ООО «3В Сервис»
РФ, 127051, Москва, ул. Трубная 25 стр 1 офис 6
Тел./ф (495) 221-22-53
www.3v-services.com

Утверждаю
генеральный директор
ООО «3В Сервис»

Петухов В.Н.

Среда динамического моделирования технических систем SimInTech™

Анализ угроз защищенности

Модуль генерации кода для систем реального времени

ШИФР ГК16А3

Москва, 2016

Аннотация

В данном программном документе приведен анализ угроз, связанных с несанкционированным изменением программного обеспечения в процессе жизненного цикла создания модуля генерации кода в среде SimInTech.

Указан порядок применения технических и административных средств, методов и контроля с целью недопущения несанкционированного изменения функциональных характеристик программного обеспечения.

СОДЕРЖАНИЕ

1. Ведение

План анализ угроз защищенности составлен для модуля генерации кода систем реального времени, входящего в состав SimInTech.

Программа для ЭВМ “Среда динамического моделирования SimInTech”, (сокращенное название «SimInTech»), свидетельство о регистрации №2010617758 - современная среда интеллектуальной системы автоматизированного **проектирования** (САПР), предназначенная для детального исследования и анализа нестационарных процессов в системах автоматического управления, в следящих приводах и роботах, в любых технических системах, описание динамики которых может быть реализовано методами структурного моделирования.

SimInTech обеспечивает создание алгоритмов управления в виде функционально-блочных диаграмм. ПО содержит в себе математическое ядро для проведения динамического расчета созданного алгоритма управления путем задания входных воздействий и анализа изменений внутренних параметров и выходных значений во время моделирования.

SimInTech является базовым программным обеспечением для верифицируемого модуля. Комплексная система моделирования систем управления и программирования приборов включает в себя:

- модуль генерации кода для автоматической генерации исходных кодов и исполняемых модулей;
- среду разработки для проектирования алгоритмов управления в виде наглядных функционально-блочных диаграмм;
- систему исполнения программ для контроллеров систем управления, для выполнения сгенерированных при помощи генератора кода исполняемых модулей на приборах.

Предметом данного отчета является анализ угроз несанкционированного изменения ПО в процессе применения модуля генерации кода для систем управления реального времени.

1.1 Цели анализа угроз защищенности

В процессе жизненного цикла разработки и поддержки модуля генерации кода происходят изменения, связанные с созданием новых версий как самого модуля, так и других частей комплексной системы моделирования.

Основное назначение данного документа: обеспечить процесс разработки программного обеспечения таким образом, чтобы неуполномоченные лица и не предназначенные для этой цели системы не могли читать и изменять программы и данные, и, в то же время, был обеспечен необходимый доступ для уполномоченных лиц и предназначенных для этой цели систем.

2. Основание для разработки

Основанием для разработки является:

Договор N 437 - 01 от 26.07.2013 по теме: «Разработка программного обеспечения верхнего уровня программно-технического комплекта средств автоматического управления».

Заказчик ООО «Московский завод «ФИЗПРИБОР».

SimInTech. Техническое задание. Модуль генерации кода систем реального времени.

SimInTech. Руководство пользователя.

План особо важных работ по доработке программного обеспечения на 2015 год. Утвержден 15.02.2015. ООО «3В Сервис».

Требования к плану работ обеспечены со стороны следующих стандартов:

- ГОСТ Р МЭК 61513-2011;
- ГОСТ Р МЭК 62138-2010;
- ГОСТ Р МЭК 60880-2011.

3. Термины и определения

3.1 Защищенность (security): Способность компьютерной системы защитить информацию и данные так, чтобы не допустить их несанкционированного прочтения или изменения другими системами и отдельными лицами, и для того, чтобы допущенные к ним системы и лица не получали отказов.

система хранения различных видов файлов, истории их изменений, архивных фалов, расположенная на сервере с возможностью удаленного доступа.

3.2 Тестовая версия ПО: версия программного обеспечение прошедшая проверку разработчиком и готовая для независимого тестирования. набор последовательности работы ПО для преобразования входных данных программ:ы или подпрограммы в выходные данные.

3.3 Новая версия ПО: версия программного обеспечения, прошедшая независимую проверку и предназначенная для передачи заказчику или пользователю для опытной эксплуатации.

