЯ РЕШЕНИЯ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Проводится системный анализ проблемы защиты информации с целью обеспечения защищенности объекта защиты в течение периода его функционирования. Система обеспечения информационной безопасности рассматривается как проблемосодержащая система. Для улучшающего вмешательства в проблемную ситуацию на основе метода декомпозиции системного анализа и требований структурированного описания среды защиты предложены модель состава объекта защиты (корпоративной информационной системы), модель существенной среды, учитывающая специфичность целенаправленных угроз, сформированы аспекты обеспечения информационной безопасности как на уровне информационной инфраструктуры, так и на уровне программной системы, реализующей бизнес-процессы.

Предлагаемые решения, проведенные на основе методов системного анализа применительно к геоинформационной системе, позволяют значительно повысить уровень защиты информационных систем.

Информационная безопасность; системный анализ; корпоративные информационные системы; система обеспечения информационной безопасности; декомпозиция; объект защиты; существенная среда; телекоммуникационная система; моделирование угроз геоинформационная система.

I.V. Mashkina, A.U. Sentsova, R.M. Guzairov, V.E. Kladov

USE SYSTEM ANALYSIS METHODS FOR THE SOLUTION OF INFORMATION PROTECTION PROBLEM OF INFORMATION SYSTEMS

In this article the system analysis of information protection problem for the purpose of security of protection object during the period of its functioning is carried out. The information security system is considered as problem including system. For improving intervention in a problem situation on the basis of the decomposition method of the system analysis the model of composition security object (corporate information system), the model of the essential environment considering purposeful threats specificity are offered, aspects of information security are generated both at level of an information infrastructure, and at level of the program system realizing business processes.

The offered decisions been spent on the basis of the system analysis methods for geoinformation system allow to raise level of information security systems.

The system analysis; the decomposition method; information system; the telecommunication system; information services; model of security objects; technology protection; software; thread model; geoinformation system.

Корпоративные информационные системы (ИС) становятся сегодня одним из главных инструментов управления бизнесом, важнейшим средством производства современного предприятия, они используются в банковской, финансовой сферах, в сфере государственного управления.

Инфраструктура корпоративной ИС является географически распределенной, структурная единица корпоративной ИС – сегмент корпоративной информационной системы.

Однако применение информационных технологий немыслимо без повышенного внимания к вопросам информационной (компьютерной) безопасности из-за наличия угроз защищенности информации. Для современного этапа развития теории и, в особенности, практики обеспечения защиты информации (ЗИ) характерна противоречивая ситуация, с одной стороны, усиленное внимание к безопасности информационных объектов, существенное повышение требований по ЗИ, принятие Международных стандартов, постоянно растущие расходы на обеспечение защиты, с другой – растущий ущерб, причиняемый собственникам и владельцам информационных ресурсов, о чем свидетельствуют публикуемые регулярно данные об ущербе мировой экономики от компьютерных атак, можно сделать вывод о том, что современные системы обеспечения информационной безопасности (СОИБ) не в полной мере обеспечивают выполнение требований по защите информации в течение всего периода функционирования объекта защиты. В корпоративных информационных системах критичная ситуация в сфере информационной безопасности усугубляется в связи с использованием глобальной сети для внешних и внутренних электронных транзакций предприятия.

Основные недостатки использующихся повсеместно СОИБ определяются сложившимися жесткими принципами построения архитектуры и применением оборонительной стратегии защиты от известных угроз. Однако постоянно констатируется появление неизвестных ранее типов деструктивных информационных воздействий. Кроме того, если информационная система обеспечивает бизнес-процессы достаточно большой организации, то она практически никогда не остается постоянной. Как следствие, решения по безопасности, принятые на этапе проектирования СОИБ, быстро утрачивают соответствие той системе, ресурсы которой она призвана защищать. Поэтому в процессе эксплуатации постоянно изменяющейся СОИБ одной из главных проблем в области информационной безопасности является обеспечение требуемого уровня защиты. Учитывая вышеизложенное, защита информации должна быть *управляемой* деятельностью.

