k2[vk_]:=Last[Solve[$k2^2$ – 2HS[vk]k2+KP[vk]==0, k2]] Необходимо нажать Shift+Enter.
Расшифровка использованных встроенных и внешних функций:
First – первый элемент списка vk;
Part[vk,i] – i-й элемент списка vk;
ru, rv, ruu, ruv, rvv – частные производные $\vec{r}(u,v) = (x(u,v), y(u,v), z(u,v))$;
EP, FP, GP – элементы первой квадратичной формы поверхности;
LV, MV, NV – элементы второй квадратичной формы поверхности;
HS – средняя кривизна поверхности;
KP – главная кривизна поверхности;
k1 и k2 – главные кривизны поверхности.
**vk1:={u, v, $uv^2$}**
**ru[vk1]** Необходимо нажать Shift+Enter.
{1,0,$v^2$}
**rv[vk1]** Shift+Enter
{0, 1, 2uv}
**ruu[vk1]**
{0, 0, 0}
**ruv[vk1]**
{0, 0, 2v}
**rvv[vk1]**
{0, 0, 2u}
**EP[vk1]**
$1+v^4$
**FP[vk1]**
$2uv^3$
**GP[vk1]**
$1+4u^2v^2$
**LV[vk1]**
0
**MV[vk1]**

$$\frac{2v}{\sqrt{1+4u^2v^2+v^4}}$$

**NV[vk1]**

$$\frac{2u}{\sqrt{1+4u^2v^2+v^4}}$$

**Жарый С.В.**

## КОНЦЕПТУАЛЬНЫЕ ВОПРОСЫ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.

*s.zhariy@auchan.ru*
*Филиал РГППУ в г. Берёзовский. Кафедра ВТ и программирования*
*г. Березовский*

**Введение**

Одной из наиболее серьезных проблем, затрудняющих применение современных информационных технологий (ИТ), является обеспечение их информационной безопасности

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.

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 настоящей докладе 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.

**Понятийные основы**

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.

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

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.

**Направления совершенствования нормативно-методического обеспечения**

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

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

**Нормативная база**

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

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. Следует также отметить, что в этом случае мы изолируем себя от наиболее развитых стран, идущих по пути применения "Общих критериев оценки безопасности ИТ", лишимся возможности использовать их методический и инструментальный аппарат, а также использовать их сертифицированные продукты и продвигать свои на их рынок.

На мой взгляд, наиболее приемлемым является построение системы российских государственных стандартов по оценке безопасности ИТ на основе самого совершенного на настоящий момент документа в этой области — "Общих критериев" (ОК).

Анализ ОК свидетельствует, что этот документ в полной мере удовлетворяет всем указанным выше требованиям.

Рассмотрим наиболее важные положительные качества ОК.

*Охват всего спектра информационных технологий и возможность учета особенностей каждой конкретной системы при задании требований по безопасности.*

ОК предназначены для оценки безопасности как систем информационных технологий, разрабатываемых для автоматизации в конкретной области применения, так и отдельных продуктов ИТ, которые имеют универсальное предназначение. ОК применимы к оценке безопасности как аппаратных средств, так и программного обеспечения ИТ.

С целью оптимального сочетания как предопределенного набора требований, так и требований, учитывающих особенности конкретной области применения ИТ, в ОК используются два ключевых понятия: **профиль защиты** и **задание по безопасности**.

**Профиль защиты** представляет собой функционально полный, прошедший апробацию, стандартизованный набор требований, предназначенный для многократного использования.

**Задание по безопасности** — это полная комбинация требований, являющихся необходимыми для создания и оценки информационной безопасности конкретной системы или продукта ИТ.

*Широкий спектр, детальность и структурированность требований к механизмам безопасности, мерам и средствам обеспечения их реализации.*

ОК содержат две категории требований: **функциональные требования** и **требования гарантированности**.

**Функциональные требования** описывают те функции, которые должны быть реализованы в ИТ для обеспечения их безопасности.

**Требования гарантированности** определяют меры и средства, которые должны быть использованы в процессе создания ИТ для получения необходимой уверенности в правильности реализации механизмов безопасности и в их эффективности.

*Охват всего процесса создания ИТ, начиная от формирования целей и требований обеспечения безопасности и кончая поставкой и наладкой ИТ на конкретном объекте.*

Важной отличительной чертой ОК является полнота охвата требованиями всего жизненного цикла ИТ. В соответствии с ОК, на начальном этапе разработки ИТ должна быть определена модель жизненного цикла ИТ, в которой необходимо представить все меры и средства, применяемые разработчиком для достижения требуемого уровня безопасности ИТ. Меры и средства обеспечения гарантированности безопасности охватывают следующие аспекты:

- среда и средства разработки;
- состав, полнота и адекватность проектных материалов;
- конфигурационное управление;
- документация;
- тестирование;
- оценка уязвимости;
- поставка и наладка.

*Возможность формирования наборов требований по уровням безопасности ИТ, сопоставимых с другими системами оценки.*

В ОК указывается, что они разработаны с учетом совместимости с существующими критериями, чтобы сохранить преемственность оценок безопасности.

*Комплексность подхода к обеспечению безопасности ИТ.*

В соответствии с ОК, 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.

*Расширяемость требований к безопасности ИТ.*

"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.

**Методическое обеспечение**

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.

Необходимость наличия типовых методик испытаний будет возрастать по мере увеличения числа однородных продуктов для типовых механизмов безопасности.

**Инструментальные средства**

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.

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.

**Заключение**

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 формирование 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.

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.

*Литература*


1. *Information Technology Security Evaluation Criteria(ITSEC). Harmonised Criteria of France — Germany — the Netherlands — the United Kingdom* -- Department of Trade and Industry, London, 1991
2. *Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения* -- Гостехкомиссия России.Москва, 1992
3. *Common Criteria for Information Technology Security Evaluation. Version 1.0* , 96.01.31
4. В.В Липаев -- *Программно-технологическая безопасность информационных систем* -- Jet Info, 6-7, 1997
5. В. Бетелин , В Галатенко -- *Информационная безопасность в России: опыт составления карты* -- Jet Info, 1998, #1
6. М. Кобзарь , И. Калайда -- *Общие критерии оценки безопасности информационных технологий и перспективы их использования* -- Jet Info, 1998, #1
7. В.В Липаев -- *Отладка сложных программ* -- М.: Энергоатомиздат, 1993
8. W.E Howden -- *Functional program testing and analysis* -- N.Y.: McGraw Hill, 1987