БЕЗОПАСНОСТЬ ПРОГРАММНЫХ СИСТЕМ

Обзор функций подсистемы безопасности

Обеспечение безопасности программных систем на сегодняшний день является одной из стратегических задач при их разработке. Рассматривая проблемы обеспечения безопасности, можно выделить две большие области: функциональную и информационную безопасность.

Кирилл **Силкин**
компания ЭлеСи

Функциональная безопасность призвана решать проблемы, связанные с отказовыми ситуациями - восстановление работоспособности систем при возникновении непредумышленного воздействия на них (дефекты программ, работа с некорректными данными, сбои аппаратуры).

Проблемы, решаемые в области информационной безопасности, напротив связаны с зашитой от предумышленных воздействий на систему или на информацию, которой система оперирует.

Проблемы информационной безопасности возникают вследствие увеличения сложности, масштабности систем, увеличения количества их пользователей, накопления массивов деловой, конфиденциальной информации и затрагивают сейчас практически все программные комплексы.

Также можно отметить тот факт, что полностью решить проблемы информационной безопасности практически невозможно. Всегда будут существовать люди, заинтересованные в получении конфиденциальной информации своих конкурентов. Постоянно развиваются программные комплексы по преодолению систем информационной безопасности. Так что можно говорить только о снижении уровня риска несанкционированного доступа при использовании систем информационной безопасности.

Основными факторами развития подсистем информационной безопасности являются необходимость защиты от незаконного использования или искажения информации, предназначенной ограниченному кругу лиц. Разработчиками программных систем активно внедряются методики и средства защиты от несанкционированного доступа и других деструктивных воздействий. Для решения проблем, связанных с информационной безопасностью систем разрабатываются стандарты обеспечения информационной безопасности.

В номере «itech - интеллектуальные технологии» №3 в статье «Обеспечение информационной безопасности АСУ ТП» мы рассматривали принципы построения подсистемы безопасности пакета InfinitySCADA. Сегодня мы продолжим разговор на эту тему и расскажем, какими функциями обладает подсистема информационной безопасности InfinitySuite.

ПРИНЦИПЫ ПОСТРОЕНИЯ ПОДСИСТЕМЫ БЕЗОПАСНОСТИ INFINITYSUITE

Итак, вспомним о том, на каких принципах построена подсистема безопасности InfinitySuite. Поскольку программный пакет работает в семействе ОС Windows, то пользователями системы являются пользователи доменов и рабочих групп Windows и при настройке прав доступа к защищаемым ресурсам системы используются учетные записи пользователей Windows. Для идентификации пользователей используются стандартные протоколы аутентификации Kerberos и NTLM.

Защищаемыми ресурсами системы являются данные и основные функции. Процесс доступа к защищаемым ресурсам в общем случае проходит следующим образом:

- Клиент проходит аутентификацию на сервере, который является владельцем защищаемых ресурсов.
- Клиент передает серверу запрос на доступ к защищаемым ресурсам.
- Сервер на основании данных о разрешениях подсистемы безопасности определяет возможность доступа клиента к защищаемым ресурсам.

Более подробную информацию о принципах построения подсистемы безопасности можно найти в статье «Обеспечение информационной безопасности АСУ ТП средствами программного комплекса Infinity SCADA».

Безопасность программных систем

ЧТО МЫ ЗАЩИЩАЕМ

Итак, подсистемы информационной безопасности призваны защищать системы и данные от несанкционированного доступа, хищения информации и тому подобных проявлений злого умысла сторонних лиц.

При разработке подсистемы информационной безопасности InfinitySuite были выделены защищаемые ресурсы системы. Как уже было сказано, к защищаемым ресурсам относятся данные и основные функции системы. Приведем полный список защищаемых ресурсов и их владельцев для подсистемы информационной безопасности InfinitySuite:

Рассмотрим более детально каждый защищаемый ресурс.

