Функциональная безопасность информационных технологий в критически важных системах

Тарасов А.А.,

Шубинский И.Б.

Россия, Москва, ВНИИАС ОАО «РЖД»

Информационная система представляет совокупность информационных и телекоммуникационных средств, с помощью которых формируются механизмы обработки, передачи, хранения и использования информации. Процессы, реализующие указанные механизмы в соответствии с предусмотренными оригинальными методами и способами, являются информационными технологиями. В настоящее время происходит формирование качественно новых информационных технологий, связанных с возникновением таких систем, как интеллектуальные средства управления и проектирования, интегрированные и гибридные экспертные системы, информационная поддержка CALS-технологий по всему жизненному циклу продукции и другие.

Успешное становление новых технологий невозможно без параллельного развития методов и средств обеспечения их безопасности. Безопасность в широком смысле представляет собой совокупность безопасных условий деятельности, а применительно к критически важным системам информационной инфраструктуры - совокупность безопасных условий их функционирования. Нарушение процессов нормального функционирования критически важных систем (КВС) может привести к срыву выполнения жизненно важных функций государственного управления, управления войсками, оружием, экологически опасными и экономически важными производствами и т.д. и, как следствие, недопустимому ущербу национальным интересам.

Безопасность информационных технологий в КВС регулируется техническими регламентами. Цели создания этих регламентов едины как для промышленной продукции и процессов производств, так и для информационной продукции и информационных процессов. Они заключаются в «защите жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества; охраны окружающей среды, жизни или здоровья животных и растений; предупреждения действий, вводящих в заблуждение потребителей» (закон Российской Федерации «О техническом регулировании»). Отсюда следует разное смысловое содержание понятий «защищенность информационных технологий» и «безопасность информационных технологий». Первое понятие предусматривает защиту информационных технологий от несанкционированных действий нарушителей (НСД), от деструктивных воздействий, вызванных компьютерными и(или) телекоммуникационными отказами, сбоями, программными ошибками и не распространяется на задачи защиты внешней среды от негативного влияния информационных технологий.

Понятие «безопасность информационных технологий» шире и охватывает не только НСД и деструктивные воздействия аппаратных и программных средств, но и воздействия ошибок в выходных результатах информационных процессов на внешнюю среду и возможность возникновения по этой причине опасных последствий. Минимизация опасных ошибок, а, следовательно, и опасных последствий, осуществляется с помощью методологии функциональной безопасности. Защита от НСД с определенным уровнем гарантии реализуется с помощью технологии защиты

информации. Исключение или парирование деструктивных воздействий отказов, сбоев и ошибок аппаратных и программных средств, в большинстве своем, достигается с помощью технологий надежности. Таким образом, научные и практические основы обеспечения безопасности информационных технологий (ИТ) взаимоувязаны с научными дисциплинами защиты информации, надежности и функциональной безопасности технических систем .

В докладе обсуждается научное направление обеспечения функциональной безопасности ИТ, которое активно развивается в течение последнего десятилетия и направлено на гарантированное обнаружение и устранение критичных (опасных) отказов и ошибок в выходных результатах выполнения информационного процесса, вызванных ранее не устраненными входными и промежуточными деструктивными воздействиями.

Под функциональной безопасностью ИТ понимается способность выполнять все предусмотренные функции безопасности, которые при реализациях ИТ обеспечивают отсутствие недопустимого риска, связанного с причинением вреда людям, животным и растениям, имуществу и окружающей среде.

Требования к функциональной безопасности ИТ должны заключаться в следующем:

- вероятность появления потенциально опасной ситуации, а тем более аварии, по вине самой ИТ должна быть минимальной, не выше заданной;
- при возникновении потенциально опасной ситуации система должна парировать ее (переходить в защитное состояние), а при возникновении аварии – обеспечивать минимальный материальный ущерб и отсутствие человеческих жертв.

Теория безопасности должна изучать комплекс вопросов, связанных с определением возможности возникновения аварий и катастроф в результате отказов технических средств, действий персонала или недопустимых воздействий внешней среды и с разработкой методов защиты от таких событий и борьбы с их последствиями. При этом должно рассматриваться не только поведение системы в экстремальных ситуациях, но и категории угроз безопасности (в том числе военные, экологические, социальные), методы снижения негативных последствий от катастроф, правовое и экологическое регулирование безопасности и другие вопросы, так или иначе связанные с безопасностью информационного процесса. Исходя из сказанного, можно сформулировать понятие безопасности ИТ, как антропотехническое понятие, определяющее совокупность свойств технических и технологических средств, окружающей среды и целенаправленной деятельности человека, обеспечивающих исключение (предупреждение) ситуаций, опасных для движения окружающей среды и людей.

