Создание педагогической системы обучения с применением информационно-коммуникационных технологий, максимально учитывающей психолого-педагогические и организационно-методические особенности информатизации и компьютеризации учебного процесса, поможет избежать подобных проблем.

Литература:

1. Гохлернер М.М., Ейгер Г.В. ЭВМ в преподавании гуманитарных дисциплин / Компьютер в обучении: психолого-педагогические проблемы (круглый стол) // Вопросы психологии. – 1987. № 1. – С. 60-84.

2. Карамышева Т.В. Изучение иностранных языков с помощью компьютера. В вопросах и ответах. – Изд-во «Союз». – СПб., 2001. – 192 с.

3. Курова Н.Н. Проектная деятельность в развитой информационной среде образовательного учреждения: Учеб. пособие для системы доп. проф. образования. – М.: Федерация Интернет Образования, 2002. – 64 с.

С. В. Жарый, гр. КТ-512

КОНЦЕПТУАЛЬНЫЕ ВОПРОСЫ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Одной из наиболее серьезных проблем, затрудняющих применение современных информационных технологий (ИТ), является обеспечение их информационной безопасности. Особенно важна безопасность так называемых критических приложений, к числу которых относятся системы государственного и военного управления, объекты атомной энергетики, ракетно-космическая техника, а также финансовая сфера, нарушение нормального функционирования которых может привести к тяжелым последствиям для окружающей среды, экономики и безопасности государства.

Обеспечение безопасности информационных технологий представляет собой комплексную проблему, которая включает правовое регулирование применения ИТ, совершенствование технологий их разработки, развитие системы сертификации, обеспечение соответствующих организационно-технических условий эксплуатации. Основополагающим аспектом решения проблемы безо-

пасности ИТ является выработка системы требований, критериев и показателей оценки уровня безопасности ИТ.

Состояние дел в области нормативного регулирования, методического и инструментального обеспечения оценки и сертификации безопасности ИТ в России, по общему признанию, не соответствует современному уровню развития ИТ, масштабам и разнообразию информационных угроз, требованиям законодательных и нормативных актов. Нормативные документы, применяемые различными ведомствами в рамках их полномочий, касаются отдельных аспектов обеспечения информационной безопасности. При этом отсутствует комплексность решения проблемы при разработке, внедрении и эксплуатации информационных систем (ИС).

В настоящее время сложилась насущная необходимость выработки общей политики в области оценки и сертификации безопасности информационных технологий и построения на ее основе системы нормативных документов в ранге государственных стандартов. Госстандарты позволят создать нормативную основу деятельности органов сертификации независимо от их ведомственной принадлежности.

В настоящей статье рассматриваются основы подхода к формированию нормативно-методической базы оценки и сертификации ИТ. Уточняются основные понятия, предлагаются направления совершенствования нормативной базы, методического обеспечения и инструментальных средств проведения сертификационных испытаний.

Отправной точкой при разработке нормативно-методического обеспечения оценки и сертификации безопасности ИТ должно являться однозначное установление терминологии в этой предметной области.

В существующих нормативных документах и у различных специалистов, в том числе за рубежом, существует различное понимание того, что включать в основополагающее понятие "безопасность ИТ". Наиболее часто, как, например, в Европейских критериях, безопасность ИТ определяется как комбинация конфиденциальности, целостности и доступности, где под ними понимается соответственно:

- предотвращение несанкционированного раскрытия информации;
- предотвращение несанкционированной модификации информации;
- предотвращение несанкционированного отказа в получении информации.

Данные аспекты достаточно полно характеризуют безопасность ИТ, только если считать это понятие тождественным понятию "защита информации".

Более современная точка зрения отражена в проекте международного стандарта "Общие критерии оценки безопасности информационных технологий", где определяется, что "нарушение безопасности обычно включает, но не ограничено, раскрытием ресурса неразрешенным получателям (потеря конфиденциальности), повреждением ресурса через неразрешенную модификацию (потеря целостности) или неразрешенным лишением доступа к ресурсу (потеря доступности)". При этом процессы распространения и модификации информационных ресурсов должны строго управляться.