ОПЕРАТИВНЫЕ ДАННЫЕ О СОСТОЯНИИ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА И ФУНКЦИЯ ПОДКЛЮЧЕНИЯ К СЕРВЕРУ ОПЕРАТИВНЫХ ДАННЫХ

Защищаемый ресурс	Владелец
Оперативные данные о состоянии технологического процесса Функция доступа к серверу оперативных данных Функции администрирования сервера оперативных данных и подсистемы резервирования Функции конфигурирования сервера оперативных данных	InfinityServer
Функция запуска программы просмотра мнемосхем Функция перехода в режим разработки Функция просмотра мнемосхем Функция видимости слоев мнемосхемы Функция запуска редактора VBA Функция закрытия приложения	InfinityHMI
Функция запуска программы просмотра истории значений технологических параметров Функция просмотра дерева технологических параметров Функция администрирования программы просмотра истории значений технологических параметров	InfinityTrends
Функция запуска программы просмотра сообщений Функция квитирования сообщений Функция администрирования программы просмотра сообщений	InfinityAlarms
Функция конфигурирования подсистемы безопасности клиентских приложений	InfinitySecurity

Основное, что представляет интерес с точки зрения несанкционированного доступа, это конечно данные. Они содержат полную картину о технологическом процессе. Их сохранность представляет наивысший интерес. Поэтому в системе предусмотрена защита подключения к серверу и доступа к этим данным. Для настройки доступа необходимо выделить две категории лиц пользователей: с правами на чтение и с правами на запись. Пользователям с правами на чтение необходимо разрешить подключение к серверу и чтение данных (рис. 1).

Права на чтение распространяются на все дерево сигналов, поэтому они не привязаны к конкретным узлам дерева, а задаются только один раз для каждого пользователя. При назначении разрешения на чтение пользователь может подключаться к серверу, просматривать структуру дерева сигналов, подписываться на изменения значений сигналов.

Еще более важной функцией является возможность изменения значения сигналов пользователем - запись в сервер. Как правило, эта функция необходима более узкому кругу пользователей системы.

Функция изменения значений сигналов может быть определена для каждого сигнала в отдельности или для выбранной ветки дерева. Причем при выдаче прав на запись для ветки дерева пользователь автоматически получает возможность изменения значений всех дочерних сигналов (рис. 2).

ФУНКЦИИ АДМИНИСТРИРОВАНИЯ СЕРВЕРА ОПЕРАТИВНЫХ ДАННЫХ И ПОДСИСТЕМЫ РЕЗЕРВИРОВАНИЯ

К функциям администрирования сервера оперативных данных можно отнести операции управления сервером. Поскольку в Infinity реализовано горячее резервирование серверов, то полный список функций включает в себя:

- управление правами доступа к агенту резервирования;
- подключения к агенту резервирования;
- запуск/останов серверов оперативных данных;
- резервный переход;
- управление конфигурацией серверов.

Управление правами доступа к агенту резервирования - функция доступная, как правило, только администратору системы. Только администратор может выдавать пользователям те или иные права в соответс-

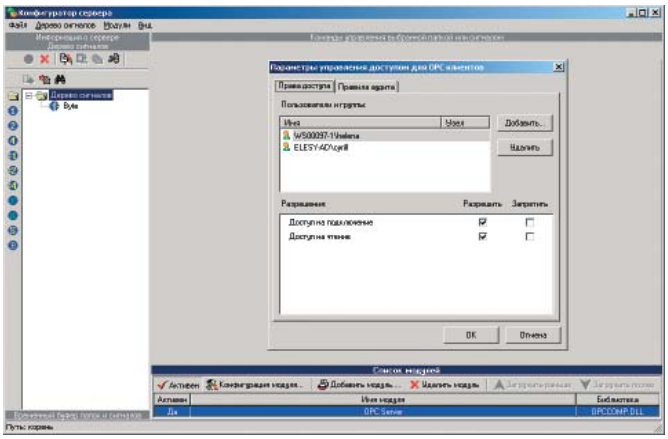

Рис. 1. Настройка прав подключения и чтения оперативных данных

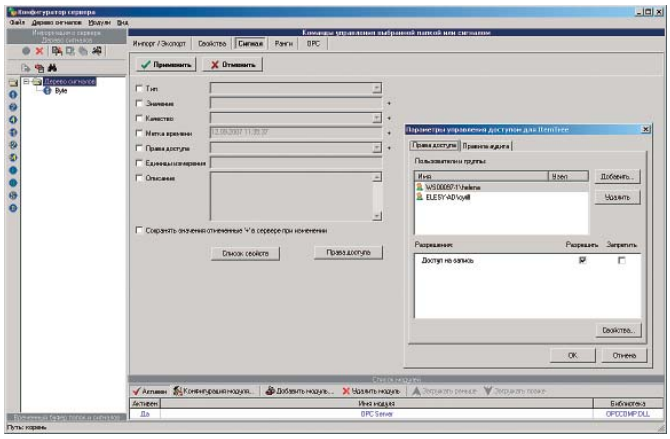

Рис. 2. Настройка прав записи оперативных данных

твии с исполняемой ролью.

