заміною реальних фізичних об'єктів і процесів, але і передбачати отримання нових результатів, властивостей об'єкта.

Обчислювальна середа в усьому світі змінюється дуже швидко, і одночасно з цим розширюються наші уявлення про сфери застосовності комп'ютерів. Тому незаперечним є необхідність більш широкого застосування навчальних комп'ютерних моделей в системі діяльності викладача фізики, що працює в системі довузівської освіти.

Вирішенню проблем подальшого розвитку в системі підготовки до вступу у ВНЗ при викладанні фізики, повинна сприяти тісна інтеграція змістового та процесуального блоків курсу загальної фізики в рамках модульного навчання. Основою індивідуалізації в модульних системах є самонавчання. Воно сприяє розвитку самостійності слухачів, критичного мислення і тому подібного. Ефективна організація самонавчання може бути здійснена шляхом широкого використання нових інформаційно-телекомунікаційних технологій.

Вдосконалення і розвиток навчального фізичного експерименту повинні здійснюватися комплексно. Високий рівень вивчення фізики в системі довузівської підготовки може бути зумовлений удосконаленням існуючих та пошуком нових методів і засобів навчання. Один з конструктивних принципів побудови шкільного курсу фізики за сучасною концепцією - розроблення педагогічних програмних засобів для використання на уроках фізики відео-і комп'ютерної техніки.

Список литературы

1. Бєліков, В.А. Види пізнавальної діяльності учнів у процесі навчання фізики / В.А. Бєліков // Удосконалення процесу навчання фізіки: Межвуз.сб.науч.тр. - Челябінськ, 1984. - С. 29-37.

2. Давидов, В.В. Про поняття розвиваючого навчання / В.В. Давидов / / Педагогіка. - 1995. - № 1. - С. 29-32.

НЕОБХОДИМОСТЬ И ПОТРЕБНОСТЬ В ЗАЩИТЕ ИНФОРМАЦИИ

О.Н. Шибко
(Украина, Днепропетровск, ГВУЗ «Национальный горный университет»)

Жизнь современного общества немыслима без современных информационных технологий. Компьютеры обслуживают банковские системы, контролируют работу атомных реакторов, распределяют энергию, следят за расписанием поездов, управляют самолетами, космическими кораблями. Компьютерные сети и телекоммуникации предопределяют надежность и мощность систем обороны и безопасности страны. Компьютеры обеспечивают хранение информации, ее обработку и предоставление потребителям, реализуя таким образом информационные технологии. Тенденция развития современных технологий характеризуется постоянным повышением значения информации.

Производственные процессы имеют в своём составе материальную и нематериальную составляющие. Первая - это необходимое для производства оборудование, материалы и энергия в нужной форме (то есть, чем и из чего

изготавливается предмет). Вторая составляющая - технология производства (то есть, как он изготавливается). Кроме производственных процессов информация играет большую роль, а иногда и является основой деятельности управленческих организаций. Сегодня у руководства большинства организаций, предприятий и банков не остается сомнений в необходимости серьезно заботиться об информационной безопасности. Здесь и необходимость сохранения различных видов тайн, обеспечение безопасности электронных документов да и безопасность самих работников организации напрямую связана со степенью информационной безопасности. Рост применения современных информационных технологий в различных сферах делает возможным распространение разных злоупотреблений, связанных с использованием вычислительной техники. в настоящее время и в ближайшем будущем наибольшую опасность представляет информационная незащищенность. Поэтому при обеспечении информационной безопасности организации необходимо учитывать, что обмен информацией является первейшим условием жизнедеятельности каждой организации. Известно, что система обеспечения информационной безопасности организации включает в себя сбор, классификацию, анализ, оценку, защиту и распространение актуальной информации для обеспечения защиты ресурсов организации с целью оптимальной реализации ее целей и интересов. В деятельности организации могут возникать четыре вида информационных рисков, а именно:

– риск утечки информации, необходимой для функционирования организации;

– риск использования в деятельности организации необъективной информации;

– риск отсутствия у руководства организации объективной информации;

– риск распространения кем-либо во внешней среде невыгодной или опасной для организации информации.

Расширение применения современных информационных технологий делает возможным распространение различных злоупотреблений, связанных с использованием вычислительной техники (компьютерных преступлений). Для противодействия им или хотя бы уменьшения ущерба необходимо грамотно выбирать меры и средства обеспечения защиты информации от умышленного разрушения, кражи, порчи, несанкционированного доступа, несанкционированного чтения и копирования. Необходимо знание основных законодательных положений в этой области, организационных, экономических и иных мер обеспечения безопасности информации. Создать абсолютно непреодолимую систему защиты принципиально невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту. Поэтому имеет смысл вести речь только о некотором приемлемом (разумно-достаточном) уровне безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности и ресурсов компьютерной системы и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы

приемлемыми. Часто приходится создавать систему защиты в условиях большой неопределённости. Поэтому принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Естественно, что для обеспечения возможности варьирования уровней защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже автору). Однако это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудовых затрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т. д.). На основе анализа можно сделать однозначный вывод: надежная защита информации не может быть обеспечена только разовыми мероприятиями, а должна быть использована совокупность различных мероприятий, осуществляемых во время разработки и эксплуатации вычислительной системы. Приведенные факты показывают, что опасность насанкционированных злоумышленных действий в вычислительных средствах и системах является весьма реальной и с дальнейшим развитием вычислительной техники угроза повреждения информации, несмотря на все усилия по ее защите, неизменно растет. Все это обуславливает необходимость углубленного анализа опыта защиты информации и комплексной организации методов и механизмов защиты.

Список литературы

1.Галатенко В.А. Основы информационной безопасности., М.: ИНТУИТ, 2004. – 250 с.

2.Герасименко В.А., Малюк А.А. Основы защиты информации М., 1994 г. – 540 с.

3.Соколов А.В., В.Ф. Шальгин. Защита информации в распределённых корпоративных сетях и системах. – М.:ДМК Пресс, 2002. – 187 с.

4.Спесивцев А.В. Защита информации в персональных ЭВМ. М. – Радио и связь, ВЕСТА, 1992 г. – 230 с.