Радиолокация земной среды и инженерных сооружений

Ю. Виноградов,
В. Котенков,
В. Лисицын,
О. Пустырев

Информация о структуре верхних слоев земной поверхности и находящихся в них объектах чрезвычайно важна для обеспечения безопасности в промышленном и жилом строительстве, на транспорте, при решении экологических задач. Один из наиболее высокопроизводительных, информативных и точных методов ее получения — радиолокационный. В разработке эффективных средств исследований в этой области — георадиолокаторов — значительных успехов добились специалисты НПП ЛОКАС, Всероссийского НИИ радиотехники и Правдинского завода радиорелейной аппаратуры. Созданные ими антенные системы награждены дипломами и золотой медалью Всемирного салона изобретений "Брюссель—Эврика".

Суть георадиолокации — в периодическом облучении исследуемой среды электромагнитными волнами, приеме и анализе отраженных от неоднородностей этой среды волн. Как правило, длительность излучаемых электромагнитных волн мала (несколько единиц или десятков наносекунд). В сравнении с другими известными методами электроразведки, радиолокационный характеризуется высокой разрешающей способностью, что позволяет выявлять природные локальные неоднородности и техногенные объекты (коммуникации, археологические и скрытые объекты, подкопы и т.п.).

Важный параметр, определяющий компромисс между достижимой глубиной зондирования и разрешающей способностью по глубине, — диапазон частот излучаемого сигнала. Рабочие частоты современных георадиолокаторов (ГРЛ) находятся в диапазоне 1—2000 МГц, а отношение разности и суммы граничных частот спектра излучаемого ГРЛ-сигнала превышает 0,85. Поэтому формировать, излучать и обрабатывать сверхширокополосные сигналы необходимо без несущей, что существенно отличает ГРЛ от традиционных радиолокаторов. Еще одно его отличие от традиционной радиолокации, рассчитанной на излучение сигнала в сравнительно однородную воздушную атмосферу, состоит в том, что для георадиолокационной технологии характерно значительное затухание радиоволн в исследуемых средах, а также электрофизическая неоднородность и дисперсионность характеристик этих сред. Таким образом, объектами зондирования в этом случае являются не только искомые предметы, находящиеся в среде, но и сама среда.

В связи с жесткими условиями работы ГРЛ должны нормально функционировать при температуре -30...+50°С, обладать вибростойкостью при ускорении до 5g и ударопрочностью до 20g, высокой надежностью, низким электропотреблением, малыми габаритами и т.п., обеспечивая стабильные параметры при излучении сигналов с амплитудой до нескольких сотен вольт и длительностью от 1 до 24 нс. Кроме того, от георадиолокационной системы требуется уверенный прием, регистрация, обработка и отображение информации. ГРЛ, отвечающие таким требованиям, представляют собой эффективное средство получения информации о структурной неоднородности исследуемой среды. Не случайно в последнее время интерес к системам такого типа быстро растет [1—6].

Всеми перечисленными достоинствами обладают подготавливаемые к производству ГРЛ серии ЛОКАС третьего поколения — ЛОКАС-3, которым предшествовали ЛОКАС-1, переданный в серийное производство в 1986 году, и ЛОКАС-2, запущенный в серию в 1991-м. Тогда же был создан модернизированный вариант ЛОКАС-2М, оснащенный автоматизированной системой управления процессами зондирования, регистрации и оперативного отображения информации, размещаемой в автофургоне. Система управления ЛОКАС-3 представляет собой компактное переносное устройство, что значительно облегчает работу с ГРЛ.

Принципиальная блок-схема ГРЛ серии ЛОКАС показана на рис. 1. Ключевые элементы локатора — антенные системы — выполнены в виде раздельных однотипных устройств излучения и приема зондирующих сигналов. Собственно антенна представляет собой плоскостной изолированный симметричный вибратор с полупроводящим экраном. Отношение интенсивности излучения в изучаемую среду и в окружающее пространство составляет не менее 20 дБ. Это позволяет вести исследования в условиях плотной городской застройки, свайных полей, внутри помещений и т.п. Антенна смонтирована в кейсе из стеклопластика совместно с передающим или приемным устройством. Генератор передатчика выполнен по схеме с внешним возбуждением и формирует сигнал в виде одного периода синусоиды.