3.4 Коммит: фиксация добавления изменения в исходных кодах, документах, и вспомогательных файлов в репозитории, обеспечивает точку сохранения процесса разработки проекта.

3.5 **Ветвь:** сохраненная в системе управления версиями последовательность коммитов обеспечивающая возможность параллельного изменения в исходных кодах, документах, и вспомогательных файлов.

3.6 Релиз: любая собранная версия программного обеспечения, предназначенная для внутреннего или внешнего тестирования.

3.7 Расчетная схема SimInTech (SimInTech simulation diagram): структурная схема, созданная в окне графического редактора SimInTech, описывающая на предметно-ориентированном языке математическую модель алгоритма, процесса или объекта, динамику поведения которого во времени, можно представить в виде системы алгебраических и дифференциальных уравнений в форме Коши. На основании расчетной схемы ядро SimInTech обеспечивает математическое моделирование динамического поведения объекта во времени с заданной точностью.

3.8 Видеокадр (mnemo): проект SimInTech в виде интерактивной и анимированной структурной схемы, позволяющий при моделировании оказывать воздействие на алгоритм или модель и наблюдать результаты работы.

3.9 Проект SimInTech (SimInTech project): файл, содержащий расчетную схему, созданную в графическом редакторе SimInTech, сохраненный на диске в виде бинарного и/или текстового файла с уникальным именем и расширением «prt» (для бинарного) и «xprt» (для текстового) файла. Проект SimInTech содержит расчетную схему – математическую модель, предназначенную для расчета тем или иным математическим решателем или расчетным кодом.

3.10 Пакет SimInTech (SimInTech pack): - файл, содержащий перечень проектов SimInTech и порядок их совместного запуска на расчет (моделирование), имеющий расширение «pak» и являющийся основным файлом для организации комплексной модели. Проекты, запускаемые на расчет в пакетном режиме, имеют одну базу сигналов в памяти компьютера и единый синхронизатор расчетного (модельного) времени, за счет чего они могут обмениваться значениями граничных (входных и выходных) сигналов между собой на каждом шаге расчета и осуществлять моделирование в едином синхронном модельном времени.

3.11. Компьютер (computer): программируемое функциональное устройство, которое состоит из одного или нескольких процессоров и периферийного оборудования, управляется хранящимися внутри программами и способно выполнять основные вычисления, включая многочисленные арифметические или логические операции без вмешательства в этот процесс человека.

Примечание – Компьютер может быть автономным устройством или может состоять из нескольких взаимосвязанных устройств.

3.12. Компьютерная программа (computer program): набор упорядоченных команд и данных, которые описывают операции в форме, приемлемой для их выполнения компьютером.

3.13. Компьютерная система (computer-based system): система контроля и управления, функции которой, в большей своей части, зависят от использования микропроцессоров, программируемого электронного оборудования или компьютеров, либо полностью определяются таким использованием.

Примечание – Эквивалентно следующему: цифровые системы, системы с программным обеспечением, программируемые системы.

3.14. Данные (data): представление информации или команд в виде, пригодном для передачи, интерпретации или обработки с помощью компьютера.

Примечание – Данные, необходимые для определения параметров и для реализации прикладных и служебных функций в системе называются «прикладными данными».

3.14. Библиотека (library): набор связанных элементов ПО, сгруппированных вместе, но индивидуально отбираемых для включения в окончательный продукт ПО.

3.16. Операционное системное программное обеспечение (operation system software): программное обеспечение, выполняемое на целевом процессоре во время работы, такое как драйверы и сервисы ввода/вывода, управление прерываниями, планировщик, драйверы связи, библиотеки прикладных программ, диагностирование во время работы, управление резервированием и смягченной деградацией.

3.17. Ролевое управление доступом (role-based access control): управление доступом на основе правил, определяющих разрешение доступа пользователей к объекту (функции, данные) не на индивидуальном основании, а на основании принадлежности к группам с идентичными задачами.

3.18. Программное обеспечение (ПО) (software): программы (т.е. набор упорядоченных команд), данные, правила и любая соответствующая документация, относящаяся к работе компьютерной системы контроля и управления. [МЭК 62138, 3.27]

3.19. Разработка ПО (software development): стадия жизненного цикла ПО, которая приводит к созданию ПО системы контроля и управления или программного продукта. Она охватывает деятельность, начиная от спецификации требований и до валидации и установки на объекте.