На мой взгляд, безопасность ИТ — это гораздо более широкое и глубокое понятие, чем защита информации. Угрозу представляет не только возможность несанкционированного доступа к ресурсам информационных систем, но и возможность через информационные технологии нанесения неприемлемого ущерба тем, в интересах кого они применяются. Эти две грани можно определить, соответственно, как внутреннюю и внешнюю безопасность ИТ.

С учетом изложенного, под безопасностью ИТ предлагается понимать их способность обеспечивать защиту информационных ресурсов от действия внешних и внутренних, случайных и преднамеренных угроз, а также выполнять предписанные им функции без нанесения неприемлемого ущерба потребителям информации.

Следует обратить внимание на используемый здесь термин "неприемлемый ущерб". Он является принципиальным, разделяя угрозы, связанные с ухудшением качества функционирования ИТ и нарушением их безопасности.

Следующей исходной позицией является определение того, что же понимать под оценкой безопасности ИТ. Оценка безопасности ИТ производится с

целью проверки соответствия достигнутого уровня безопасности заданному в ТЗ на разработку ИТ, а также соответствия требованиям стандартов и нормативных документов в отношении ИТ данного класса.

Специфика информационных технологий как объекта оценки определяется присутствием в них в качестве определяющей компоненты программного обеспечения. Ввиду большой функциональной, структурной и логической сложности программного обеспечения на практике невозможно в полном объеме оценить его поведение во всем возможном диапазоне его применения.

Предметная область безопасности обладает той особенностью, что при ее оценке приходится применять как объективные, так и субъективные критерии. Оцениваемые характеристики безопасности ИТ могут иметь как детерминированную, так и случайную природу. Некоторые исследуемые элементы ИТ, как, например, преднамеренные закладки, имеют уникальное представление и скрытый характер, что также затрудняет проведение оценок безопасности ИТ.

В силу указанных обстоятельств получение интегральных количественных оценок безопасности ИТ является проблематичным. В упоминавшихся уже "Общих критериях" говорится, что "точные и универсальные оценки безопасности ИТ невозможны". Это, однако, не исключает использования отдельных частных количественных показателей там, где это целесообразно. В частности, эти показатели могут использоваться для оценки уровня механизмов криптографической и парольной защиты, контрольного суммирования и др.

В качестве общих требований к нормативно-методической базе оценки безопасности ИТ можно выделить следующие:

- универсальность, способность обеспечивать оценку безопасности любых видов ИТ и отдельных их компонентов;
- гибкость, способность формирования требований и получения оценок безопасности ИТ, максимально учитывающих особенности их применения;
- конструктивность, способность объективным образом оценивать уровень безопасности ИТ и влиять на процесс ее обеспечения;

- преемственность, способность интерпретировать результаты оценок, полученных в других системах оценки безопасности ИТ;
- расширяемость, способность наращивания системы критериев и показателей без нарушения их общего построения.

Рассмотрение существующих систем нормативных документов в области сертификации ИТ показывает, что в своей основе они в значительной мере этим требованиям не удовлетворяют. Необходимо их совершенствование.

Основными направлениями развития нормативно-методического обеспечения оценки и сертификации безопасности ИТ являются:

- нормативная база;
- методическое обеспечение;
- инструментальные средства.

В настоящее время в России действует ряд систем сертификации безопасности ИТ: Гостехкомиссии России, ФАПСИ, Минобороны, ФСБ. Нормативная база оценки безопасности ИТ в этих системах сертификации формально является различной, хотя на практике наблюдается взаимное использование отдельных нормативных документов.

