# Надежность и безопасность ГИС

## Reliability and security of GIS

**Ключевые слова:** геоинформационная система – geoinfo system; геоинформационный анализ – geoinfo analyses; информационная безопасность – information security; надежность автоматизированных систем – reliability of automated systems; модели угроз – threat models; инженерно-техническая защита – engineering security; несанкционированные действия – unauthorized operations.

Современное развитие ГИС приводит к появлению нового типа проблем в виде конфликтующих структур принципиально нового типа. Это влечет за собой выработку новых требований к высокоорганизованной информационной среде в виде оптимальных показателей надежности, предъявляемых к ней как к автоматизированной системе, и информационной безопасности как объекта информатики.

The modern development of GIS results in coming up of fundamentally new type of problems in a form of conflicting structures of radically new type. It brings about elaboration of new requirements to its highly organized information media in a form of optimum factors of reliability offered to it as automated system, information security as informatics object.

**КАРМАНОВ / KARMANOV A.**
**Андрей Геннадиевич**
(office@itain.spb.ru)
кандидат технических наук, доцент,
начальник центра ситуационного анализа
ЗАО «Институт телекоммуникаций»,
Санкт-Петербург

**ВОРОБЬЕВА / VOROBIEVA A.**
**Алиса Андреевна**
аспирантка Санкт-Петербургского
государственного университета
информационных технологий,
точной механики и оптики,
Санкт-Петербург

Последнее десятилетие на рынке информационных систем и технологий заметно усилился интерес к геоинформационным технологиям. Это объясняется развитием цифровой техники и специальных программных комплексов, позволивших совершить качественный скачок в технологии создания высокоинтеллектуального информационного продукта, состоящего из пространственной и семантической информации. Появились 4D-интерактивные стереомодели местности, способные взять на себя интерфейсные функции управления банком данных для решения как отраслевых, так и межведомственных задач. По сути, появилась виртуальная машина времени, ограниченная исключительно человеческой фантазией. Второй фактор, привлекший внимание – это расширившийся спектр задач, которые стали подвластны современному ГИС-анализу. Это задачи управления процессами в бизнесе, промышленности, экологии, медицине, социальной сфере и, конечно же, решение специальных задач двойного назначения. Третий фактор – телекоммуникационные средства позволили принципиально изменить масштаб пользователей. Сегодня мы уже используем мировые показатели для абонентов Google Map. Современные ГИС-технологии несут в себе системообразующую функцию в информационно-управляющих системах. Даже на понятийном уровне для широкого круга пользователей видно, насколько органично взаимодействуют понятия «инфосфера» и «геоинформатика».

В любой высокоорганизованной среде появляются конфликтующие структуры. Они несут принципиально новый тип проблем в виде конфликтующих структур. Это обеспечение необходимых показателей надежности ГИС как автоматизированной системы, информационной безопасности как объекта информатики. Однако самое интересное заключается в том, что являясь информационной основой центров ситуационного анализа поддержки принятия решений лицами, принимающими решения, они начинают опираться не только на науку, но и на такое понятие, как «искусство». Это и понятно – системы с элементами искусственного интеллекта требуют особого подхода.

Например, к реализации принципа системной безопасности, в котором они конкретизируются в виде совокупности требований к качеству информационно-технологических процессов, реализуемых в ГИС, и к качеству функционирования программно-технической среды.

Основными параметрами качества информационно-технологических процессов выступают такие характеристики, как качество информации и качество обработки информации. Эти параметры характеризуют практическую возможность использования информации при проведении информационно-аналитических исследований. Качество информации характеризуется следующими тремя параметрами: достоверностью, полезностью и полнотой. Свойство «достоверность» определяет потенциальную возможность выработки правильного решения на основе полученной информации. Свойство «полезность» определяет степень соответствия рассматриваемой информации тематике решаемых проблем. Свойство «полнота» определяет степень достаточности информации для выработки решения на ее основе. Качество обработки информации характеризуется следующими тремя уровнями – уровнем обработки, доступности и консолидации. Уровень обработки информации определяет возможность применения тех или иных методов обработки информации в процессе проведения аналитических исследований. Уровень доступности определяет возможность доступа к необходимой информации в процессе проведения исследований с заданными характеристиками свое-временности ее получения. Уровень консолидации информации определяет потенциальную возможность получения необходимой степени консолидации информации в процессе проведения исследований в рамках существующих параметров этой информации по правам доступа.