3.20. Модификация ПО (software modification): изменение в уже согласованном документе (или документах), ведущее к изменению рабочей программы.

П р и м е ч а н и е – Модификации ПО могут происходить либо в процессе первоначальной разработки ПО (например, устранение ошибок, обнаруженных на поздних этапах разработки), либо когда ПО уже находится в эксплуатации.

3.21. Версия ПО (software version): экземпляр программного продукта, полученный путем модификации или корректировки предыдущего программного продукта.

3.22. Спецификация (specification): документ, в котором полным, точным и проверяемым образом изложены требования, проектные свойства и другие характеристики системы или компоненты и, часто, процедуры подтверждения удовлетворения этим требованиям.

Примечание – Существуют различные типы спецификаций, например, спецификация требований к ПО или спецификация проекта.

4. Анализ защищенности в жизненном цикле

4.1 Защищенность в жизненном цикле на этапе разработки

Разработка ПО SimInTech осуществляется итерационными циклами. Каждый цикл связан с разработкой ограниченного функционала (см. п. 4 Плана управления конфигурацией п.п. 5.1 и 5.3 Плана обеспечения качества).

В процессе разработки ПО доступ к исходным кодам должны получать все программисты, выполняющие изменения в данных в ПО SimInTech.

Каждый из программистов имеет возможность компилировать ПО и выполняет сборку ПО на своем рабочем месте, для внутренней проверки внесенных изменений и работы системы.

Для локального тестирования программисты используют тестовые примеры, которые в дальнейшем используются для независимой верификации ПО.

4.1.1 Угрозы защищенности этапа разработки

Возможные риски этапа разработки:

- Несанкционированное изменение исходных кодов программистом, работающим над частью системы, вне зоны работы программиста.
- Возможная сборка и компиляция исполняемых библиотек и модулей из несанкционированных исходных кодов и их попадание в дистрибутив.
- Возможное изменение тестовых проектов в процессе разработки и верификация на основе несанкционированно изменённых тестовых проектов.

4.1.2 Защитные меры для снижения рисков при разработке

Для снижения рисков связанных с несанкционированным изменением исходных кодов в процессе разработки используется комплексный подход, сочетающий административные процедуры и использование среды управления конфигурацией GIT и механизмов программных средства разработки в DELPHI.

4.1.2.1 Организационные и административные процедуры

Организационные меры защиты от несанкционированного изменения исходных кодов заключаются в запрете создания базовых версий ПО SimInTech разработчиками, не имеющими полномочий. Создание тестовой версии ПО SimInTech может осуществляться только ведущим разработчиком, который имеет соответствующие полномочия, согласно плану управления конфигурацией.

Программистам запрещается сохранять на сменных носителях и передавать по сети (внутренней или внешней) любые исполняемые и бинарные файлы, созданные в процессе разработки и использованные в процессе отладки разрабатываемых решений.

Размещение официальных дистрибутивов на сайте осуществляется только уполномоченными специалистами.

4.1.2.2 Ролевой доступ в системе управления изменениями

Вся разработка каждым отдельным программистом в рамках итерации ведется в отдельных каталогах исключительно под управлением системы версионного контроля GIT. Каждая доработка в рамках выполнения задачи сохраняется в виде отдельного коммита, с возможностью отката в предыдущее состояние.

Среда управления конфигурацией GIT настроена с учетом ролевого доступа программистами. Для каждого программиста создается учетная запись, в которой указываются директории и файлы, с доступами для чтения и записи. Настройки должны проверяться ведущим программистом перед каждой итерацией, но не реже одного раза в квартал.

Работа всех программистов в системе GIT передаётся в виде исходных кодов. Собранные исполняемые файлы используются только на локальных рабочих местах для тестирования и не передаются в общую систему управления версиями.

Программист может делать локальные копии файлов для работы и изменения, при создании коммита, система GIT предотвращает изменение файлов, доступа на изменение которых у программиста нет.

Слияние всех веток изменений после завершении очередной итерации выполняется только уполномоченным лицом (Ведущим программистом).

После проверки созданного ПО уполномоченным лицом, осуществляется формирование финального коммита в системе с последними изменениями.

4.1.2.3 Защитные средства среды разработки

Уполномоченный специалист (Ведущий разработчик) осуществляет присвоение идентификационных атрибутов создаваемой версии ПО SimInTech в среде разработки Delphi.