Наличие нескольких систем сертификации обусловлено рядом объективных обстоятельств: особенностями предметной области, режимными соображениями и др. В целом оно не препятствует развитию в области сертификации ИТ, чего нельзя сказать о различии их нормативных баз, поскольку:

- различие требований к механизмам обеспечения безопасности ИТ затрудняет разработку унифицированных проектных решений и приводит к созданию специализированных средств для различных областей применения, что сопровождается их удорожанием;
- возникает необходимость в разработке различного методического и инструментального обеспечения оценки безопасности ИТ, что также сопровождается значительными дополнительными затратами;
- значительно усложняется и удорожается подготовка специалистов в области безопасности ИТ;

- осложняется процесс взаимного признания сертификатов, полученных в разных системах;
- качество нормативных документов является недостаточным в силу невозможности в каждой системе сертификации выделить необходимые ресурсы на их разработку.

Указанные проблемы могут быть преодолены путем создания единой для всех систем сертификации нормативной базы оценки безопасности ИТ в ранге государственных стандартов.

Совершенствование нормативной базы оценки безопасности ИТ может идти по трем направлениям:

- принять в качестве базовой одну из существующих в России систем и дополнить ее необходимыми документами;
- принять в качестве базовой наиболее прогрессивную международную систему оценки безопасности и осуществить ее адаптацию с учетом особенностей российских условий;
- разработать принципиально новую систему оценки безопасности ИТ.

Существует, конечно, и четвертый путь — продолжение самостоятельного развития нормативной базы в каждой системе сертификации, но движение по этому пути, по меньшей мере, неразумно.

Первый путь является наиболее дешевым и быстро реализуемым, однако действующие нормативные документы систем сертификации уже не отвечают требованиям сегодняшнего дня. Дальнейшее совершенствование нормативной базы сертификации путем разработки новых документов по отдельным областям приложения ИТ без коренной переделки основы ее построения в конечном итоге приведет в тупик.

Третий путь представляется самым бесперспективным. Прежде всего потому, что пока еще никем в России не предложено достаточно ясной, полной и детально проработанной концепции построения перспективной системы оценки безопасности ИТ. Отдельные проработки в этом направлении показывают, что недостатков в них пока больше, чем достоинств, в своей основе они

не удовлетворяют указанным выше требованиям и даже концептуальная их доработка может потребовать очень много времени.

Безопасность должна обеспечиваться на всех уровнях представления ИТ, от наиболее абстрактного на этапе формирования замысла создания информационной системы до ее применения в конкретных условиях. Предусмотрены следующие уровни рассмотрения безопасности ИТ:

- безопасность окружающей среды — законы, нормативные документы, организационные меры, физическое окружение, определяющие условия применения ИТ, а также существующие и возможные угрозы безопасности ИТ;
- цели безопасности — намерения, определяющие направленность мер по противодействию выявленным угрозам и обеспечению безопасности ИТ;
- требования безопасности — полученный в результате анализа целей безопасности набор технических требований для механизмов безопасности и гарантированности их реализации, обеспечивающий достижение сформулированных целей;
- спецификации безопасности — проектное представление механизмов безопасности, реализация которых гарантирует выполнение требований безопасности;
- разработка — реализация механизмов безопасности в соответствии со спецификациями.

Оценка безопасности должна проводиться в процессе разработки ИТ на наиболее важных этапах. Предусмотрены следующие стадии оценки:

- оценка профиля защиты;
- оценка задания по безопасности;
- оценка реализованных механизмов безопасности.

Оценка задания по безопасности проводится с целью установления того, что задание соответствует требованиям профиля защиты и содержит полный, последовательный и технически правильный набор требований, необходимых для обеспечения безопасности конкретного объекта. Задание по безопасности

подлежит согласованию между заказчиками, разработчиками и оценщиками и является в дальнейшем основным документом, в соответствии с которым оценивается безопасность разрабатываемой ИС.