Основными параметрами качества функционирования программно-технической среды ГИС выступают такие характеристики, как надежность функционирования, вычислимость алгоритмов и оптимальность процедур безопасности. Надежность функционирования определяет уровень работоспособности программно-технической среды ГИС, готовность выполнять свои функции в реальных условиях при конечной надежности аппаратуры и программного обеспечения, в условиях, возникающих из-за ошибок обслуживающего персонала, сбоев, аварий и прочих возмущений. Вычислимость алгоритмов определяет способность программно-технической среды ГИС обеспечивать прагматически-приемлемые временные затраты на доступ, обработку информации и представление ее результатов согласно заданным алгоритмам. Оптимальность процедур безопасности определяет способность программно-технической среды ГИС обеспечивать определенный уровень безопасности при практически-приемлемых затратах на ресурсы и время выполнения соответствующих процедур.

Для реализации перечисленных угроз процессу принятия решения «нарушителем» могут быть проведены деструктивные действия, направленные на изменение характеристик качества информационно-технологических процессов и функционирование программно-технической среды ГИС. Для описания возможных нарушений в процессе функционирования ГИС и взаимосвязанных с ним структур может быть использована трехзвенная модель информационного взаимодействия. В рамках этой модели любой процесс использования информации можно представить в виде трех взаимосвязанных элементов: ИСТОЧНИК информации, НОСИТЕЛЬ информации, ПОЛЬЗОВАТЕЛЬ информации. Информационные процессы, протекающие в ГИС, могут быть описаны в виде множества таких моделей. Под ИСТОЧНИКОМ информации понимается объект/субъект, который может ее порождать и/или имеет право на распространение. Под НОСИТЕЛЕМ информации понимается объект/субъект, который может и имеет право на передачу/хранение/обработку/предоставление как самой первичной информации, так и результатов ее обработки (вторичной информации). Под ПОЛЬЗОВАТЕЛЕМ информации понимается объект/субъект, который может и хочет использовать информацию (первичную и вторичную) для реализации своих функций. Функции ИСТОЧНИКА и НОСИТЕЛЯ информации могут совпадать в рамках одного объекта, а при определенных условиях ПОЛЬЗОВАТЕЛЬ информации играет роль и ИСТОЧНИКА информации. В рамках такой модели можно описать способы реализации рассмотренных угроз информационной безопасности. Обеспечение информационной безопасности ГИС в рассмотренной постановке требует создания комплексной системы информационной безопасности, реализующей многоконтурную, эшелонированную защиту.

Основными направлениями деятельности в решении этой проблемы являются:

– комплексное использование организационных, технологических мер и технических решений, программных, аппаратных и специальных средств, увязанных в единый комплекс;

– использование методов и средств защиты на всех уровнях доступа к защищаемым ресурсам ГИС;

– использование методов и средств контроля доступа к информации, целостности и непротиворечивости данных в процессе хранения и передачи;

– использование для обмена данными сетевых протоколов обмена, предотвращающих несанкционированный доступ к данным;

– использование средств криптографической защиты информации, в том числе – в рамках механизмов реализации электронно-цифровой подписи;

– использование методов контроля электромагнитных излучений средствами вычислительной техники;

– использование эффективных методов и средств обнаружения и борьбы с компьютерными вирусами;

– обеспечение правовой защиты информации;

– разработка методических, нормативно-технических документов и руководств по обеспечению информационной безопасности;

– подбор и подготовка специалистов, реализующих технологические процессы по обеспечению информационной безопасности.

При реализации комплексной системы информационной безопасности необходимо разработать концепцию информационной безопасности, предполагающую описание ГИС как объекта защиты, модели нарушителя, модели угроз и политики безопасности. Описание объекта защиты предполагает спецификацию его информационно-технологических характеристик, в том числе – информационных ресурсов как совокупности структурированных и неструктурированных данных различного типа, информационных процессов прикладного и технологического характера, информационных технологий (включая вычислительную технику и операционные системы, прикладное программное обеспечение и системы управления базами данных, сетевую инфраструктуру), а также обеспечивающей инфраструктуры (помещений и инженерно-технических систем объекта информатизации), конструкторской и нормативной документации на ГИС.

Модель нарушителя информационной безопасности ГИС включает в себя описания классов внутренних и внешних нарушителей, непосредственных и опосредованных способов реализации атаки, локальных и удаленных способов реализации несанкционированных действий, характера несанкционированных действий и т.д. В соответствии с информационно-технологическими характеристиками ГИС, необходимо осуществить оценку возможных каналов утечки информации и разработать модель угроз объекту защиты, включающую в свой состав описания атак, предпринимаемых как внешними, так и внутренними нарушителями, источники угроз, описываемых моделью нарушителя, вид атаки и способ атаки, объект атаки, цель и последствия осуществления атаки, жизненный цикл угрозы и т.д.

Политика безопасности представляет собой совокупности правил, процедур, практических приемов и руководящих принципов в области безопасности, которыми руководствуются в своей деятельности все классы пользователей ГИС, в том числе – перечень контролируемых элементов, профили использования ГИС, стратегию и порядок реагирования на попытки нарушения безопасности, разделение полномочий по администрированию средств защиты и т.д.