Уполномоченный специалист осуществляет подпись всех создаваемых дистрибутивов цифровой подписью.

ПО SimInTech распространяется исключительно в виде дистрибутива, который подписан верифицированной цифровой подписью.

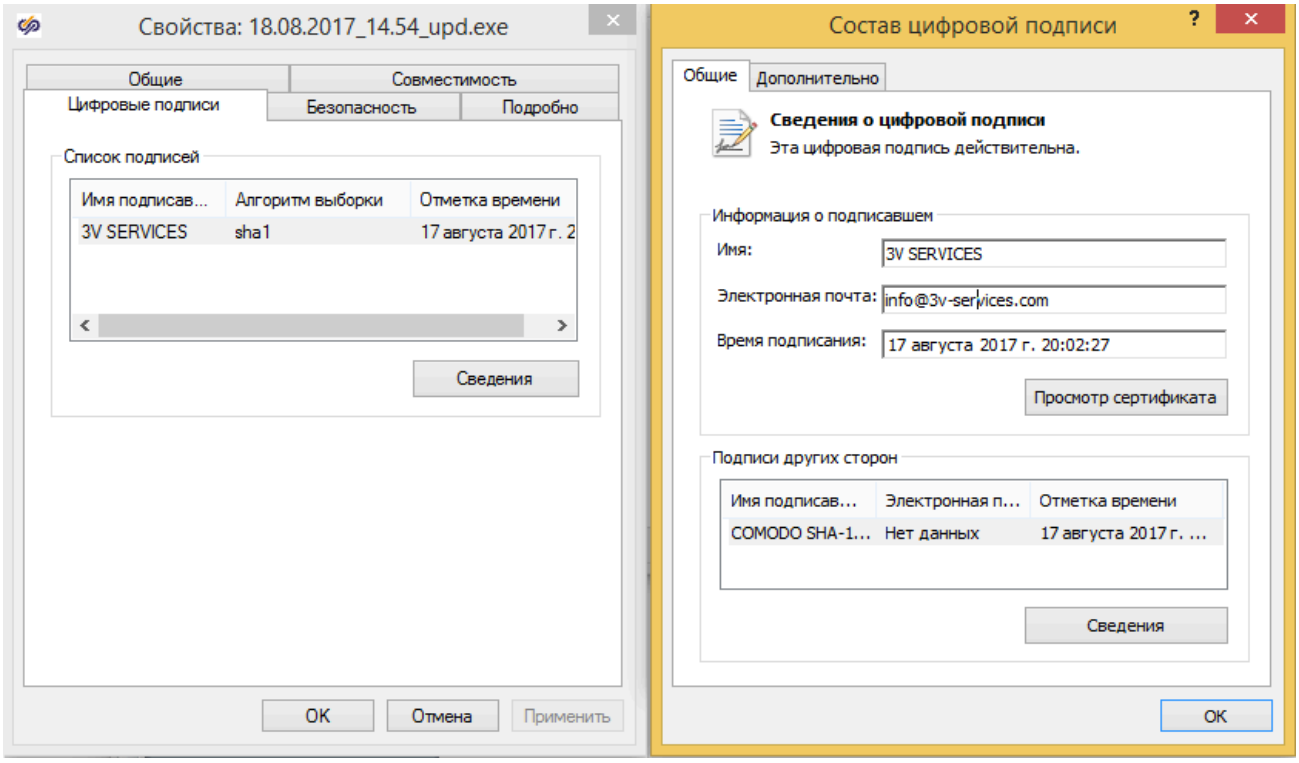

Рисунок 1. Цифровая подпись дистрибутивов

4.2 Защищенность в жизненном цикле на этапе применения

Модуль генерации кода в составе ПО SimInTech используется для генерации кода прикладного программного обеспечения. В качестве исходных данных используется проект алгоритмов в формате SimInTech.

Рекомендации по применению ПО SimInTech описаны в документе «Типовой процесс создания прикладного программного обеспечения для систем контроля и управления важных для безопасности АЭС». Основные этапы процесса представлены на рисунке 2.