Анализ различных аспектов управления ЗИ показывает, что на уровне корпорации централизованно осуществляется управление глобальной политикой безопасности, а также управление криптосредствами; на уровне сегмента корпоративной информационной целесообразна автономная работа системы управления, реализующая аудит, планирование модульного состава СОИБ и управление событиями информационной безопасности в реальном масштабе времени [1].

Поскольку объект управления – СОИБ является весьма сложной организационно-технической системой, функционирующей в условиях неопределенности состояния информационной среды, управление такой системой должно быть основано на применении *системного анализа*.

Процесс защиты информации характеризуется большим количеством и многообразием факторов, влияющих на его результат, воздействие которых часто не удается однозначно выявить и описать строго математически, проблема защиты информации относится к числу *сложных слабоструктурированных* и *слабоформализуемых* проблем.

В науке имеется опыт по решению слабоформализуемых проблем – это *системный анализ* объектов исследования.

В системном анализе акцентируется внимание на трудностях формулировок задач, на способах преодоления этих трудностей. С практической стороны системный анализ есть теория и практика *улучшающего вмешательства* в проблемную ситуацию [2].

Применение методов системного анализа к исследованию проблемы ЗИ диктуется требованиями практики, которая поставила специалистов по защите информации перед необходимостью *проектировать* сложные системы защиты информации, *изучать* протекающие в них процессы, *управлять* ими в условиях неопределенности, неполноты информации, дефицита времени и ограниченности ресурсов.

Специфической особенностью рассматриваемых в литературе методик системного анализа [3] является то, что они используют закономерности построения, функционирования и развития систем, формирование вариантов структуры системы и выбор наилучшего варианта. Методы системного анализа – декомпозиция, анализ и синтез системы, снимающей или ослабляющей проблему практики.

В процессе исследования используются основные принципы системного анализа, сформулированные в [3] применительно к ЗИ.

Анализ различных вариантов декомпозиции жизненного цикла, проблем, приведенных в [2], показал, что, применительно к проблеме разрешения имеющихся противоречий в области обеспечения безопасности информации, возможно формирование следующего варианта декомпозиции: выявление проблемы обеспечения безопасности информации и оценка её актуальности; определение цели организации, формулирование общей цели и задач СОИБ, декомпозиция целей; разработка модели СОИБ и её декомпозиция, анализ объекта исследования; поиск возможностей повышения эффективности ЗИ: разработка модели управляющей системы и её детализация; прогнозирование показателя эффективности СЗИ – уровня защищенности информации.

Первый этап системного анализа связан с формулированием проблемы. Необходимость системного анализа возникает, когда проблема не только существует, но и требует решения. Рабочая формулировка проблемы обеспечения ИБ: как повысить эффективность СОИБ? Как сформировать рациональный комплекс средств защиты информации в КИС? Как реагировать на опасные события в сети, чтобы минимизировать ущерб?

В системном анализе систему, в деятельности которой проявилась проблема, называют *проблемосодержащей*. Проблемосодержащая СОИБ связана с другими системами и входит как часть в некоторую надсистему. Сама СОИБ в свою очередь состоит из частей-подсистем, причастных к данной проблеме.

Применение системного подхода к решению проблемы обеспечения *полноты* и *эффективности* реализации *функций* СОИБ на различных этапах её *жизненного цикла* вызывает необходимость разработки *управляющей* системы, призванной не только обеспечить рациональные ресурсные, финансовые и временные характеристики, но и повысить степень *научной обоснованности* и *оперативности* принимаемых управленческих решений.

При этом проектирование, модернизация и обеспечение эффективного функционирования СОИБ являются нетривиальными задачами [3]. Очевидно, что и управление ЗИ так же не является тривиальной задачей.

Модель проблемной ситуации в ЗИ содержит совокупность трех взаимодействующих систем: *проблемосодержащей* системы – СОИБ; *проблеморазрешающей* системы, т.е. системы, которая разрабатывается для того, чтобы повлиять на процессы защиты информации таким образом, чтобы проблема исчезла или ослабла; окружающей, или *существенной среды*, в условиях которой функционирует СОИБ.