Если отказ может привести к тяжелым последствиям, и тем более стать причиной аварийной ситуации, то он является недопустимым и возникает по вине разработчика. Поэтому при разработке системы и на стадии ее проектирования необходимо провести следующие исследования.

1. Проанализировать возможность возникновения аварийной ситуации, рассмотреть и описать сценарии их развития, классифицировать возможные последствия аварий, установить вероятности получения каждой степени поражения.

2. Установить перечень выходных параметров системы, которые претерпевают существенные изменения в процессе аварии. По возможности выявить те показатели, изменение которых предшествует критическому состоянию и по изменению значения которых можно предотвратить (прогнозировать) возможность аварии.
3. Установить потенциально опасные узлы и элементы системы, нарушение работоспособности которых может иметь недопустимые последствия.
4. Установить предельно допустимые условия эксплуатации и режимы работы системы. Оценить возможную продолжительность работы системы в экстремальных условиях, в том числе при потере работоспособности ее отдельных узлов и элементов.
5. Рассмотреть возможные действия пользователей системы и обслуживающего ее персонала и проработать способы защиты от их ошибок (как умышленных, так и неумышленных), которые могли бы привести к недопустимым последствиям.

Эти исследования должны проводиться при подготовке «Доказательства безопасности», которое является основой для разработки конструкции системы, ее структуры и схем отдельных узлов, алгоритмического и программного обеспечения, т.е. разработки безопасной системы, устойчивой к возникновению «нештатных» ситуаций.

Методы обеспечения безопасности весьма разнообразны, но могут быть сведены к двум основным принципам.

Первый принцип связан с введением избыточности в создаваемые элементы, узлы, устройства и системы. Избыточность схемной (введение в состав информационной системы так называемых безопасных логических элементов, компараторов, ключей и т.д.), структурной или аппаратной (дублирование, троирование и т.д. в в системе аппаратных средств, функциональных узлов и элементов), программной (решение задачи двумя независимыми программными продуктами), функциональной (создание возможности решения одной и той же задачи путем реализации полной или упрощенной функции, но с меньшей точностью), информационной (кодирование информации внутри системы с последующим декодированием и проверкой ее безошибочности перед использованием), временной (увеличение времени восприятия или выдачи воздействия), комбинированной (при использовании нескольких из перечисленных методов). Таким образом, требования безопасности накладывают дополнительные условия на комплектующие изделия и материалы, на конструкцию, на схемные решения и структуру системы, на представление информации в ней и т.д.

В соответствии со *вторым принципом* обеспечение безопасности достигается применением средств, локализующих развитие неблагоприятных процессов, защищающих систему от выдачи неправильных воздействий, предупреждающих о возможном наступлении экстремальных ситуаций, управляющих функционированием объекта в критических случаях (парирующих развитие отказа и переводящих объекты управления в защитное состояние). Для этих целей используются контролирующие и диагностирующие устройства, которые оценивают значения выходных параметров системы и значения специальных диагностических признаков, а в необходимых случаях и окружающей среды (вибрации, температура, электромагнитная обстановка и др.). Сравнение измеренных сигналов с их заданными значениями, обработка информации и принятие решения о необходимых действиях для предотвращения аварийной ситуации должны осуществляться устройствами, которые сами обладают

высокой достоверностью, т.е., в данном случае, отвечающих требованиям безопасности.

Естественно, возможно и одновременное использование обоих методов реализации требований безопасности при построении одной системы.

Основным направлением всех работ и исследований в области безопасности является принцип исключения возможности появления потенциально опасной ситуации (или сведению вероятности появления этого события к минимально допустимой величине). Поэтому достижение безопасности функционирования ИТ должно базироваться на следующих основополагающих принципах:

- обеспечение безопасного функционирования информационной системы;
- обеспечение качественного изготовления устройств системы и ее программного обеспечения;
- принцип допущения худшего случая, при котором система даже при маловероятном сочетании поражающих факторов должна исключать появление потенциально опасной ситуации;
- организация непрерывного контроля функционирования ИТ и информационной системы в целом в процессе эксплуатации;
- осуществление непрерывного мониторинга состояния устройств системы методами диагностики.

В докладе детально обсуждаются базовые положения создания функционально безопасных ИТ:

- Подход, основанный на жизненном цикле безопасности;
- Задание на основе оценки рисков как качественных, так и количественных требований к безопасности;
- Реализация механизмов гарантированного обнаружения ошибок в выходных результатах, основанных на технологии формирования нескольких независимых по входным, промежуточным и выходным данным информационных каналов, объединенных безопасным компаратором;
- Оперативная оценка опасности последствий обнаруженных ошибок в выходных результатах, устранение их или перевод ИТ в защитные состояния;
- Выполнение Доказательства безопасности как паспорта ИТ на всех этапах жизненного цикла;
- Оценивание соответствия требованиям функциональной безопасности ИТ.