## ВЫВОДЫ

В рамках концепции информационной безопасности ГИС необходимо разрабатывать требования к комплексной системе защиты информации, в том числе:

– требования к системе по защите информации от НСД;

– требования к средствам контроля эффективности защиты информации от НСД;

– требования к криптографическим средствам защиты информации, реализующим функции усиленной аутентификации, шифрования, электронно-цифровой подписи, безопасного обмена ключами;

– требования к средствам противодействия скрытому информационному воздействию (вирусы, программные закладки, не декларированные возможности);

– требования к организационно-технологическим мерам защиты;

– требования к системе инженерно-технической защиты объекта информатизации.

С целью конкретизации структуры и состава такой комплексной системы информационной безопасности ГИС вводится 7 уровней безопасности: уровень защиты внешней среды, уровень защиты линий связи, уровень защиты функционирования объектов сети ГИС, уровень защиты сетевого и межсетевого взаимодействия, уровень защиты вычислительных ресурсов, уровень защиты программных ресурсов, уровень защиты информационных ресурсов. Каждый уровень отвечает за обеспечение функций безопасности на отдельно взятом участке ГИС. При

этом каждый из уровней подвержен определенным видам несанкционированных действий нарушителя и каждому из указанных уровней строго соответствуют определенные механизмы обеспечения требований политики безопасности. Уровни безопасности могут быть реализованы автономно, но при этом все они связаны друг с другом. Результат несанкционированных действий на нижнем уровне может прямо или косвенно сказаться на более высоких уровнях, поэтому механизмы безопасности более низких уровней «работают» на обеспечение требований политики безопасности на вышележащих уровнях.

**Литература**

1. *Бир С.* Кибернетика и управление производством. – М.: «Наука», 1965.

2. *Демидов Н.Н.* Разработка средств и методов проектирования информационных технологий управления в кризисных ситуациях. – М., 1998.

3. *Ефремов В.А., Статьев В.Ю.* Место информационной телекоммуникационной системы специального назначения в государственном управлении // Сб. ФАПСИ. – 1994. – № 2.

4. *Жирков О.А., Тихомиров М.М.* Технология презентации свободного аналитического доклада по проблеме ситуации на ситуационном цент-ре // Проблемы информатизации. – 1999. – № 3.

5. *Журавлев Ю.И., Рудаков К.В.* Современные математические технологии прогнозирования и распознавания // Проблемы информатизации. – 1999. – № 2.

6. *Ильин Н.И.* Методология создания системы ситуационных цент-ров высших, федеральных и региональных органов управления. – Информационно-вычислительная техника. – 1997. – № 1.

7. *Ильин Н.И.* Принципы создания общероссийской системы Ситуационных центров на федеральном и региональном уровнях // Проблемы информатизации. – 1997. – Вып. 4.

8. *Иоффин А.И.* Системы поддержки принятия решений // Мир ПК. – 1993. – № 5.

9. *Литвак Б.Г.* Экспертные оценки и принятия решений. – М.: «Патент», 1996.

10. *Лощинин А.А.* Информационные модели территориальных административных систем // Информационные технологии в структурах государственной службы. – 1999. – Вып. 3.

11. *Петров А.В., Тихомиров М.М., Федулов Ю.Г.* Применение ситуационных центров в региональном управлении. – М.: РАГС, 1999.

12. *Петров А.В.* Грамотная разработка решения – основа его правильности // Государственная служба. – 1998. – № 1–2.

13. *Тихомиров М.М.* Принципы групповой автоматизированной подготовки аналитических докладов на ситуационном центре // Информационные технологии в структурах государственной службы. – 1999. – Вып. 3.

14. Системный проект «Комплекс аналитических средств типового ситуационного центра региона – субъекта Российской Федерации». – М.: Межрегиональная ассоциация «Информационное единство», 1998.

15. Типовой многоцелевой ситуационный центр. Основные положения по созданию ситуационных центров автоматизированных систем организационного управления. – М.: НИИ «Восход», 1993.

16. Типовой ГИС для информационной поддержки управленческих решений. Системный проект. – М.: ЦИТИС, 1993.

17. Центр поддержки принятия стратегических решений. – М.: Информационные бизнес-системы, 2002.

18. *Качанова Т.Л. Фомин Б.Ф.* Информационная технология решения стратегических проблем // Проблемы инновационного развития. – 2002. – Вып. 1.

19. *Симаков В.С., Луценко Е.В.* Дельта 2.0. Адаптивная система анализа и прогнозирования состояний сложных систем. – Краснодар: Изд-во Кубанского ГТУ, 2001.