творчество. И определяется как набор знаний и навыков, необходимых работнику для выполнения возложенных на него функций и задач.

Пути повышения уровня знаний включают в себя: курсы и семинары; тренинги в Компании и вне нее; стажировки; руководство и консультации на рабочем месте; самообучение; дистанционное образование, позволяющие развить способности персонала в той или иной области.

Компания для выполнения обязательств по поставке продукции/услуг определенного качества в быстро меняющихся рыночных условиях, когда потребности и ожидания потребителей постоянно увеличиваются, проводит обучение персонала на всех уровнях в соответствии с требованиями МС ИСО 9001: 2000 (п. 6.2.)

Перед разработкой и планированием обучения определяются вопросы, ограничивающие процесс обучения. Они могут включать в себя: регулятивные законодательные требования; требование политики, наложенные Компанией, включая те, которые связаны с человеческими ресурсами; финансовые вопросы; требования, связанные со временем и расписанием; возможности, мотивация и способности сотрудников, подлежащих обучению; факторы, такие как доступность собственных ресурсов для выполнения обучения; ограничения на любые другие доступные ресурсы.

Ведь современный бизнес, с его жесткой конкуренцией и периодическими потрясениями, требует такой стратегии, которая бы гарантировала наиболее эффективное использование ресурсов и максимальную устойчивость от внутренних и внешних кризисов при вступлении в ВТО. И один из механизмов устойчивости и развития бизнеса является обучение персонала на всех уровнях в соответствии с требованиями МС ИСО 9001.

СПОСОБЫ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ И ЦЕЛОСТНОСТИ ДАННЫХ В УЧЕБНО-МЕТОДИЧЕСКОМ КОМПЛЕКСЕ

Богачев А.В.
Московский государственный институт электронной техники, Москва

В современных условиях глобальной информатизации общества, проникновения информационных технологий в различные сферы деятельности, все заметнее становится тенденция к информатизации различных аспектов деятельности учебных заведений. Применение учебно-методических комплексов (УМК) позволяет успешно решать задачи по созданию информационного образовательного пространства.

Под учебно-методическим комплексом можно понимать комплексную систему учебных и методических материалов, основанную на использовании современной компьютерной техники, и организованную в виде программно-телекоммуникационной среды, объединяющей учащихся, педагогов, научных работников, администрацию учебных заведений. Подобная коммуникационная среда создается для УМК кафедры информатики и программного обеспечения вычислительных систем (ИПОВС) Московского института электронной техники.

Вследствие организации информационного обмена через локальную сеть, необходимо отслеживать все обращения пользователей к информационным ресурсам, разграничивать уровни доступа к данным, обеспечить блокировку несанкционированных подключений и борьбу с утечками информации. Фактически, в связи с необходимостью применения новых технологий обработки и хранения информации и передачи ее по открытым каналам связи, ростом числа потенциальных источников угрозы, некомпетентностью пользователей системы, а также усложнением прикладного и системного программного обеспечения, задачи по обеспечению информационной безопасности становятся наиболее актуальными.

В настоящее время структура УМК ИПОВС обеспечивает целостность и конфиденциальность данных при информационном обмене при помощи криптографических методов защиты, а также протоколирования и аудита.

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационной системе. У каждого сервиса свой набор возможных событий, которые можно разделить на внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов).

Аудит – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически с целью выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нее. Реализация протоколирования и аудита решает следующие задачи:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

В основе применяемой методики обмена зашифрованными данными между пользователями лежит алгоритм является RSA, основанный на операциях с большими простыми числами и их произведениями. Алгоритм основан на использовании того факта, что задача факторизации является трудной, т.е. легко перемножить два числа, в то время как не существует полиномиального алгоритма нахождения простых сомножителей большого числа.

На практике данный алгоритм в работе УМК реализуется следующим образом. Обозначим как А и Б двух пользователей, действующих в системе, осуществляющих обмен зашифрованными сообщениями.

Шифрование с открытым ключом состоит из следующих шагов:

1. Пользователь Б создает пару ключей $Ks_Б$ и $Kp_Б$, используемых для используемых для шифрования и дешифрования передаваемых сообщений.