Подключение к агенту резервирования необходимо для ограничения списка лиц, которым доступна информация о состоянии системы резервирования. Как правило, это администраторы или диспетчера системы, которые могут оценить, в каком состоянии она находится.

Запуск и останов серверов необходим в случае изменения конфигурации системы. Эта функция тоже, как правило, отводится администраторам.

Резервный переход необходимо иногда проводить при некорректной работе серверов. Поэтому функция доступна диспетчерам системы (рис. 3).

ФУНКЦИИ КОНФИГУРИРОВАНИЯ СЕРВЕРА ОПЕРАТИВНЫХ ДАННЫХ

Еще одной задачей, которая требует разграничения прав доступа, является изменение конфигурации серверов данных. Для ограничения прав на конфигурирование были введены следующие категории:

- управление правами доступа к конфигурации серверов;
- чтение конфигурации серверов;
- изменение конфигурации серверов.

Управление правами доступа к конфигурации серверов - функция, доступная только администратору системы. Только администратор может выдавать пользователям те или иные права в соответствии с исполняемой ролью.

Чтение конфигурации серверов может быть доступно всем пользователям или ограничено рядом лиц, которым необходимо просматривать, но не изменять конфигурационную информацию.

Изменение конфигурации серверов относится к функциям администрирования системы, которая должна быть доступна только администраторам (рис. 4).

Следующие функции подсистемы безопасности InfinitySuite относятся к клиентским приложениям системы. Роль пользователя системы определяет набор клиентских приложений и их функций, которые ему доступны. Поскольку зачастую приложения выполняют достаточно большой набор функций, то существует необходимость ограничивать доступный пользователю набор в рамках одного приложения.

Кроме того, часто бывает необходимо ограничить доступ пользователя к сторонним приложениям или функциям операционной системы. Такие возможности требуются, например, для рабочих мест операторов или диспетчеров.

Клиентская часть подсистемы безопасности InfinitySuite решает все эти задачи. С ее помощью можно ограничить запуск сторонних приложений или использование компонент ОС Windows.

Ниже рассмотрим ограничения возможностей клиентских приложений InfinitySuite, доступные в подсистеме безопасности.

