димого разрешения спектральных приборов и набора длин волн излучателей.

Также нами разрабатываются технические принципы и проектный облик оптической орбитальной наблюдательной системы для задач дистанционного зондирования Земли с высоким пространственным разрешением. Основное достоинство разрабатываемой системы обусловлено малой массой оптических элементов, что достигается за счет использования сегментирования главного зеркала и использования адаптивных средств синтеза его поверхности. Адаптация осуществляется по сигналу от гетеродинных фазовых датчиков, измеряющих фазу волнового фронта излучения источника, размещенного в центре кривизны главного зеркала.

Упомянутый подход позволяет обеспечить пространственное разрешение в несколько дециметров с помощью орбитальной системы массой 10-15 кг, что обуславливает низкую стоимость ее вывода на орбиту. Подобные системы наблюдения имеют большое практическое значение и уверенный спрос на получаемую с их помощью информацию. Немаловажное значение эта информация имеет и для наук о земле, включая географию, океанографию, геолого-минералогические и сельскохозяйственные науки.

Ключевым вопросом для рационального использования получаемой информации является построение научных моделей ее интерпретации, которые связали бы интенсивностно-цветовые изменения в изображении с соответствующими параметрами земной поверхности, будь то влажность почвы или температура льда. Решение данной задачи предполагает этап комплексных междисциплинарных исследований с использованием разработанной аппаратуры, когда дистанционное наблюдение проводится одновременно с измерениями максимального набора параметров на местности.

В ЦНИИ РТК накоплен большой опыт организации междисциплинарных исследований, как с привлечением сторонних специалистов, так и с организацией комплексных лабораторий, состоящих из представителей различных специальностей. Это создает широкие предпосылки для активного научного сотрудничества, производственной кооперации и успешного проведения комплекса намеченных междисциплинарных исследований.

КРИПТОГРАФИЯ – ОТ ИЗБРАННЫХ К ШИРОКИМ МАССАМ

Максимушкина Е.В.
Тамбовский государственный университет имени Г.Р. Державина, Тамбов

То, что информация имеет ценность, люди осознали очень давно, – недаром переписка сильных мира сего издавна была объектом пристального внимания их недругов и друзей. Тогда-то и возникла задача защиты этой переписки от чрезмерно любопытных глаз.

История криптографии – ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные.

С широким распространением письменности криптография стала формироваться как самостоятельная наука. Почему же необходимость использования криптографических методов в информационных системах стала в настоящий момент особо актуальна? С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц. С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем еще недавно считавшихся практически не раскрываемыми.

Как отмечал Хорст Файстель (Horst Feistel), в обществе растет беспокойство по поводу того, что компьютеры представляют сейчас или будут представлять в ближайшем будущем опасную угрозу тайне частной жизни. Поскольку многие компьютеры содержат персональные данные и доступны через удаленные терминалы, они являются непревзойденным средством накопления больших массивов информации об отдельных людях и группах людей. Поэтому компьютерные системы подобного назначения должны быть приспособлены к защите хранящейся на них информации от всех людей, за исключение, естественно, тех, кому разрешен доступ к ним, путем зашифрования данных в формы, весьма устойчивые к попыткам взлома.

Не так давно информация приобрела самостоятельную коммерческую ценность и стала широко распространенным, практически рядовым товаром. Ее производят, хранят, транспортируют, продают и покупают, а значит – воруют и подделывают – и, следовательно, ее необходимо защищать. В современном обществе все больше проявляется информационная обусловленность, успех любого вида деятельности все сильней зависит от обладания определенными сведениями и от отсутствия их у конкурентов. И чем сильней проявляется указанный эффект, тем больше потенциальные убытки от злоупотреблений в информационной сфере, и тем больше потребность в защите информации. Одним словом, возникновение индустрии обработки информации неумолимо привело к возникновению индустрии средств защиты информации. И она включает в себя не только серьезнейшую работу по усовершенствованию уже имеющихся и созданию качественно новых систем шифрования, но и обучение в этом направлении.

Учитывая все нарастающие потребности разных сфер общества в специалистах по защите информации, многие вузы страны начинают активную подготовку студентов по соответствующим специальностям. Но не все четко себе представляют, с чем сопряжено изучение такого предмета, как криптография, являющегося одной из основных составляющих такой подготовки. (Среди всего спектра методов защиты данных от нежелательного доступа особое место занимают криптографические методы.) А по-

скольку теоретическая криптография – очень «математизированная» научная дисциплина, то для изучения этого предмета необходимо знать (или, как минимум, иметь общие сведения) такие понятия высшей алгебры, как вычеты и сравнения по модулю, группа, кольцо, линейные преобразования кольца, построение больших простых чисел. Также необходимы знания по теории вероятностей, теории кодирования. Кроме того, поскольку шифрование – это достаточно трудоемкий с точки зрения вычислений процесс, то для возможности компьютерной реализации таких алгоритмов необходимо обладать навыками низко- и высокоуровневого программирования, обладать навыками работы в сети и с самой сетью.