В соответствии с методом *декомпозиции* системного анализа применительно к проблеме ЗИ приведем модель входов СОИБ КИС, которая включает входы: от вышестоящей системы (головной организации, учреждения, предприятия), от нижестоящих систем (партнеров, клиентов, поставщиков), от существенной среды, от проблеморазрешающей управляющей системы (рис. 1)

Модель входов организационно-технической системы рекомендует определить, что понимать под термином «существенная среда» [2]. Функционирование СОИБ связано с процессами информационного противоборства, направлено на противодействие внешним и внутренним угрозам. Поэтому в данном случае под существенной средой понимается множество потенциально возможных угроз информационной среде КИС, внешних и внутренних.

Проблемосодержащая СОИБ является объектом исследования, а в качестве целевой выступает управляющая проблеморазрешающая система. Данная модель позволяет не только повысить полноту *набора целей*, но и структурировать их совокупность, что впоследствии позволит осуществить постановку задач принятия рациональных решений по управлению ЗИ.

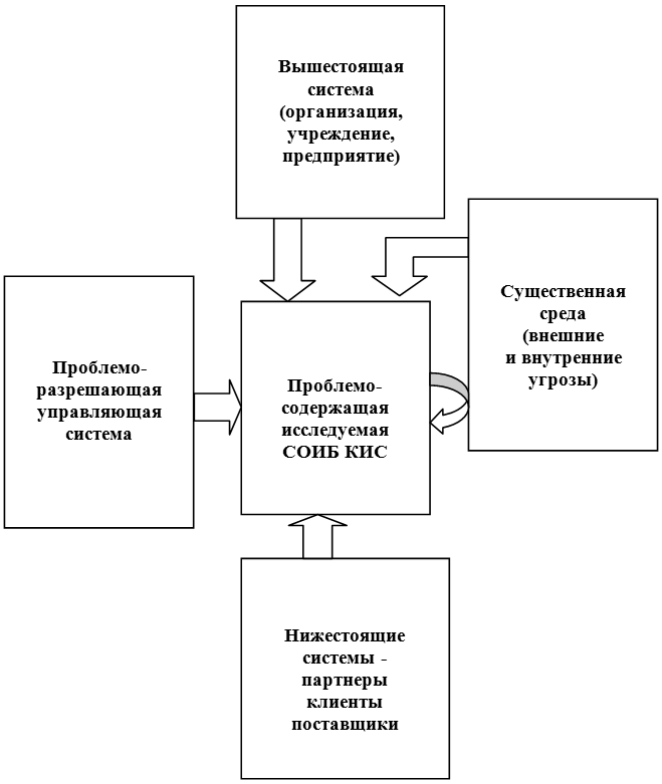

Рис. 1. Схема входов СОИБ

Целью вышестоящей системы: организации, государственного или коммерческого предприятия, – является повышение *эффективности процесса информатизации*, которая в настоящее время недостаточна из-за ежегодного ущерба от преступлений в сфере ИТ, совершаемых с использованием средств вычислительной техники.

Для проблемосодержащей системы главное – разрешить проблему, цели проблеморазрешающей системы связаны с рациональным расходованием ресурсов на решение проблемы. Цели существенной среды и СОИБ противоположны.

В соответствии с ГОСТ Р 51624-2000 [4] общей целью защиты информации является *предотвращение* или *снижение ущерба*, наносимого собственнику, владельцу или пользователю системы вследствие реализации угроз безопасности информации. Частными целями защиты информации, обеспечивающими достиже-

ние общей цели, являются: обеспечение правового режима использования массивов данных и программ обработки информации; предотвращение несанкционированного уничтожения, искажения, копирования информации, блокирования доступа к информации; сохранения возможности *управления* процессом обработки и использования информации в условиях несанкционированных (программно-технических) воздействий на защищаемую информацию; предотвращение утечки информации по техническим каналам.

Системотехника выдвигает требование количественной оценки характеристик систем [5]. Поэтому цель защиты информации должна включать, кроме формулировки, *показатель эффективности* достижения цели и его требуемое значение, а также время актуальности цели на этапах жизненного цикла, в течение которых цель должна достигаться.