2. Пользователь Б делает доступным некоторым надежным способом свой ключ шифрования, т.е. открытый ключ $Kp_Б$. Составляющий пару закрытый ключ $Ks_Б$ держится в секрете.

3. Если Б хочет послать подписанное сообщение А, он шифрует сообщение, используя открытый ключ пользователя А ($Kp_А$).

4. Когда А получает зашифрованное сообщение, он проверяет и дешифрует его, используя свой закрытый ключ $Ks_А$. Никто другой не сможет дешифровать сообщение, так как этот закрытый ключ знает только А.

Характерной чертой используемого метода информационного обмена является то, что нет необходимости создавать абсолютно надежный канал для рассылки секретных ключей. Вместе с тем необходимо отметить, что сложность вычисления значений «односторонней функции» и ее обратной, т.е. сложность зашифрования и расшифрования, обычно значительно выше, чем сложность этих процедур при, например, симметрических методах шифрования, что существенно увеличивает время, необходимое для выполнения данных операций. Кроме того, в настоящее время неизвестны практически реализуемые односторонние функции, для которых абсолютно убедительно доказана невозможность их обращения квалифицированным злоумышленником.

Таким образом, использование алгоритма асимметричного шифрования в «чистом виде» не позволяет эффективно решить проблему безопасной передачи информации. Одним из возможных способов решения задачи эффективного шифрования с передачей секретного ключа, использованного отправителем, может использоваться следующая последовательность действий:

1. Пользователь А посылает зашифрованное сообщение пользователю Б. Перед передачей сообщения А генерирует случайный ключ Ksimm.

2. А зашифровывает асимметричным алгоритмом Ksimm на открытом ключе пользователя Б ($Kp_Б$) и отправляет зашифрованный ключ Ksimm пользователю Б.

3. А зашифровывает симметричным алгоритмом сообщение на ключе Ksimm и отправляет его Б.

Таким образом, сообщение сначала симметрично зашифровывают случайным ключом, затем этот ключ зашифровывают открытым асимметричным ключом получателя, после чего сообщение и ключ отправляются по сети.

Описанные недостатки применяемой методики шифрования данных компенсируются следующим образом:

- проблема распространения ключей симметричного шифрования устраняется из-за того, что Ksimm, на котором шифруется сообщение, передается по открытым каналам связи в зашифрованном виде. Для зашифрования Ksimm используется асимметричный алгоритм;

- проблема медленного выполнения шифрования при использовании асимметричных алгоритмов не возникает, так как асимметричным алгоритмом шифруется только Ksimm, а все данные зашифровываются быстрым симметричным алгоритмом.

Материалы общероссийской научной конференции с международным участием

Физико-математические науки

ОСНОВНЫЕ ФИЗИЧЕСКИЕ ИДЕИ О ПРИРОДЕ ВАКУУМА

Рабжабов О.Р.
Дагестанская государственная сельскохозяйственная академия, Махачкала

По представлениям современной науки, реальный (физический) вакуум – это не пустота или «отсутствие всякого присутствия». Отказ от представлений о вакууме, как о пустоте является концептуальным положением современной физики. В настоящее время экспериментальным фактом можно считать утверждение о том, что вакуум – среда с очень сложной структурой, которая изменялась в ходе эволюции Вселенной и которую можно перестраивать путем изменения состояний материи, взаимодействующей с вакуумом, конкретно – путем концентрации энергии в малых областях пространства. Такая концентрация энергии изменяет не только ситуацию в системе частиц, но и саму структуру пространства. Это утверждение отражает тот факт, что вакуум является характеристикой самого пространства – времени.

Вакуум представляет собой сложный физический объект, в котором непрерывно происходит рождение и уничтожение виртуальных частиц (материализованных порций энергии). Вакуум является динамической системой, обладающей некоторой энергией, которая все время перераспределяется между виртуальными (воображаемыми) частицами.