защита информации

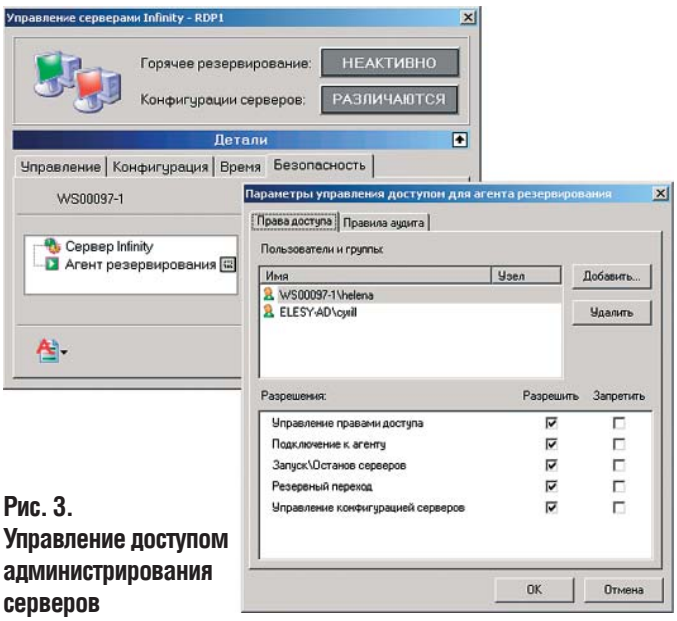

Рис. 3. Управление доступом администрирования серверов

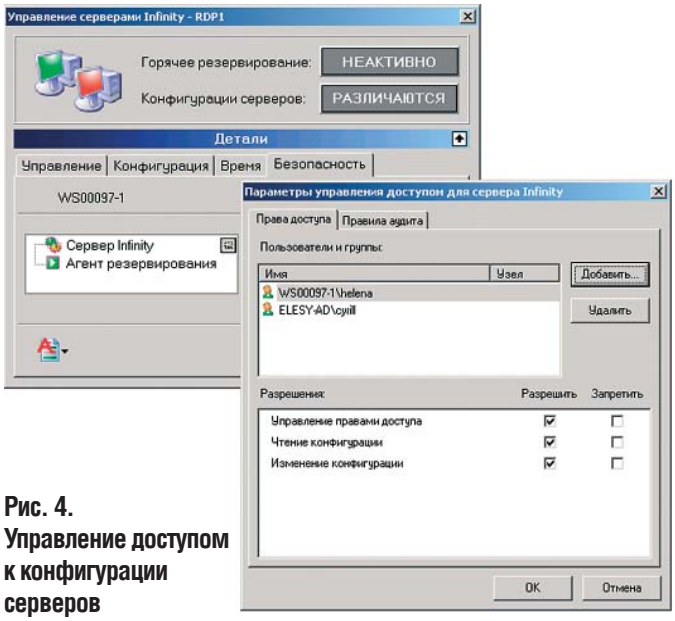

Рис. 4. Управление доступом к конфигурации серверов

Безопасность программных систем

Существует общая для всех клиентских приложений функция-ограничитель. Это функция запуска приложения. Эта функция позволяет запускать выбранное приложение только тем пользователям, которые указаны в настройках подсистемы безопасности.

ФУНКЦИЯ ПРОСМОТРА МНЕМОСХЕМ INFINITYHMI

На каждом пункте управления существует набор мнемосхем, по которым диспетчера оценивают состояние технологического процесса и управляют им. Данная функция необходима для того, чтобы разделить зоны ответственности между диспетчерами с целью разрешить просматривать только определенные мнемосхемы тому или иному пользователю. Для каждого пользователя или группы пользователей добавляется свой набор мнемосхем. При настройке могут быть использованы маски - это достаточно гибкий и удобный инструмент настройки.

ФУНКЦИЯ ПЕРЕХОДА В РЕЖИМ РАЗРАБОТКИ И ЗАПУСКА РЕДАКТОРА VBA INFINITYHMI

Функция разграничения прав на переход в режим разработки мнемосхем и запуска редактора VBA сценариев необходима для защиты от несанкционированного изменения экранов. Права на конфигурирование мнемосхем, как правило, выдаются администраторам системы.

ФУНКЦИЯ ВИДИМОСТИ СЛОЕВ МНЕМОСХЕМЫ INFINITYHMI

Мнемосхемы могут содержать несколько слоев. Каждый слой может быть необходим для работы одному или нескольким пользователям. Поэтому для разделения прав для доступа к слоям была введена эта функция. Так же как и для функции открытия мнемосхем при постройке могут использоваться маски с названиями слоев.

ФУНКЦИЯ ЗАКРЫТИЯ ПРИЛОЖЕНИЯ INFINITYHMI

Эта функция необходима пользователям, которые должны постоянно мониторить состояние технологического процесса. Для них важно не только постоянно видеть мнемосхему, но и случайно не закрыть необходимое окно. Для этого и выделена функция возможность закрытия приложения InfinityHMI.

ФУНКЦИЯ ПРОСМОТРА ДЕРЕВА ТЕХНОЛОГИЧЕСКИХ ПАРАМЕТРОВ INFINITYTRENDS

Дерево исторических технологических параметров предоставляется только кругу лиц, занимающихся анализом ситуаций, связанных с тем или иным поведением системы. Поэтому мы даем возможность ограничить круг лиц, которые могут получить доступ к этому ресурсу.

ФУНКЦИЯ АДМИНИСТРИРОВАНИЯ INFINITYTRENDS И INFINITYALARMS

Как и все функции администрирования компонент системы, функция администрирования клиентских приложений может быть доступна только администраторам. Поэтому данные функции тоже выделены в состав защищаемых ресурсов.