Показателем эффективности достижения цели ЗИ обычно считается уровень защищенности информации η на объекте защиты, или относительный риск нарушения информационной безопасности. Значение η задается заказчиком в зависимости от максимального уровня критичности обрабатываемой на объекте защиты информации, и может принимать значение от 0,9 до 1. Время актуальности цели определяется планами обработки информации на объекте защиты [6].

В практике системного анализа в качестве глобального *объекта декомпозиции* берется исследуемая проблема и проблемосодержащая система.

Для целей анализа проблемы защиты информации необходима модель СОИБ. В качестве нее можно использовать модель деятельности, придав соответствующую интерпретацию входящим в модель компонентам (рис. 2).

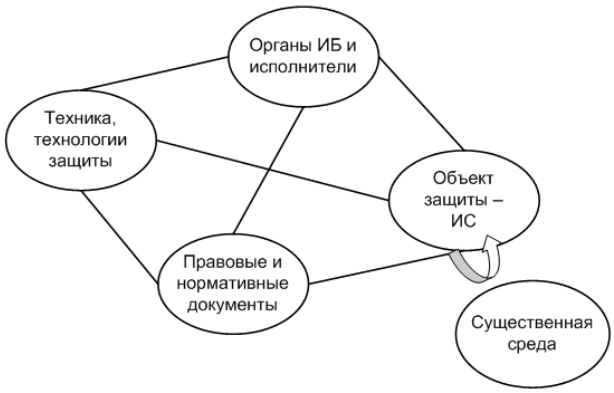

Рис. 2. Схема компонентов СОИБ

Одна из важных задач информационного обеспечения в процессе системного анализа состоит в разработке и накоплении *моделей*.

Для *анализа* процессов ЗИ необходимы *модели*, которые детализируют компоненты: *объект защиты, существенная среда*, техника, технологии защиты. Метод декомпозиции является одним из способов упрощения сложной СОИБ. Он состоит в постоянно нарастающей детализации базовых моделей системы защиты, в разложении сложного целого на все более мелкие и простые части.

После разработки упрощенной модели деятельности необходимо в соответствии с методом декомпозиции системного анализа осуществить многоступенчатый процесс от начальной декомпозиции (рис. 2) до завершающего уровня.

Объект защиты – информационная система является сложной организационно-технической системой, состоящей из двух компонентов: информационной инфраструктуры и информационных сервисов. Информационная инфраструктура

является средой, в которой функционируют информационные сервисы. Качество информационных сервисов напрямую зависит от качества информационной инфраструктуры и управления ею. Информационная инфраструктура современных ИС – телекоммуникационная система (ТКС).

ТКС – это носители и средства обработки информационных ресурсов, среда, обеспечивающая производство и потребление информационных продуктов и услуг.

Важнейшим системным свойством ТКС является возможность осуществления коммуникационных функций через стандартизированные унифицированные интерфейсы. Это позволяет прикладным системам рассматривать ТКС как «черный ящик» и строить свою реализацию без учета специфических особенностей конкретной ТКС.

Модель состава объекта защиты с декомпозицией компонента «информационная инфраструктура» приведена на рис. 3.

Программная система также может быть представлена в виде совокупности взаимодействующих программных модулей. Однако каждая конкретная программная система имеет свой состав модулей, определенный специфическими задачами, на решение которых направлена данная система в зависимости от реализуемых бизнес-процессов.

Моделирование угроз нарушения безопасности информации позволяет специалисту по защите информации получить достаточно убедительные доводы о наличии потенциальных угроз на *конкретном* объекте защиты, что способствует финансированию проекта СОИБ в необходимом объеме. На рис. 4 приведена модель состава *существенной среды* – преднамеренных угроз объекту защиты.