ВЕРОЯТНОСТНАЯ ОЦЕНКА НАДЕЖНОСТИ ЭКСПЛУАТИРУЕМЫХ СООРУЖЕНИЙ С ПОВРЕЖДЕНИЯМИ

Муравьева Л.В.
Волгоградский государственный архитектурно-строительный университет, Волгоград

В настоящее время в строительных науках вероятностные методы применяются лишь узким кругом специалистов, занимающимися теорией надежности строительных конструкций. Создание надежной, безопасной конструкции, выполнение технических и экономических требований – это задачи, которые необходимо выполнить при проектировании любого сооружения. Однако использование этих методов совершенно необходимо в области оценки работоспособности эксплуатируемых сооружений, где важную роль играют случайности реального мира.

Рассмотрим в качестве примера, трубопровод, в настоящее время расчет надежности линейной части трубопроводов до сих пор проводят на основе традиционных методов строительной механики с использованием концепции коэффициентов запаса. Но во время эксплуатации он испытывает нагрузки и воздействия, которые, в общем случае, представляют собой случайные функции. Но детерминированная модель, даже очень сложная, позволяет ограничиться однократным решением задачи на ЭВМ, что вполне приемлемо для практики.

Оценка же стохастического поведения сложной системы и вероятность выхода ее параметров за область допустимых состояний (выброс) проводится в настоящее время, как правило, методом статистического моделирования. Однако, для получения необходимых статистических данных в области малых вероятностей требуется проведение порядка 10^3 – 10^4 испытаний. В этом случае решение задачи может быть получено только с использованием упрощенных базовых моделей поведения системы.

Сегодня актуальным становится вопрос внедрения вероятностных методов расчета в практику.

Поэтому в настоящей статье предложен инженерный подход к оценке надежности сложных систем, позволяющий резко сократить число испытаний при статистическом моделировании (до 2^{n-1}, где n - число учитываемых параметров состояния). Он может быть реализован на основе применения стандартных пакетов прикладных программ, широко использующихся в проектной и исследовательской практике. При вероятностном расчете можно использовать нормативные рекомендации по определению физико-механических характеристик материалов трубопроводов и нагрузки. Это создает благоприятные условия для внедрения вероятностных методов расчета в практику.

При решении задачи о состоянии конструкции в условиях эксплуатации, участок магистрального газопровода может быть охарактеризован конечным числом независимых параметров. Часть из которых характеризует нагрузки, другие – прочность материалов, третьи - отклонение реальных условий работы конструкции.

Уравнение границы области допустимых состояний конструкции представляется в виде

$$\tilde{y}(x_1, x_2, x_3) = 0$$

где $\tilde{y}(x_1, x_2 \ldots x_n)$ - функция работоспособности. Для оценки эксплуатационной надежности оболочки трубопровода предложено использовать характеристику прочности, которую А.Р.Ржаницын назвал резервом прочности.

Параметры системы: внутреннее давление транспортируемого продукта $X_1 = \tilde{p}$; температурное воздействие транспортируемого продукта $X_2 = \Delta\tilde{t}$; весовое воздействие грунта засыпки $X_3 = \tilde{q}(x)$. При проведении моделирования в i-й точке факторного пространства учитывается изменение фактора X_3 по длине рассматриваемого линейного участка магистрального газопровода.

Предложена модель, определяющая функцию надежности конструкции в зависимости от изменений уровней параметров весового и эксплуатационного воздействия.

Получение модели, описывающей реакции изучаемой системы на многофакторное возмущение, является одной из задач математического планирования эксперимента. Наиболее распространенными и полно отвечающими задачам статистического моделирования являются полиномиальные модели. Тогда зависимость между уровнями факторов и реакцией системы, представляем в виде полинома первого порядка

$$y = b_0 + b_1\tilde{X}_1 + b_2\tilde{X}_2 + b_3\tilde{X}_3 + \\ + b_{12}\tilde{X}_1\tilde{X}_2 + b_{23}\tilde{X}_2\tilde{X}_3 + b_{123}\tilde{X}_1\tilde{X}_2\tilde{X}_3$$

Полный факторный эксперимент дает возможность определить коэффициенты регрессии, соответствующие не только линейным эффектам, но и всем эффектам взаимодействий.

Условиями работоспособности конструкции в этой задаче является не превышение прогибов и напряжений в конструкции, значений условия прочности при определенном уровне нагружения.

Основным объектом анализа являлись нагрузки, которым подвергается трубопроводная конструкция во время работы..