ФУНКЦИЯ КВИТИРОВАНИЯ СООБЩЕНИЙ INFINITYALARMS

Квитирование - подтверждение получения уведомления от системы пользователем. Квитирование подразумевает под собой начало тех или иных действий, напрямую связанных с ситуацией, о которой информирует система. Возможность квитирования сообщений является еще одним защищаемым ресурсом системы.

ФУНКЦИЯ КОНФИГУРИРОВАНИЯ ПОДСИСТЕМЫ БЕЗОПАСНОСТИ КЛИЕНТСКИХ ПРИЛОЖЕНИЙ

Как и все функции конфигурирования, настройка прав доступа к клиентским приложениям является критичной с точки зрения информационной безопасности функцией, поскольку именно при некорректной настройке этой части системы может возникнуть угроза несанкционированного доступа к данным системы. Вследствие этого функция причислена к составу защищаемых ресурсов (рис. 5, 6).

Итак, мы познакомились со всеми доступными на текущий момент функциями подсистемы информационной безопасности InfinitySuite.

Можно с большой уверенностью сказать, что функции обеспечения информационной безопасности при построении систем на базе InfinitySuite позволят снизить риск несанкционированного доступа к информации и функциям всей системы.

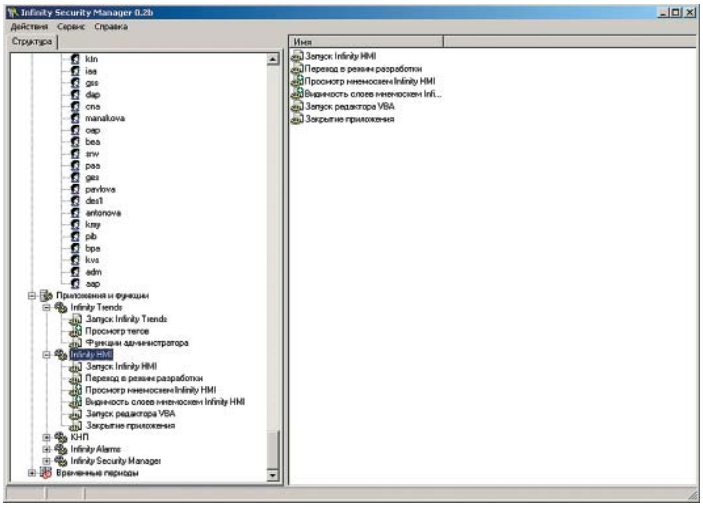

Рис. 5. Менеджер клиентской безопасности

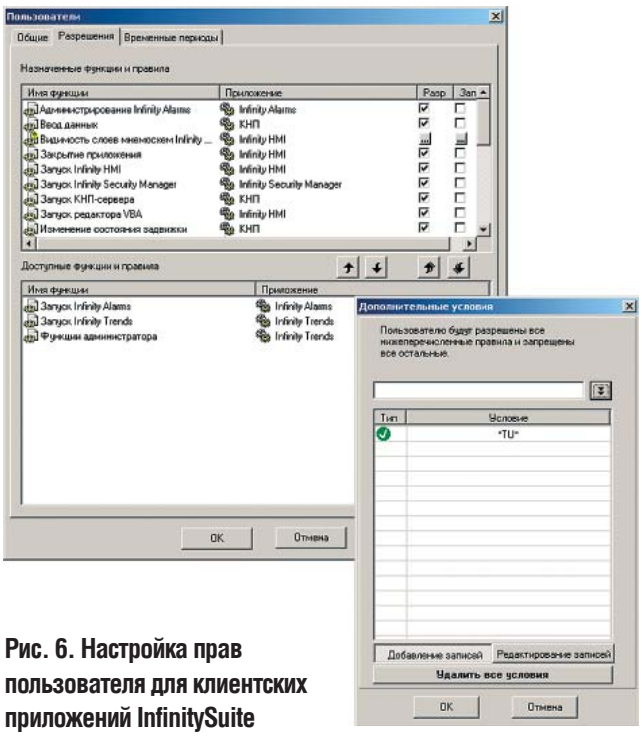

Рис. 6. Настройка прав пользователя для клиентских приложений InfinitySuite