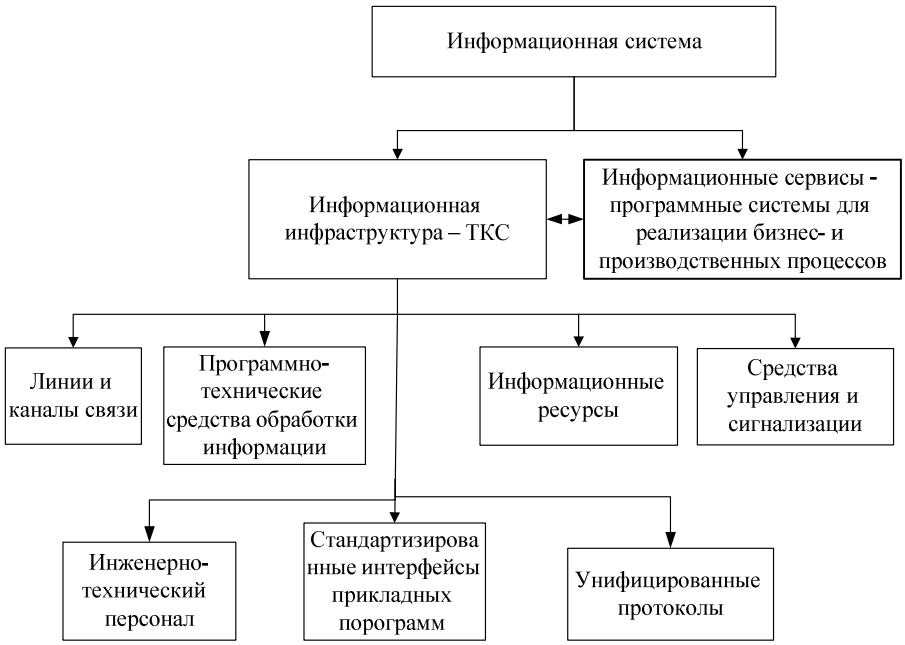

Рис. 3. Модель объекта защиты

Относительно модуля СОИБ *«техника, технологии защиты»* заметим, что защита информации на уровне информационной инфраструктуры осуществляется на четырех уровнях модели OSI: физическом, канальном, сетевом и транспортном.

Защита на уровне ТКС включает в себя следующие аспекты:

- обеспечение доступности за счет исключения единых точек сбоя;
- учет требований безопасности в структуре самой сети: организация внутренних защищенных подсетей и внешних экранируемых сегментов;
- совершенствование информационного взаимодействия за счет модернизации стеков существующих протоколов и использования таких механизмов защиты как аутентификация и криптография;
- виртуализация каналов информационного взаимодействия путем использования VLAN на канальном уровне и MPLS при межсетевом взаимодействии;
- использование автономных средств защиты, таких как межсетевые экраны, системы предотвращения вторжений, антивирусы, сканеры безопасности, системы управления информационной безопасностью и другие.

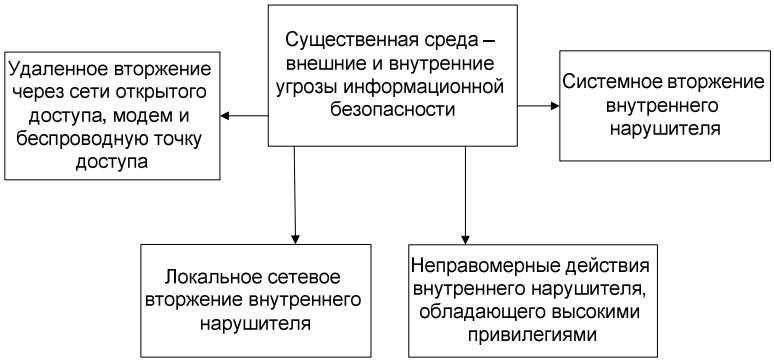

Рис. 4. Модель состава преднамеренных угроз

Успех создания проблеморазрешающей управляющей системы зависит от возможности предварить её разработку и внедрение описанием всего комплекса решаемых задач.

Рассмотрим более конкретно применение методов системного анализа применительно к корпоративным геоинформационным системам (ГИС). В настоящее время корпоративные ГИС широко используются как во всем мире, так и в России. При проектировании и эксплуатации корпоративных ГИС особое значение в последнее время приобретает решение проблемы ИБ, поскольку ценность циркулирующей в такой системе информации может быть весьма высока. Под *ГИС* понимается специализированная информационная система, которая предназначена для работы с геопространственными данными и семантическими данными. В качестве примера рассмотрим программную систему ArcGIS.