Представление о вакууме как непрерывной активности содержащихся в нем виртуальных частиц вытекает из принципа неопределенности Гейзенберга. Принцип неопределенности Гейзенберга имеет такое выражение: $\Delta E \cdot \Delta t \geq h$. Согласно этому, квантовые эффекты могут на время нарушать закон сохранения энергии. В течение короткого времени t энергия, взятая как бы «взаймы», может расходоваться на рождение короткоживущих частиц, исчезающих при возвращении «займа» энергии. Это и есть виртуальные частицы. Возникая из «ничего», они снова возвращаются в «ничто». Так, что вакуум в физике оказывается не пустым, а представляет собой море рождающихся и тут же гасящихся всплесков, - виртуальных частиц.

Однако воспользоваться энергией вакуума мы не можем, так как это есть наинизшее энергетическое состояние полей. При наличии внешнего источника энергии можно реализовать возбужденные состояния полей – тогда будут наблюдаться обычные (не виртуальные) частицы. Вакуум поляризуется внешним полем, и поле может порождать из вакуума пары различных частиц, причем легче всего рождаются самые легкие, т.е. электронно-позитронные пары. Такие пары интенсивно порождаются в поле с напряженностью E_0, работа которого на расстоянии комптоновской длины волны $l=\hbar/mc\approx3\cdot10^{-11}$ см порядка энергии покоя пары равной $2mc^2\cong10^6$ эВ, т.е. $A=F\cdot l=eE_0\cdot\frac{\mathbf{h}}{mc}$. Отсюда для нахождения образования одной частицы можем написать $eE_0\,\hbar/mc\cong mc^2$ или $E_0\cong\frac{m^2c^2}{e\mathbf{h}}\cong3\cdot10^{16}$ В/см.

Пары достаточно быстро, хотя и не в катастрофическом темпе, могут рождаться и в более слабых полях. Поэтому достижение полей, например с $E_0 \cong10^{14}$ В/см уже позволило бы, вероятно, наблюдать рождение пар в вакууме.

Вакуум поляризуется не только сильным электрическим полем, но и магнитным полем, причем характерное значение напряженности магнитного поля H_0 такое же, как и для электрического поля E_0. В магнитном поле с напряженностью более H_0 вакуум ведет себя подобно нелинейной анизотропной среде и сильно влияет на распространение электромагнитных волн.

Уравнения, которые открыл Дирак, показывают, что в природе существуют частицы с положительной энергией – электроны и античастицы – позитроны, энергия которых отрицательна. Они рождаются парами электрон-позитрон из физического вакуума. Сам же вакуум представляет собой некоторое латентное (скрытое) состояние электронов и позитронов. В среднем физический вакуум не имеет ни массы, ни заряда, ни каких-либо других физических характеристик. Однако в малых пространственных областях (порядка 10^{-33} см) вакуума значения физических характеристик могут стать отличными от нуля – на малых расстояниях вакуум спонтанно флуктуирует. В вакууме постоянно происходят процессы рождения и уничтожения частиц и античастиц разного сорта. Образно говоря, в малых пространственно-временных областях вакуум похож на «кипящий бульон», состоящий из элементарных частиц. Поэтому в квантовой теории возникло представление о физическом вакууме как о «квантовой жидкости», находящейся в вечном движении. Такая жидкость описывается уравнениями квантовой гидродинамики и, естественно, обладает упругими свойствами.

Рассмотрим энергетические свойства квантового вакуума. Из соотношения неопределенности и закон сохранения массы-энергии можно рассчитать промежуток времени, соответствующий массе электрона: $\Delta t=10^{-21}$ с. Смысл этих расчетов с точки зрения классической механики кажется безумным: в течение столь малых промежутков времени энергия вакуума испытывает достаточно большие колебания, чтобы за это время из него рождались электроны – и все прочие элементарные частицы.

Такие частицы назвали виртуальными. Индивидуально они никак не проявляют себя, но как системный ансамбль вполне заметно влияют на различие свойства материи (магнитный момент электрона, спектральные характеристики атомов и др.) Таким образом, этот вакуумный виртуальный «туман» - совершенно реальный феномен.

В 1980 г. А.Е. Акимов предложил новую теоретическую модель квантового вакуума. В основу этой