эффективных методов и средств для повышения качества решения ключевых проблем разработки и верификации микропроцессорных СОБД.

К одному из вышеописанных способов относится автоматизация задач с помощью дополнительного специального ПО. Такой подход позволяет уменьшить влияние человеческого фактора во время проверки спецификаций и упростить разработку контролепригодного АПК. Средства автоматизации могут сократить затраты, например, выявляя ошибки проектирования до тестирования или имитационных испытаний. Для СОБД важным является то, что автоматизация дает возможность улучшить показатели отказоустойчивости и безопасности. Однако данный способ требует формализации, что затруднительно при разнообразии решаемых задач и элементной базы.

В докладе рассматривается три программных комплекса (ПК), разработанных для автоматизации ряда процессов разработки и верификации микропроцессорных СОБД. Данные ПК работают с программами PIC-контроллеров модели 16F877A и других, имеющих аналогичный набор команд исполнения.

Первый из них, *Formal Time Verifier,* основан на практике верификации микропроцессорных СЖАТ и предназначен для оценки временных параметров анализируемых систем: определение гарантированного времени перехода в безопасное состояние по тайм-ауту, вычисление частоты опроса внешних устройств и др. Такие задачи характерны для СОБД, так как они относятся к системам реального времени. ПК позволяет вычислять время выполнения между двумя произвольными точками, определять обстоятельства зацикливания программы, формировать доказательство обязательного завершения алгоритма, выполнять поиск точек программы, где выполнение обязательно произойдет при каждом выполнении тела цикла. Функционально *Formal Time Verifier* проводит синтаксический разбор исходного кода программы, далее создается граф переходов и в последующем ПК использует специально разработанные алгоритмы, представляющие собой решения задач на графах.

Во вторую группу задач входит оценка степени диверситета систем. Диверситет является одним из основных способов повышения отказоустойчивости и безопасности СОБД; он заключается в создании как можно более разных систем таким образом, чтобы в случае отказа они вели себя по-разному. Это позволяет обнаружить проблему и перейти в безопасное состояние. Важной задачей при построении таких систем является оценка достигнутой степени диверситета, которая позволяет сделать вывод о его эффективности. Для решения подобных задач разработан ПК *Diverse Axiomatic Basis Checker,* который использует диверсификацию аксиоматических базисов, когда проектируемая система опирается на заранее определенные формализованные утверждения. Соответственно, ПК проверяет данные утверждения на основе исходного кода программ, анализируя константные отказы и отказы короткого замыкания произвольных информационных линий, охватывая отказы ячеек памяти, дешифратора команд и выполнения инструкций микроконтроллера, отказы регистров и аккумулятора.

Третий ПК *Address Detection* автоматизирует метод обнаружения отказов на основе доступности адресных данных, выбирая набор адресов по запросу пользователя. В него входят такие параметры, как множество отказов для проверки или разрешенные адресные диапазоны, и на их основании ПК проводит поиск оптимальных адресов. Целями автоматизации данного ПК являются уменьшение ошибок во время поиска адресов, нахождение оптимального из возможных наборов и уменьшение затрат.

В докладе рассматриваются задачи автоматизации, разработанные алгоритмы и особенности применения предложенных программных средств. Представленные ПК опробованы в лаборатории «Безопасность и электромагнитная совместимость технических средств» БелГУТа и зарегистрированы в 2017 году в Национальном центре интеллектуальной собственности (г. Минск).

УДК 621.38

КОМПЛЕКСНЫЙ ПОДХОД ПО ОБЕСПЕЧЕНИЮ ФУНКЦИОНАЛЬНОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА МПСУ ЖАТ

А. Ю. ВАСИЛЬЕВ
ООО «ЛокоТех-Сигнал», Российская Федерация, г. Москва

Широкое применение цифровых технологий в системах автоматизированного управления технологическими процессами обуславливает возникновение нового класса угроз – угроз информационной безопасности [1].

При реализации защиты от данного класса угроз в системах автоматизированного управления ответственными технологическими процессами (ОТП) возникает ряд трудностей, обусловленных следующими особенностями:

– различная продолжительность жизненных циклов функциональной и информационной безопасности (ФБ и ИБ);

– отсутствие на широком рынке внешних средств защиты, учитывающих повышенные требования к аппаратной и программной составляющим систем для ОТП;

– ограничения по возможности использования встраиваемых средств защиты ввиду отсутствия запаса вычислительных ресурсов у существующих систем и ограничений со стороны требований по ФБ при разработке новых.