ArcGIS – семейство программных продуктов, выпущенное американской компании *ESRI* (*Environmental Systems Research Institute*). Новейшая версия программного продукта – *ArcGIS 10.* На рис. 5 изображена инфраструктура ГИС, построенная в соответствии с требованиями к архитектуре безопасности, для реализации геоинформационных сервисов с помощью системы ArcGIS, которая в свою очередь представлена в виде взаимодействующих модулей программной системы как результат ее декомпозиции.

Обеспечение безопасности геоинформационной системы (ГИС) требует необходимости комплексного подхода. Серверы реляционных баз данных ГИС поддерживают значительный массив различных типов приложений и прав пользователей. Поэтому для обеспечения конфиденциальности, целостности и доступно-

сти, необходимо применять политику безопасности на нескольких уровнях: транспортный уровень, уровень сети, системный уровень, уровень операционной системы, уровень СУБД, уровень баз данных, уровень таблиц, уровень объектов.

Проведем анализ существенной среды для данного объекта защиты – ГИС. Особое внимание следует уделить уровню приложений и сетевому уровню. Необходимо учесть угрозы, возможные при входе в операционную систему, систему управления базами данных, возможные угрозы базам данных и при обращении к слоям таблиц.

Рассмотрим существенную среду ГИС на уровне приложений и сетевом уровне. На уровне приложений наиболее опасны угрозы подмены идентификатора и повышения привилегий. Если парольная информация передается в открытом виде, то она может быть просмотрена в локальных сетях. Она также может быть перехвачена при ее передаче по сети Интернет.

Злоумышленник может воспользоваться перехваченными именами и паролями для легального входа в операционную систему, например, сервер ГИС.

Если по умолчанию вся информация на уровне web-служб и приложений также передается в открытом виде, то она легко может быть перехвачена. Кроме того, угроза нарушения конфиденциальности информации может реализоваться из-за кэширования карт: web-клиенты могут обратиться к элементам карт в КЭШе, минуя контроль безопасности web-служб.

Угроза утечки информации высокого уровня критичности связана с возможным неконтролируемым распространением информации легальным пользователем, имеющим доступ к ней и нарушающим свои привилегии после получения доступа.

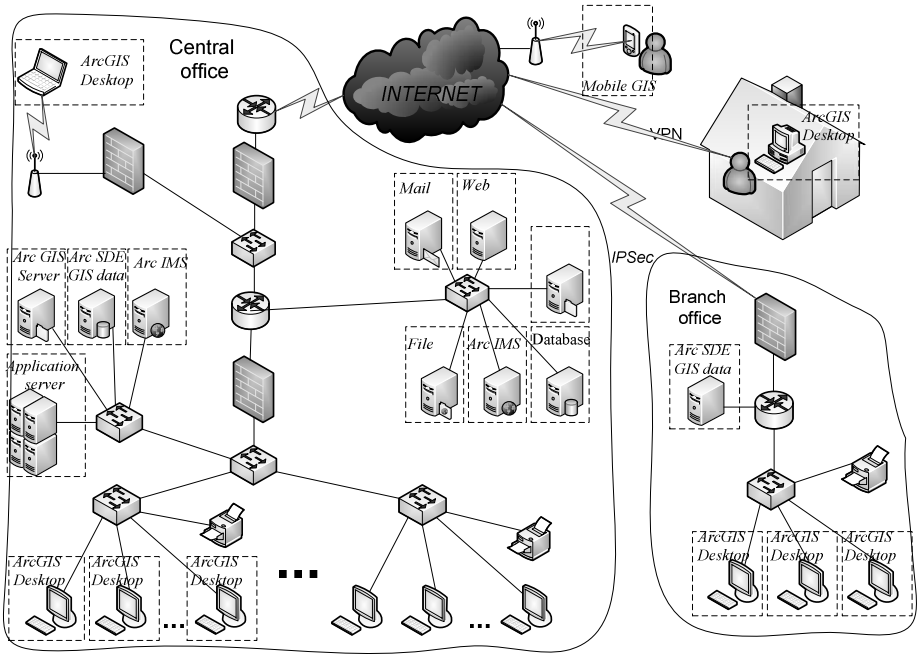

Рис. 5. Инфраструктура ГИС для реализации геоинформационных сервисов с помощью системы ArcGIS

На сетевом уровне в результате сканирования сети ГИС, выявления уязвимостей межсетевых экранов, использования недостатков протоколов маршрутизации (RIP, OSPF), удаленного поиска (ARP, DNS) и управления сетью (ICMP, SNMP), злоумышленник может подменить сетевые маршруты или объекты, например сервер ГИС.