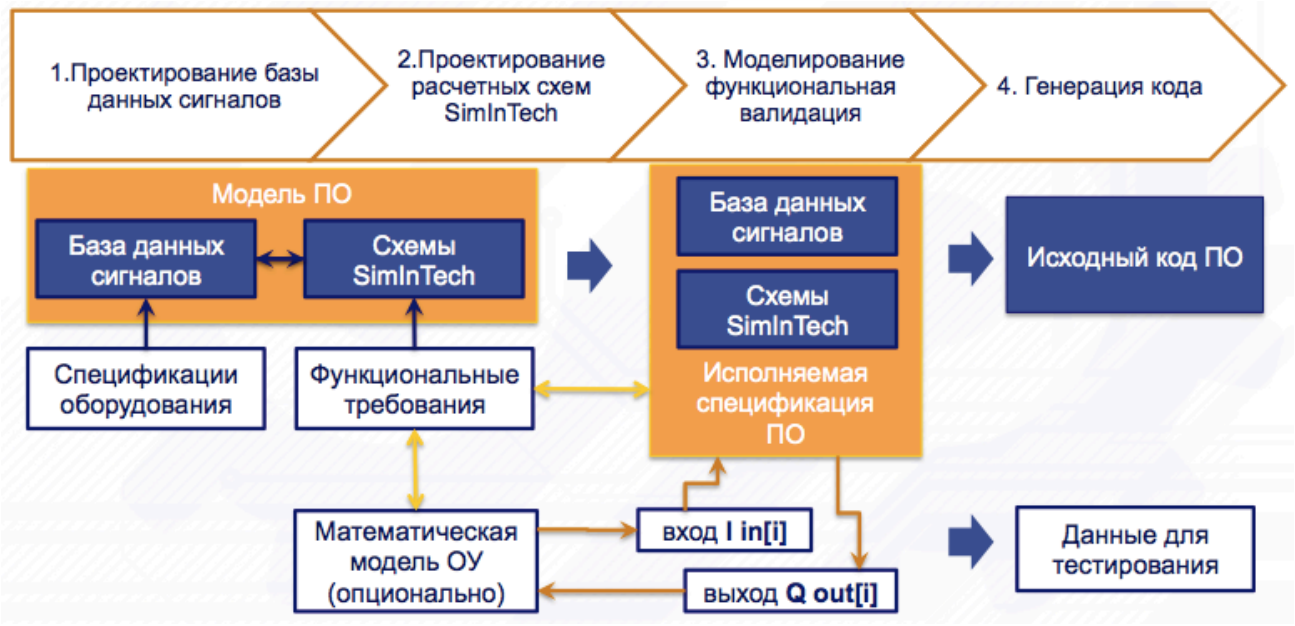

Рисунок 2. Типовой процесс создания прикладного ПО в SimInTech

Для обеспечения защищенности от несанкционированного изменения данных, необходимо защитить процесс подготовки проекта в SimInTech, а также исходный код, полученный в результате работы модуля генерации кода.

4.2.1 Угрозы защищенности этапа применения

Разработка проекта в среде SimInTech сопровождается созданием файлов, содержащих проекты в формате SimInTech, базу данных сигналов и другие вспомогательные данные.

ПО SimInTech использует файлы для хранения всех данных в процессе. Угрозами на этапе применения модуля генерации кода являются:

- Угрозы несанкционированного изменения файлов проектов, базы данных сигналов, и тестовых проектов, на этапах 1 – 3.

- Несанкционированное изменение библиотек и модулей установленного ПО и, как следствие, возможное изменение в генерации кода.
- Угроза изменения файлов исходных кодов после автоматической генерации кода.

4.2.2 Защитные меры для снижения рисков этапа применения

4.2.2.1 Защита проекта алгоритмов в SimInTech

На этапах 1 - 3 создания прикладного ПО в среде SimInTech необходимо применять средства, и способы защиты информации применяемые в общем проекте создания системы управления, рекомендованные стандартами ГОСТ Р МЭК 61513-2011, ГОСТ Р МЭК 62138-2010, ГОСТ Р МЭК 60880-2011.

ПО SimInTech допускает применение к своим файлам любых рекомендованных средств защиты информации, включая:

- Ролевое управление доступом к файлам.
- Использование систем управления версиями.
- Шифрование данных при хранении.
- Резервирование данных.
- Другие средства защиты, применяемые в процессе разработки систем управления.

Кроме этого на этапе подготовки данных рекомендуется использовать встроенные средства зашиты информации в ПО SimInTech:

- Интеграция с системой управления версиями GIT или SVN.
- Использование паролей для защиты проектов от изменения.
- Сохранение копий предыдущих файлов при изменениях системы.