Преодоление этих трудностей возможно двумя путями:

1 Независимое рассмотрение требований по функциональной и информационной безопасности и построение внешнего контура защиты от угроз ИБ вокруг системы.

2 Объединение жизненных циклов ФБ и ИБ с учетом особенностей систем.

В настоящее время, как правило, применяется первый путь. Например, в работе [2] показывается, что функциональную, информационную и физическую безопасности можно рассматривать как ортогональные требования и выполнять их независимо. Действительно, такой подход, на первый взгляд, наиболее прост и очевиден. Он декларируется и многими международными стандартами [3]. Однако из-за вышеперечисленных особенностей, применение этого подхода приводит к тому, что стоимость системы резко увеличивается из-за необходимости установки внешних средств защиты и их резервирования. Кроме того, применение ряда мер защиты иногда оказывается невозможным ввиду технических ограничений существующих систем, например, при передаче сигналов от напольных устройств на борт локомотива [2]. Таким образом, применение независимого подхода зачастую неэффективно, особенно для систем, имеющих большие объемы внедрения, к каким относятся системы ЖАТ, поскольку капитальные затраты на обеспечение ИБ при этом возрастают пропорционально числу систем.

Второй подход предполагает необходимость комплексного подхода к проблеме обеспечения ИБ и ФБ. Он основан на том факте, что требования к системе со стороны ИБ и ФБ зачастую похожи и различаются не столь кардинально. Ключевым отличием между ИБ и ФБ является то, что ФБ рассматривает защиту от искажения информации в системе ОТП под действием только случайных факторов, а ИБ – под действием преднамеренных. Если искажается одна и та же информация, а разница только в природе действующего фактора, то защита от преднамеренных искажений информации будет включать в себя защиту от случайных искажений, т. е. методы ИБ будут включать в себя методы ФБ. Это позволяет, во-первых, обеспечить возможность оптимизации затрат при построении системы защиты, во-вторых, повысить сам уровень защиты, т. к. применяемые методы и средства теперь становятся внутренними по отношению к защищаемой системе, в-третьих, повышается надежность системы.

С целью обоснования второго подхода рассмотрим жизненные циклы ФБ и ИБ. Жизненный цикл системы, к которой предъявляются требования функциональной безопасности, согласно международному стандарту МЭК 61508 [4] состоит из следующих этапов: концепция, определение системы и условий применения, анализ рисков, требования к системе, распределение требований в системе, проектирование, изготовление, установка, валидация, приемка системы, эксплуатация и техническое обслуживание, модификация и модернизация, вывод из эксплуатации.

В свою очередь жизненный цикл системы, к которой предъявляются требования информационной безопасности, согласно МЭК 62443 [5] состоит из схожих этапов: идентификация, составление концепции, функциональный анализ и технические требования, функциональный проект, рабочий проект, конструирование, действие (ввод в эксплуатацию и техническое обслуживание), контроль за соблюдением установленных требований, снятие с эксплуатации.

При первом подходе, при введении новых нормативных документов по информационной безопасности, существующие системы должны быть модернизированы, чтобы соответствовать новым требованиям. Поэтому жизненные циклы функциональной и информационной безопасности будут следовать условно последовательно, т. е. вначале идут этапы жизненного цикла, относящиеся к функциональной безопасности, а на этапе модернизации начнется жизненный цикл, относящийся к информационной безопасности.

Для вновь проектируемых систем структура имеет иной вид. В данном случае жизненные циклы выполняются условно параллельно, т. е. после этапа цикла функциональной безопасности (или одновременно с ним) идет аналогичный этап жизненного цикла информационной безопасности.

Теперь рассмотрим возможность объединения требований и методов их реализации на примере этапа жизненного цикла «Изготовление системы» (рисунок 1).