На сетевом уровне за счет возможности удаленного запуска приложений могут реализовываться угрозы, которые приведут к подмене идентификационной информации, искажению данных, нарушению конфиденциальности информации.

Вирусы или программные закладки, занесенные на сервер или рабочую станцию пользователя ГИС, могут обеспечивать удаленный доступ к ним, кражу аутентификационной информации.

Возможны атаки на базу учетных записей SQL сервера СУБД для взлома паролей может использоваться целый ряд программ, после подключения под учетной записью, от имени которой работают службы СУБД, возникает угроза раскрытия данных и чтения геоинформации из баз данных.

С целью реализации угрозы несанкционированного доступа к категорированной информации возможно внедрение в SQL запросов вредоносной дополнительной вставки в пользовательские входные переменные, которые выполняются с командами SQL.

Система защиты должна эффективно функционировать на всех этих уровнях, иначе злоумышленник сможет реализовать ту или иную атаку на геоинформационные ресурсы. Совокупность применения различных механизмов защиты на всех уровнях ГИС позволит построить эффективную и надежную систему обеспечения информационной безопасности ГИС и даст возможность снизить, а во многих случаях и полностью предотвратить возможный ущерб от атак на компоненты и ресурсы системы обработки пространственной информации.

Соблюдение правил авторизации должно обеспечиваться на каждом из вышеперечисленных уровней. Чтобы получить доступ к более критичной информации, пользователь должен иметь соответствующие полномочия для одного и более уровней.

При проектировании программных систем для реализации бизнес-процессов целесообразно использовать встроенные средства защиты. Но встроенные в программные системы средства защиты часто имеют недостатки. Не является исключением и ArcGIS:

- невозможно разрешить и запретить доступ только к определенным слоям данных;
- пользователь, имеющий доступ к web-приложению, получает данные от всех его web-служб даже без разрешения доступа к ним;
- невозможно разграничивать права по выполнению различных видов операций для различных пользователей;
- пользователям корпоративной сети сервера ГИС предоставляется или не предоставляется полный доступ к данным сервера без возможности более детального разграничения доступа.

Применение технологии *системного анализа* к построению *модели управляющей системы* позволит определить её подсистемы, компоненты и способы их соединения, задать ограничения, при которых система должна функционировать, выбрать наиболее эффективное сочетание людей (экспертов, специалистов ИБ, аналитиков), ЭВМ и программного обеспечения.

Если для повышения уровня защищенности идти по пути использования встроенных в программную систему средств защиты, то *на прикладном уровне* защиты можно предложить следующие мероприятия (пример для ArcGIS):

- введение в ролевую модель элементов мандатного доступа (роль, связанная с доступом только к несекретной информации; роль, имеющая доступ как к несекретной, так и к информации ограниченного доступа; роль, имеющая полный доступ);

- создание служб, связанных с одним ресурсом, имеющих сходные названия, но разный набор операций;
- карты можно опубликовать как службы с названиями, отражающими объект и уровень конфиденциальности, и представлять доступ ролям в соответствии с их уровнем доступа;
- исключить локальных пользователей сервера ГИС из групп agsadmin и agsusers, чтобы они были вынуждены использовать web-доступ к серверу через разграничение доступа к службам и приложениям;
- установить при размещении секретной информации в отдельных столбцах таблицы разрешение на уровне отдельных столбцов таблицы, что, однако, усложняет систему разрешений. Для скрытия отдельных столбцов в таблицах можно создать представление или процедуры, которые будут отфильтровывать ненужные столбцы и позволят ограничить операции, доступные пользователям. Установку разрешений целесообразно проводить на уровне схем;
- предотвратить бесконтрольный доступ к КЭШу изображений, минуя систему безопасности;
- использовать криптографические технологии, появившиеся в MS SQL Server 2008 и MS Server 2008, обеспечивающие прозрачное шифрование всей базы данных и логического диска, в том числе системного, на котором могут быть установлены серверы ArcGIS и SQL. Данные меры позволяют устранить возможность копирования БД, изменения конфигурационных файлов, файлов разрешений и служб. При этом целесообразно использовать сертифицированные российские криптопровайдеры, встроенные в зарубежные программные продукты;
- проработать вопросы контроля вводимой в поля и формы ввода информации для защиты от угроз различных инъекций враждебного кода. При использовании аутентификации с помощью клиентских сертификатов от таких полей можно вообще отказаться.