Приемный тракт состоит из входного аттенюатора, построенного на коммутируемых резистивных элементах с глубиной регулирования 64 дБ, малошумящего широкополосного усилителя,

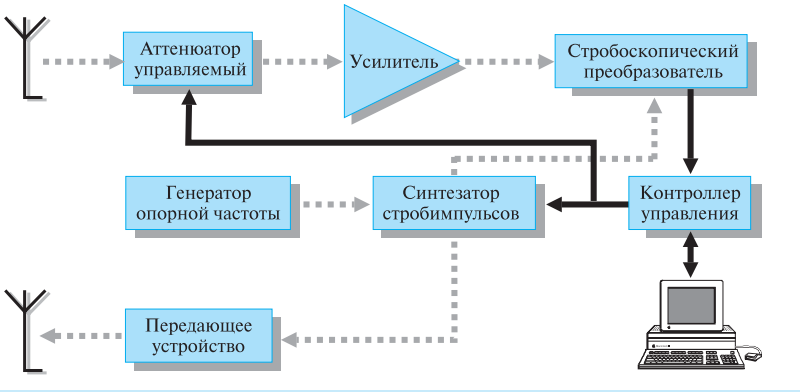

Рис. 1. Блок-схема ГРЛ

стробоскопического устройства выборки и хранения. Временное расположение строб- и синхроимпульса, задаваемое цифровым синтезатором, определяется управляющим кодом и изменяется с заданным интервалом дискретизации по временной шкале с максимальным значением 1,2 мкс. Синхронизация обеспечивается опорным кварцевым генератором. Формирование управляющих кодов, прием кодов от устройства выборки и хранения, обслуживание канала сопряжения с компьютером осуществляется программируемым контроллером управления. В ГРЛ может применяться IBM-совместимый компьютер, который обеспечивает управление адаптацией режимов работы ГРЛ, наблюдением, регистрацией и обработкой информации.

В НПП ЛОКАС более чем за десять лет накоплен значительный опыт использования технологии подповерхностного радиолокационного зондирования в инженерно-геологических изысканиях под объекты промышленного, жилищного, дорожного и специального строительства в различных регионах России [7—18]. С помощью ГРЛ ЛОКАС-2 и ЛОКАС-2М решались две основные задачи: исследование геологического строения разреза и прослеживание отдельных его границ, а также изучение коммуникаций и строительных конструкций. Оценка возможности применения ГРЛ для диагностики технического состояния и контроля качества аэродромных сооружений показала, что ЛОКАС 2 и ЛОКАС 2М могут выявить асбоцементные коллекторы диаметром 0,6 м, расположенные под асфальтобетонными покрытиями аэродрома на глубине четырех метров, а также конструктивные элементы рулежных дорожек и взлетно-посадочных полос (швы, арматура и т.п.), локальные и протяженные неоднородности и изменения структуры жесткого покрытия [10—12].

Опытно-демонстрационные работы ГРЛ ЛОКАС-2 на объектах МосНПО РАДОН в декабре 1993 — июне 1994 года показали возможность и целесообразность применения радиолокационного зондирования в технологиях обезвреживания радиоактивных отходов. Сегодня это единственный метод, позволяющий изучать состояние и сезонные изменения закрытых емкостей захоронения радиоактивных отходов без нарушения целостности конструкций, что имеет неоценимое значение для защиты окружающей среды от воздействия радионуклидов [13].

В 1994 году специалисты НПП ЛОКАС и треста МосЦТИСИЗ Минстроя РФ исследовали грунты под одной из московских школ, чтобы определить причины деформации аварийного здания и выработать рекомендации по его безопасной эксплуатации [14]. Наличие и характер обводнения грунтов были выявлены с использованием изделия 17ГРЛ-2 и программно-аппаратного комплекса георадиолокационных данных Geoshell/Geobase 2.0 НПП ЛОКАС. Радиолокационное зондирование помогло обнаружить активный подземный эррозионный процесс у заднего северного угла здания, который снижал прочность грунтового основания и приводил к возникновению и развитию процессов разрушения в фундаменте и стенах здания (рис. 2).