Цель оценки реализованных механизмов обеспечения безопасности ИТ заключается в установлении того, что механизмы безопасности обеспечивают выполнение всех требований, содержащихся в задании по безопасности.

"Общие критерии" представляют собой наиболее полный на настоящее время набор критериев в области безопасности ИТ, который удовлетворяет потребностям основных категорий и групп пользователей ИТ. Это является основанием для принятия ОК в качестве международного стандарта.

Требования ОК являются базовыми для формирования стандартизованных профилей защиты. При необходимости на этапе составления задания по безопасности они могут быть дополнены не входящими в ОК специфическими требованиями. Однако при этом заключение о безопасности ИТ не будет обладать той степенью универсальности и сопоставимости оценок, как полученное только на основании требований из ОК.

Методическое обеспечение должно охватывать все аспекты проверки выполнения требований, предъявляемых к безопасности ИТ.

Важнейшим и наиболее объемным видом испытаний при оценке безопасности ИТ является функциональное тестирование, предназначенное для проверки работоспособности механизмов безопасности и их соответствия предъявленным к ИТ функциональным требованиям. Для проведения тестирования должна быть подготовлена необходимая программно-методическая документация. В ее состав входят: программа тестирования, методика тестирования и контрольные результаты.

В программе тестирования для каждой функции безопасности, определенной в функциональных требованиях, должны быть заданы цель тестирования, объем и порядок его проведения. Методика проведения тестирования должна содержать описание условий и процедур проведения испытаний, состав тестов и порядок обработки результатов тестирования.

Выделяются два аспекта, которые определяют качество и гарантированность проведения тестирования: достаточность и глубина.

Достаточность характеризует полноту охвата тестированием функций безопасности и объем проводимого тестирования. При анализе достаточности должно быть продемонстрировано соответствие между параметрами функций безопасности и результатами тестирования, подтверждающее проверку выполнения заданных требований.

Глубина характеризует уровень детальности проводимого тестирования. Она определяет вероятность выявления ошибок в реализованных механизмах обеспечения безопасности ИТ. Кроме того, от глубины тестирования зависит возможность обнаружения в ИТ закладных элементов.

Важным аспектом испытаний средств безопасности ИТ, на который не всегда в должной мере обращается внимание, является оценка уязвимости средств безопасности (СБ).

Оценка уязвимости СБ ИТ производится с целью проверки способности реализованных механизмов безопасности противостоять информационным воздействиям, являющимся результатом неправильной конфигурации, неправильной эксплуатации, либо попыткам взлома.

Задачами, решаемыми при оценке уязвимости СБ ИТ, являются:

- анализ уязвимостей СБ ИТ;
- оценка мощности функций безопасности;
- оценка возможностей неправильного применения;
- анализ тайных каналов.

Анализ уязвимостей СБ ИТ предназначен для выявления возможных недостатков, которые могли бы быть использованы злоумышленниками для проникновения в среду ИТ, доступа к защищаемым ресурсам, а также для нарушения нормального режима функционирования ИТ. Анализ уязвимостей должен проводиться как путем аналитического исследования проектных материалов, так и путем натурного моделирования с использования имитаторов угроз безопасности. В зависимости от заданного уровня гарантированности предполага-

ется различная степень знакомства злоумышленника с проектными материалами, а также различный уровень его подготовленности и оснащенности.

Анализ тайных каналов направлен на выявление существования и оценку потенциальной возможности использования непредусмотренных каналов проникновения в среду ИТ и передачи информации. Задача выявления тайных каналов в методическом плане является весьма сложной и трудно поддается формализации.

Качество и сроки выполнения работ по сертификации в значительной мере зависят от используемых инструментальных средств. Наибольшее применение инструментальные средства находят в следующих направлениях:

- генерация тестов;
- имитация угроз;
- анализ текстов программ.

Генераторы тестов можно разделить на две большие группы:

- генераторы стохастических тестов;
- генераторы целенаправленных тестов.