В случае ArcGIS шифрование трафика происходит на сетевом уровне прозрачно для клиента и сервера ГИС, поскольку поддержка протоколов SSL/TLS изначально встроена в ArcGIS Server 9.3 и в web-браузеры. Поддержка IPSec встроена в клиентские и серверные операционные системы Windows. Шифрование трафика с помощью SSL/TLS обычно требует минимальных затрат и настроек и обычно является предпочтительным.

Перечень возможных средств и технологий обеспечения информационной безопасности на уровне ТКС был рассмотрен выше.

Предлагаемые решения, проведенные на основе *методов системного анализа,* позволяют значительно повысить уровень защищенности информационных систем, в том числе и ГИС.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Галицкий А.В., Рябко С.Д., Шаньгин В.Ф.* Защита информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004. – 616 с.
2. *Перегудов Ф.И., Тарасенко Ф.П.* Введение в системный анализ: Учеб. пособие для вузов. – М.: Высш. шк., 1989. – 367 с.
3. *Шумский А.А., Шелупанов А.А.* Системный анализ в защите информации. – М.: Гелиос АРВ, 2005. – 224 с.
4. ГОСТ Р 51624 – 2000.
5. *Семечкин А.Е.* Системный анализ и системотехника. – М.: SvS-Аргус, 2005. – 536 с.
6. *Герасименко, В. А.* Защита информации в автоматизированных системах обработки данных: в 2-х кн. – М.: Энергоатомиздат, 1994.

Статью рекомендовал к опубликованию к.т.н. А.А. Бакиров.

Машкина Ирина Владимировна
Уфимский государственный авиационный технический университет.
E-mail: mashkina_vtzi@mail.ru.
450000, Республика Башкортостан, г. Уфа, ул. К. Маркса, 12.
Тел: +79279277089.
Д.т.н.; профессор.

Сенцова Алина Юрьевна
E-mail: sentsova.alina@yandex.ru.
Тел: +79659255317.
Студентка.

Гузаиров Рустем Муратович
E-mail: callow@mail.ru.
Тел: +79272396699.
Сотрудник УГАТУ.

Кладов Виталий Евгеньевич
E-mail: Kladovv@mail.ru.
Тел: +79173460298.
К.т.н.; доцент.

Mashkina Irina Vladimirovna
The Ufa state Aviation Technical University.
E-mail: mashkina_vtzi@mail.ru.
12, K. Marx's Street, Ufa, 450000, Russia.
Phone: +79279277089.
Dr. of Eng. Sc.; Professor.

Sentsova Alina Uryevna
E-mail: sentsova.alina@yandex.ru.
Phone: +79659255317.
Student.

Guzairov Rustem Muratovich
E-mail: callow@mail.ru.
Phone: +79272396699.
Researcher.

Kladov Vitaliy Evgenyevich
E-mail: Kladovv@mail.ru.
Phone: +79173460298.
Cand. of Eng. Sc.; Associate Professor.

УДК 621.311

В.А. Шарай, О.С. Бурангулова, М.В. Андриуца

МОНИТОРИНГ СОСТОЯНИЯ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ СТРУКТУРНО-СЛОЖНЫХ СИСТЕМ НА ОСНОВЕ ЛОГИКО-ЧИСЛОВЫХ МОДЕЛЕЙ

Рассматривается методика мониторинга состояния надежности и безопасности структурно-сложных технических систем в общем, и систем защиты информации в частности, а также необходимое для реализации такого мониторинга математическое обеспечение, которое позволяет уменьшить его инерциальность. Логико-числовые модели являются основой математического обеспечения для систем мониторинга, основными