XXIX Неделя науки СПбГТУ. Материалы межвузовской научной конференции. Ч.III: С.19-20, 2001.

УДК 519.6

С.А. Кабыш (асп., каф. ИМТ), А.М. Горинштейн, к.т.н., проф.

ЛИНГВИСТИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СИСТЕМ УПРАВЛЕНИЯ ТРУБОПРОВОДАМИ ОТ ДЕФЕКТНЫХ ДАННЫХ

Эффективная защита от дефектных данных является одним из главнейших условий правильного функционирования АСУТП (автоматизированных систем управления технологическими процессами). Известно, что основной причиной большей части аварий и катастроф сложных человеко-машинных систем являются антропогенные ошибки, заключающиеся во вводе неверных значений параметров, неверном указании режимов или вводе команд и т.п. По последствиям к этому близки ситуации, когда интерпретирующие технические компоненты АСУТП неверно воспринимают формально правильные, но слабо защищенные от искажений данные и команды, либо когда формирующие компоненты выдают ошибочные данные или команды.

Под дефектными в представляемой работе понимаются данные, которые не соответствуют форматам (протоколам, регламентам, пользовательским и операторским инструкциям), установленным в конкретной АСУТП для соответствующих вводимых элементов информации, либо не отображают фактические значения переменных величин (в пределах разрешенных допусков), команд, режимов и т.д., подлежащих вводу в АСУТП.

Предполагается, что проникновение дефектных данных происходит, главным образом, при кооперативных (по терминологии, используемой в теории игр) взаимодействиях действующих субъектов с АСУТП, когда все они заинтересованы в регламентной работе, а дефектные данные вводятся непреднамеренно. Для противоположных ситуаций с антагонистическими взаимодействиями требуются иные меры защиты.

Конкретные задачи защиты от дефектных данных по-разному формулируются и решаются на трёх основных стадиях жизненного цикла системы:

- стадия разработки информационного обеспечения АСУТП;
- стадия инсталляции информационного обеспечения, под которой понимается ввод условно постоянной информации (меню, тезаурусов, состава и форматов информации в диалоговых окнах);
- стадия текущей эксплуатации.

На двух последних стадиях происходят взаимодействия "человек-реальная система", но с точки зрения защитных процедур они существенно различаются в двух отношениях:

во-первых, инсталляцию обычно проводит немногочисленный персонал с относительно высоким уровнем подготовки, а в эксплуатации участвуют большие контингенты, и средний уровень подготовки здесь зачастую ниже;

во-вторых, стадия инсталляции выполняется единожды или, по крайней мере, не так часто, и это делает допустимым применение длительных защитных процедур; при эксплуатации время реакции АСУТП на вводимые данные и команды бывает жестко ограничено, что сужает диапазон приемлемых защитных процедур.

При разработке информационного обеспечения АСУТП важно учесть факторы помехозащищенности его элементов, под которой здесь понимается в первую очередь их взаимная различимость. Для количественной оценки степени различимости необходимо ввести адекватную скалярную метрику $\rho(e_1, e_2)$ в пространствах информационных элементов определенного типа E. Понятие метрики пространства, являющееся одним из базовых в функциональном анализе, широко используется, в частности в вычислительной

математике, применительно к пространствам из элементов числовой природы (скаляров, векторов, матриц, функций). Применительно к рассматриваемым ситуациям это понятие необходимо распространить с (определенными ограничениями) на элементы нечисловой природы (литералы, пиктограммы, фразы), учитывая при этом физические принципы ввода таких данных (буквенно-цифровые группы с учетом раскладки клавиатуры, сигнальные флажки с учетом их взаиморасположения в диалоговом окне, символы-иконки из предъявляемого набора, звукоряды при голосовой подаче команд). Минимально допустимые метрические промежутки устанавливаются с учетом опасности последствий подмены e_1 на e_2, а также имеющихся статистических данных об эргономике и психофизиологии работы человека-оператора.

При инсталляции конкретной версии информационного обеспечения АСУТП весьма желательно провести полный анализ попарной различимости внутри эквифункциональных групп элементов системного тезауруса. При обнаружении опасно близких пар их следует либо заменить, либо присвоить им категорию объектов, ввод которых требует подтверждения.

Опасность проникновения дефектных данных на стадии эксплуатации может быть уменьшена при оснащении АСУТП блоками автоверификации данных (АВД) – компьютерными процедурами проверки их бездефектности непосредственно после ввода и перед выполнением соответствующей команды основного рабочего процесса. Можно строить такие программные процедуры-фильтры для анализа интервальных (принадлежащих сплошным множествам) и дискретных данных, для взаимно независимых и взаимосвязанных данных. Возможно, хорошим решением будет возможность оперативной установки уровня "глубины" фильтрации, чтобы оптимально сочетать тщательность защитных мер с приемлемой продолжительностью сеанса АВД.

Трубопроводные коммуникации относятся к техническим системам повышенного риска, в которых последствия проникновения дефектных данных могут быть весьма тяжелы. В работе рассматриваются особенности действующих и перспективных АСУТП трубопроводных систем с точки зрения применения изложенных выше положений.