Разработку алгоритмов рекомендуется разбить на две части:

- Первичная настройка и первичная настройка проекта ПО «SimInTech» в режиме «Разработчик».
- Создание прикладного ПО систем управления в режиме «Пользователь».

4.2.2.2 Защита модуля генерации кода ПО SimInTech

Для снижения риска модификации средств разработки необходимо использовать только версии, полученные от разработчика.

Компьютеры, на которых развернуты средства разработки ПО SimInTech, должны быть защищенные средствами антивирусной защиты и защиты от проникновения. Инсталляция ПО SimInTech должна производиться лицом, обладающим правами администратора.

При установке ПО SimInTech необходимо убедиться, что дистрибутив подписан цифровой подписью (см. рисунок 1).

После первого запуска программы убедиться, что окно содержит правильный идентификатор версии (п. 5.1.1 Плана управления конфигурацией) (см. рисунок 3).

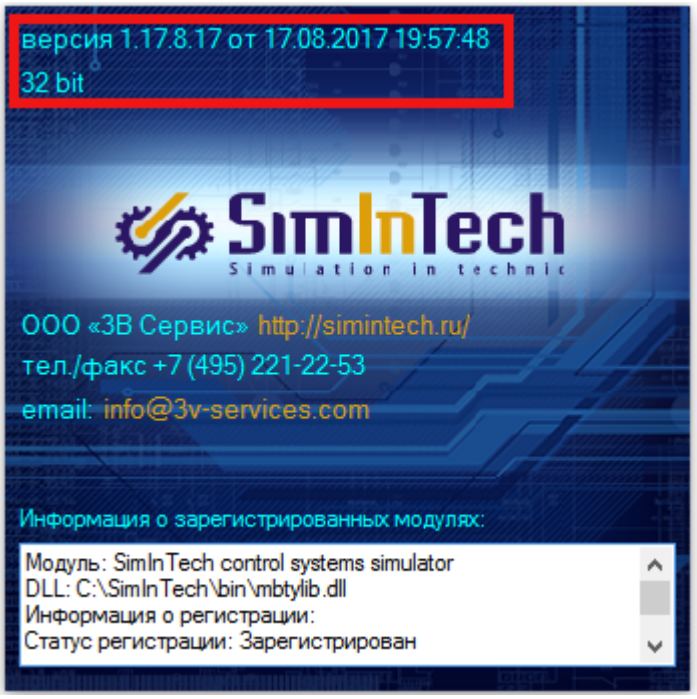

Рисунок 3. Идентификатор версии в окне сведения о программе.

Такую же проверку необходимо проводить после каждого обновления системы.

Разработку алгоритмов управления рекомендуется вести в режиме пользователя без прав администратора и права изменения директории установки ПО SimInTech.

Обновления системы рекомендуется проводить средствами автообновления, в случае наличия доступа к сети интернет, с рабочего места разработчика.

Режим обновления ПО SimInTech должен быть установлен в «обычный режим», для исключения обновления «тестовыми версиями».

4.2.2.3 Защита исходного кода

Код, созданный генератором кода, представляет собой набор файлов, к которым необходимо применять такие же средства защиты, как и к файлам проектов (см. п. 4.2.2.3).

При использование исполнительной системы NordWind в режиме отладки прикладного ПО в среде SimInTech необходимо проверять соответствие файлов расчетной схемы и исполняемого кода, подключенного в режиме отладки.

В случае не совпадения расчетной схемы и сгенерированного кода ПО SimInTech выдает предупреждение в окне отладки (см. рисунок 4).

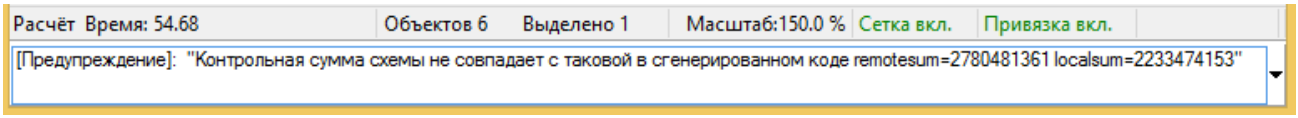

Рисунок 4. Предупреждения о несоответствии контрольной суммы прикладного ПО и расчетной схемы