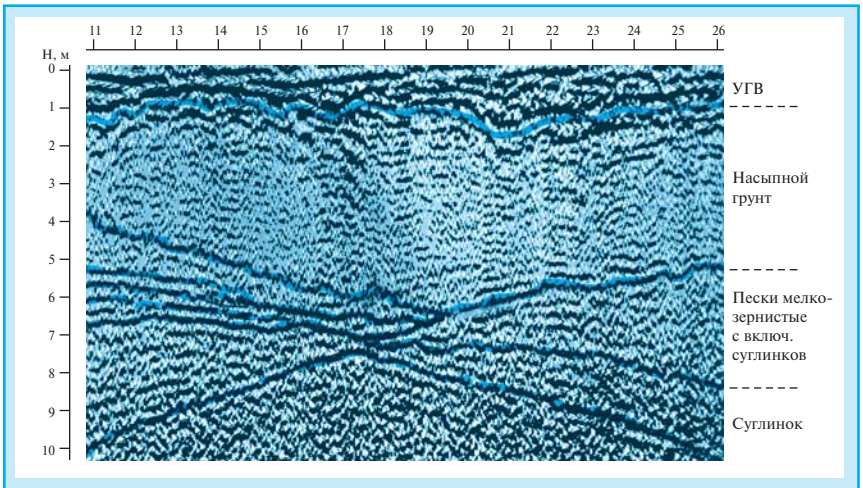

Рис. 2. Фрагмент радиолокационного разреза грунтов протяженностью 30 м перед фасадом здания школы

Настораживают результаты проведенного в конце 1997 года радиолокационного зондирования дренирующего участка плотины в Истринском районе Московской области [18]. Зондирование на глубину восемь метров позволило составить представление о состоянии тела плотины и контактной зоны с ложем. На представленном фрагменте поперечного профиля длиной 15 м водоток уходит под кромку железобетонного покрытия верхнего бьефа с аномальными зонами проникновения в тело плотины (рис. 3). Эта зона прослеживается от 1,2 м (левая сторона рисунка) до 3,0 м (правая сторона). Проведенное обследование позволило выявить в теле плотины общую аномальную зону грунтов с высоким содержанием песчаной фракции, что обусловило ее обводнение и образование проницаемых каналов с выносом наружу грунтов тела плотины.

Итак, технологии подповерхностного радиолокационного зондирования помогают решить целый комплекс проблем, связанных с безопасностью. В инженерной геологии, например, они способны повысить надежность и качество инженерно-геологических изысканий и обеспечить принятие оптимальных проектных решений. Инженерный мониторинг зданий и сооружений с использованием ГРЛ позволит предотвращать катастрофы, связанные с их разрушением. Режимные наблюдения за состоянием полотна автомагистралей увеличат их пропускную способность и повысят безопасность движения. Такие же наблюдения за взлетно-посадочными полосами аэродромов, несомненно, сделают более

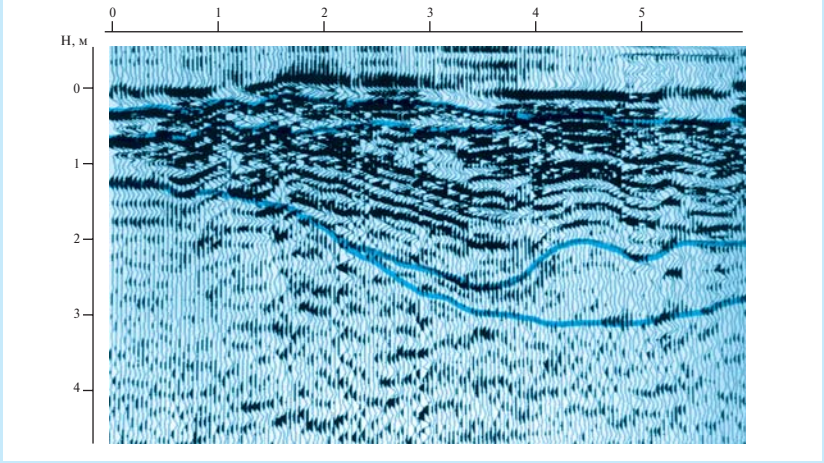

Рис. 3. Фрагмент поперечного радиолокационного профиля с аномальной зоной разуплотнения

безопасными авиаперевозки. Своевременное выявление дефектов защитных сооружений, обеспечение безаварийной эксплуатации дамб, плотин, нефте- и газопроводов с помощью ГРЛ поможет уберечь природу и человека от многих экологических катастроф.

Сфера применения георадиолокационной технологии непрерывно расширяется. Сегодня накопленный в этой области научно-технический потенциал позволяет приступить к созданию аппаратно-программных средств для обнаружения и обезвреживания мин, а также поиска пострадавших в завалах людей и организации аварийно-спасательных работ.