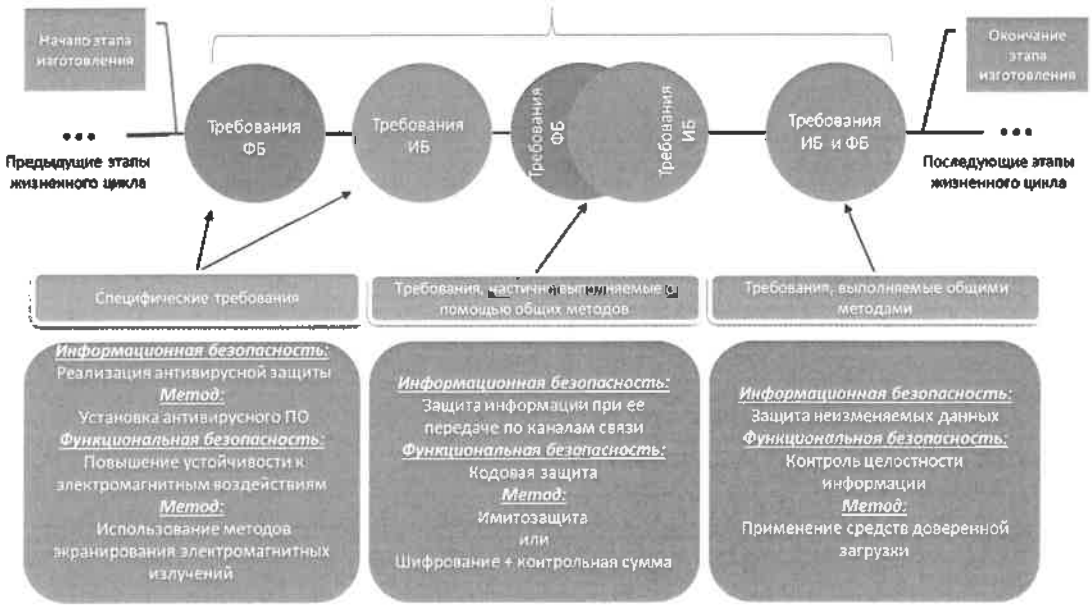

Рисунок 1 – Комплексный подход при реализации этапа «Изготовление системы»

Как видно из рисунка, некоторые требования являются специфичными для того или иного вида безопасности, например, для обеспечения ИБ необходима реализация антивирусной защиты, которая совершенно не требуется для обеспечения ФБ.

Часть требований может обеспечиваться совместным применением методов ФБ и ИБ: это, например, защита информации при ее передаче по каналам связи. В качестве методов могут применяться имитозащита или шифрование данных, дополненных контрольной суммой. Сущность обоих методов состоит во внесении избыточности, однако, в отличие от ФБ, избыточность, вносимая для обеспечения ИБ, должна вноситься таким образом, чтобы злоумышленник не имел возможности получить полную информацию о системе за разумное время, т. е. часть информации должна быть засекречена.

И, наконец, имеется группа требований, которые могут быть частично или полностью реализованы общими методами. Примером таких требований является защита неизменяемых данных для ИБ и контроль целостности информации для ФБ. Оба этих требования могут быть обеспечены с помощью применения средств доверенной загрузки.

Таким образом, предложенный подход позволит оптимизировать программные и аппаратные средства, что в свою очередь приведет к уменьшению стоимости системы, а также устранит возможные проблемы с совместимостью.

При реализации такого подхода следует отметить ряд трудностей: сложность реализации, т. к. разработчик должен иметь соответствующие компетенции не только в области функциональной, но и в области информационной безопасности, и отсутствие в настоящее время нормативной базы и нормативного регулирования для его реализации.

Список литературы

1 **Гросс, В. А.** Повышение киберзащищенности МПСУ ЖАТ / В. А. Гросс // Автоматика, связь и информатика. – 2016. – № 5. – С. 12–15.

2 **Безродный, Б. Ф.** Отличительные особенности кибербезопасности АСУ ТП / Б. Ф. Безродный // Железнодорожный транспорт. – 2018. – № 5. – С. 52–54.

3 Железные дороги. Системы связи, сигнализации и обработки данных. Требования к обеспечению безопасной передачи информации: ГОСТ Р МЭК 62280-2017. – Введ. 01.07.2017. – М. : Стандартинформ, 2017.

4 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью : ГОСТ Р МЭК 61508–2012. – Введ. 29.12.2012. – М. : Стандартинформ, 2012.

5 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели: ГОСТ Р 56205–2014. – Введ. 10.11.2014. – М. : : Стандартинформ, 2014.