В приложении к анализу безопасности ИТ более предпочтительными являются генераторы целенаправленных тестов. Помимо испытаний функциональных механизмов безопасности, областью применения генераторов тестов является также анализ текстов программ для выявления недекларированных возможностей и закладных элементов.

Генераторы тестов, предназначенные для испытаний безопасности ИТ, должны обладать следующими функциональными возможностями:

- формирование заданных структур и последовательностей входных данных, определяемых особенностями реализации механизмов безопасности;
- обеспечение заданной степени покрытия области входных данных и элементов структуры исследуемых программ;
- выявление критичных условий функционирования механизмов безопасности и маршрутов реализации программного кода;

- формирование тестов по условиям реализации предыдущих этапов тестирования.

Имитаторы угроз предназначены для натурного моделирования воздействия на ИТ типовых угроз. Посредством имитаторов угроз проверяются механизмы защиты от программных вирусов, средства экранирования от проникновения из внешних вычислительных сетей и т.д.

Для автоматизации исследования исходных текстов программ применяются статические и динамические анализаторы. Статические анализаторы предназначены для оценки корректности структуры построения программ, выявления участков программного кода, к которым отсутствует обращение, установления точек входа и выхода из программ, не предусмотренных спецификациями, проверки полноты описания и использования программных переменных, поиска специальных программных конструкций, которые могут быть идентифицированы как программные закладки.

Динамические анализаторы используются для трассировки выполнения программ, выявления критических путей, оценки полноты покрытия возможных ветвей программ при функциональном тестировании.

В настоящее время развивается еще одна область применения инструментальных средств — использование информационных и экспертных систем для формирования требований к безопасности ИТ и оценки уровня их выполнения. Применение таких средств позволит значительно повысить степень обоснованности задания требований, их адекватность реальным условиям применения ИТ, даст возможность осуществлять выбор механизмов безопасности, наиболее полно удовлетворяющих заданным требованиям.

Анализ состояния дел в области сертификации безопасности информационных технологий показывает, что имеется существенное отставание в уровне развития нормативного, методического и инструментального обеспечения оценки безопасности от тех потребностей, которые продиктованы масштабами развития и внедрения ИТ в системы критических приложений. Требуется выработка общей политики по оценке и сертификации безопасности ИТ и формиро-

вание на ее основе комплекса нормативных документов в ранге государственных стандартов.

Систему российских государственных стандартов представляется рациональным разрабатывать на основе наиболее совершенного на настоящий момент документа в этой области — "Общих критериев оценки безопасности информационных технологий", который планируется к принятию в качестве международного стандарта. "Общие критерии" в полной мере удовлетворяют всем современным требованиям и обладают огромным потенциалом развития и адаптации к различным условиям применения. Они позволяют сформировать совокупности критериев оценки, аналогичные принятым в настоящее время в действующих системах сертификации средств защиты информации в России, и тем самым обеспечить безболезненный переход на новую нормативную базу.

Качество проведения сертификации ИТ может быть повышено путем внедрения типовых методик испытаний по базовым механизмам обеспечения безопасности, мерам гарантированности и однородным группам изделий ИТ, а также применения соответствующего инструментария.

Выработка общей концепции совершенствования сертификации информационных технологий и разработка на ее основе комплекса нормативных документов, методического и инструментального обеспечения потребует скоординированных усилий действующих в России систем сертификации средств зашиты информации. Это может быть сделано в рамках государственной программы по созданию безопасных информационных технологий.

А. З. Кабиров, гр. КТ-512

ИНТЕРНЕТ – КОММЕРЦИЯ

Одна из наиболее актуальных на сегодняшний день тем – развитие интернет-коммерции в России. Эта сфера деятельности начинает приобретать все большее значение в современном мире, и в нашей стране соответственно, в связи с тенденцией к всеобщей глобализации экономики. Интернет и электронная торговля играют в этом процессе одну из важнейших ролей.