Литература

1. **Финкельштейн М.И., Кутев В.А., Золотарев В.П.** Применение радиолокационного подповерхностного зондирования в инженерной геологии. – М.; Недра, 1986.
2. Geological survey of Canada, Paper 90-4, Ground Penetrating Radar, 1992.
3. **Котенков В.Е., Смирнов Н.С., Хабаров Ю.Е.** Георадиолокаторы подповерхностного зондирования. – Вестник ноу-хау, 1993, № 3.
4. **Аленкович Г., Левитас Б., Минин А.** Портативный георадиолокатор для подземных исследований. – Современные технологии автоматизации, 1996, №1.
5. **Помозов В., Семейкин Н. и др.** Георадар.– Современные средства автоматизации, 1997, №3.
6. Георадар "ЗОНД". – Электроника: НТБ, 1997,№2.
7. Отчет о результатах испытаний георадиолокатора 17ГРЛ1 на железнодорожной линии Беркакит - Томмот. – Мосгипротранс, 1985.
8. Акт "Испытания экспериментального образца георадиолокатора 17ГРЛ1 на объектах Северо-Муйского тоннеля", Бамтоннельстрой, Северомуйск, 1985.
9. Применение метода радиолокационного зондирования при инженерных изысканиях для строительства. Отчет И-2155. – Госстрой РСФСР, МосЦТИСИЗ, 1988.
10. Опытно-производственные испытания георадиолокатора 17ГРЛ2 на магистральной рулежной дорожке аэродрома Домодедово. Протокол испытаний. ГПИ АЭРОПРОЕКТ- ВНИИРТ, 1991.
11. Демонстрационные испытания георадиолокатора 17ГРЛ2 на рулежных дорожках аэродрома г.Клин. Протокол испытаний. – в/ч 52689 - ВНИИРТ, 1992.
12. Отчет "Исследование и экспериментальная отработка подповерхностного георадиолокатора для контроля состояния взлетно-посадочной полосы". – НИР Прогресс. НПП ЛОКАС, 1994.
13. Опытно-демонстрационные работы с георадиолокатором ЛОКАС-2 на полигоне МосНПО РАДОН. Отчет МосНПО РАДОН - НПП ЛОКАС. – Москва, 1994 г.
14. Результаты исследования грунтов, полученные с помощью георадиолокатора 17ГРЛ2, при проведении инженерно-геологических изысканий на объекте Школа № 497. – НПП ЛОКАС,1994.
15. Результаты георадиолокационного зондирования на объекте ст. Решетиха Горьковской ж.д. Протокол испытаний. – НПП ЛОКАС,1995.
16. Опытно-демонстрационные испытания георадиолокатора 17ГРЛ2М на объектах Мостеплосети. Протокол испытаний. – НПП ЛОКАС,1996.
17. Отчет об инженерно-геологических условиях строительства офисно-жилого здания на проспекте Андропова 2/10. – Минстрой России, ИМЦстройизыскания,1997.
18. Результаты георадиолокационных исследований дренирующего участка тела плотины рыбокомбината "Малая Истра". Отчет. – НПП ЛОКАС, 1997.

Fastgate — система быстрой индентификации пассажиров авиалайнеров

Дайджест

В международном аэропорту Бермуд проходит испытания новая автоматизированная система идентификации пассажиров фирмы IBM. В системе объединены сетевая технология и перспективные биометрические методы идентификации, что позволяет быстро и надежно устанавливать личность пассажира. Путешественники предъявляют системе Fastgate стандартную кредитную, туристическую или коммерческую карту, официально зарегистрированную любой организацией, которая при выдаче карты заносит в досье имя, адрес, дату рождения, номер паспорта, а также вносит в карту биометрические данные клиента (отпечатки пальцев, геометрию ладони или характер речевого сигнала). При регистрации в аэропорту пассажир вводит карточку в считывающее устройство и отвечает на несколько базовых вопросов с помощью сенсорного экрана. Для установления личности система Fastgate сравнивает биометрическую информацию и через непосредственное соединение в режиме on-line запрашивает у базы данных подтверждение полномочий. Это позволяет удостовериться в отсутствии каких-либо факторов, препятствующих допуску пассажира в самолет. Как правило процесс проверки занимает менее 15 сек.

Материалы фирмы IBM: http://www.chips.ibm.com/sige

Зеркала, зеркала, везде зеркала

Дайджест

Фирма Micros разработала программные средства распознавания лица, названные True Face Access. Для сравнения видеоизображения лица человека с хранимым в памяти системы используется технология нейронной сети. При установлении соответствия человек получает право доступа к охраняемому объекту. В разработке системы принимали участие специалисты Eastman Kodak и Sun Microsystems.

http://www.micros.com

Пропуск — человеческое тело

Дайджест

Вряд ли кому-то понравится идея пропустить электрический ток через его тело. Однако специалисты Исследовательского центра фирмы IBM в Сан-Хосе предлагают использовать естественную электропроводность тела для передачи данных, утверждая, что это совершенно безопасно. Совместно с учеными Массачусетского технологического института они разработали персональную сеть (Personal Area Network — PAN), работающую с токами в несколько наноампер. Возбуждаемое при этом электрическое поле в тысячу раз меньше поля, возникающего при расчесывании волос. Пересылаемая и принимаемая информация хранится и обрабатывается микропроцессорами, которыми оснащены приемники и передатчики. Первоначально PAN-блок по своим размерам был сопоставим с пачкой сигарет, сейчас — с кредитной картой. Возможности новой технологии огромны. Самое простое ее применение — защита от несанкционированного доступа, самое фантастичное — обмен данными между людьми путем простого рукопожатия. Сегодня вокруг нас множество цифровых электронных устройств. Но совместно использовать их данные и ресурсы можно будет только тогда, когда они научатся нас различать. Объединение этих устройств в сети откроет такую возможность, предоставив нам новые услуги, и сделает нашу жизнь еще более комфортной.

Данные фирмы IBM, http://www.chips.ibm.com

Миру угрожают электронные гангстеры

Правоохранительные органы стран "большой восьмерки" утвердили план совместной борьбы с киберпреступностью. Документ предусматривает безоговорочную выдачу компьютерных взломщиков в руки правосудия тех стран, на территории которых было совершено преступление. И вскоре США был передан гражданин России Владимир Левин, арестованный еще в 1995 году и находившийся в лондонской тюрьме. Ему было предъявлено обвинение в… похищении 10 млн.долл. со счетов клиентов одного из самых надежных банков Северной Америки — Сити-банка. Сидя в своей квартире в Питере, компьютерный "медвежатник" внедрялся в сеть банка, снимал со счетов клиентов деньги и направлял их "тихой скоростью" в разные города и страны. А затем через подставных лиц пытался собрать дань. Случай был воспринят как сенсация. А между тем, Владимир Левин — вовсе не первый электронный гангстер. Киберпреступность заявила о себе еще 30 лет назад и с тех пор приобрела такие масштабы, что, по мнению ученых, сравнялась с ядерной, химической и бактериологической опасностью. И это совсем не преувеличение…

…Не спасли банк ни бронированные двери, ни специальные запоры, ни вооруженная охрана. В денежное хранилище никто не входил. На сейфовых замках не осталось ни царапины, ни отпечатка пальца. Однако 123 тыс. долл. исчезли бесследно. Это таинственное похищение произошло в одном из столичных филиалов крупнейшего российского банка. Доллары испарились в буквальном смысле со скоростью света. Сыщикам стоило немалого труда обнаружить преступника (точнее, преступницу). Дело в том, что некто В. Виноградова совершила грабеж, не покидая своего служебного кабинета. Она проникла в денежное хранилище … по проводам, используя вместо традиционной для банковских грабителей отмычки клавиатуру компьютера. Несколько нажатий на клавиши, и электрические сигналы переместили немалое состояние со служебного счета Инкомбанка на частные счета друзей "взломщицы".

На этот раз злоумышленник был обнаружен. Но в целом криминальное использование современных информационных технологий делает компьютерную преступность не только весьма прибыльным, но и достаточно безопасным делом. И не зря подкомитет ООН по преступности ставит эту проблему в один ряд с терроризмом и наркобизнесом. В одном из банков Великобритании с помощью компьютера в одно мгновение был похищен миллиард долларов. Чем не преступление века? А всего (по самым скромным подсчетам) ежегодные потери от компьютерной преступности в Европе и Америке составляют десятки миллиардов долларов!

В 90% случаев сыщикам даже не удается выйти на след преступников. И это в Америке, где первое подобное правонарушение было зафиксировано еще в 1966 году и полиция уже накопила некоторый опыт в этой области. В России же подразделение по борьбе с хищениями, совершаемыми с использованием электронных средств, создано лишь в январе 1996 года. С тех пор возбуждено уже немало уголовных дел, но нет уверенности, что все они будут доведены до суда. Дела разваливаются, так как выявить личность преступника порой просто невозможно. Так, еще в 1993 году в компьютерную сеть Центробанка неизвестным лицом была введена команда о переводе более 68 млрд. руб. на другие счета. Преступники не найдены. В начале 1995 года злоумышленники через компьютерную сеть одного из московских банков фиктивно перевели на его счет 2 млрд.руб., попытавшись потом перевести эту сумму на другие счета. Преступление было предотвращено. Но уголовное дело приостановлено "за неустановлением виновных лиц"…

Прокомментировать ситуацию согласился программист одной из московских фирм, который, правда, попросил не называть его имени.

— Проблема даже не в том, что наши сыщики плохо работают или российские банки экономят на защите своих компьютерных сетей. Уверен, что при желании сумел бы безнаказанно проникнуть сквозь любую защиту. Не верите? Вспомните про американского школьника, который буквально поставил на уши ЦРУ, шутки ради проникнув в сверхсекретные файлы. А там защитные коды не чета нашим банковским. Не сложно написать и "мерцающую программу", которая через модемную связь произвольно включалась бы в счета разных предприятий, организуя денежные переводы за какие-либо "услуги", скажем, за маркетинг. Как поймать такого воришку, если сигналы легко перебрасываются через спутник и могут поступать в тот же Центробанк хоть из Зимбабве, хоть с Берега Слоновой Кости? А если компьютер-взломщик и найдется, то выяснится, что он работает в автономном режиме в каком-нибудь ничейном сарае… Деньги прокручиваются через несколько банков, и если их след все же обнаружится, конечный получатель только пожмет плечами: мол сам удивляюсь, откуда они, — и ничего с ним никто не сделает. Уверен, что при тотальной криминализации нашего общества компьютерная преступность не стала еще в России национальным бедствием лишь из-за не менее тотальной технической отсталости.

Компьютерная преступность — это не только хищения денег. Это и "шалости" с электронными вирусами, которые приводят порой к весьма плачевным последствиям. Америка уже накопила немалый печальный опыт в этой области. В 1988 году электронный вирус, неведомым образом попавший в компьютер Мичиганского госпиталя, перепутал в электронной памяти фамилии пациентов, их диагнозы и назначенное лечение, поставив под угрозу жизнь многих больных… В том же году молодой лоботряс Корнелл Морисс заразил вирусом крупнейшую компьютерную сеть Internet, что вывело из строя 6 тыс. компьютеров в 700 университетах, фирмах, федеральных агентствах. Ущерб составил 100 млн.долл. Исследовательскому центру НАСА пришлось на два дня закрыть свою сеть, чтобы восстановить нормальное обслуживание 52 тыс. пользователей. Сегодня, когда сеть Internet стала поистине всемирной, последствия подобной "шалости" трудно предугадать.

В России проблемой компьютерных вирусов занимается группа специалистов ФСБ, у которых нам, к сожалению, не удалось получить информацию о масштабах этого явления в нашей стране. Но программисты утверждают, что сейчас по компьютерам кочует около 5 тыс. разных вирусов и каждую неделю появляются пять новых. По их мнению, большая часть этой "инфекции" создается в границах бывшего СССР. Оценить степень ее опасности можно на примере уголовного дела, возбужденного прокуратурой Литвы в 1992 году. Тогда "электронная зараза" попала в компьютер Игналинской атомной электростанции, что привело к выводу из строя ее защитной системы. Еще чуть-чуть, и был бы второй Чернобыль…

Компьютеризация России — естественный, неизбежный и очень важный для страны процесс. Но надо помнить, что принесет он, к сожалению, не только благо. Уже сегодня киберманьяку вполне по силам оставить часть страны без света и телефонной связи или парализовать работу аэропортов и железных дорог. Самое неприятное, что весьма непросто отличить мелкое компьютерное хулиганство от серьезных попыток преднамеренного взлома сетей стратегических объектов. Поэтому вполне понятно, что с ростом зависимости страны от компьютеров компьютерные сети необходимо включить в число объектов стратегического назначения со всеми вытекающими отсюда последствиями. Если этого не сделать, в недалеком будущем с помощью телекоммуникационных средств злоумышленники, не вставая с дивана, смогут легко совершать террористические акты и даже небольшие государственные перевороты "в отдельно взятой стране". И все это легким нажатием кнопки "мыши"…

И. Царев