Обеспечение информационной безопасности является одной из важнейших задач, возникающих при эксплуатации АСУ ТП. В статье представлены решения компании «ЭлеСи» для защиты информационных ресурсов АСУ ТП средствами программного комплекса Infinity SCADA, описаны принципы построения подсистемы безопасности Infinity SCADA.

ОБЕСПЕЧЕНИЕ информационной безопасности АСУ ТП

К.ф.м.н. Д.В. **Шаповалов**,
К.А. **Силкин**

Бурное развитие вычислительной техники и интенсивное внедрение информационных технологий в различные сферы человеческой деятельности способствовали резкому росту кибернетического терроризма. Обеспечение информационной безопасности стало жизненно необходимым, особенно в автоматизированных системах управления технологическими процессами (АСУ ТП), применяемых при эксплуатации территориально распределенных объектов, в которых используются потенциально опасные для окружающей среды и человека технологии. Несанкционированный доступ к подобным объектам может иметь катастрофические последствия, в связи с этим трудно недооценить актуальность проблемы безопасности в АСУ ТП. Защита информационных ресурсов АСУ ТП требует системного подхода, который предполагает, что средства и действия, используемые для обеспечения информационной безопасности – организационные, физические и программно-технические, – рассматриваются как единый комплекс взаимосвязанных, взаимодополняющих и взаимодействующих мер. К числу данных мероприятий относятся: организация физической охраны средств

вычислительной техники, носителей информации; ограничение физического доступа пользователей к терминалам, томам, каталогам, файлам; управление потоками информации посредством настроек сетевого оборудования, брандмауэров; обеспечение идентификации, контроля, аудита доступа пользователей к информационным ресурсам системы и т.п. Данная статья не ставит перед собой в качестве цели полное, исчерпывающее описание всего перечня мероприятий, необходимых для обеспечения информационной безопасности АСУ ТП. В работе рассматриваются лишь некоторые аспекты решения указанной проблемы с позиций программного обеспечения верхнего уровня АСУ ТП. В статье описываются решения по обеспечению информационной безопасности АСУ ТП, реализованные в программном комплексе Infinity SCADA компании «ЭлеСи».

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Проблема обеспечения информационной безопасности на уровне программных систем не является новой. Данной тематике посвящено большое количество книг и статей. Определен и стандартизован набор функций безопасности, которые должна реализовывать программная система. К числу основных функций безопасности относятся: аутентификация пользователей в системе, авторизация и аудит доступа пользователей к защищаемым ресурсам системы, передача и хранение конфиденциальной информации в зашифрованном виде, контроль подлинности и целостности программных компонент и др. В программном комплексе Infinity SCADA встроена поддержка всех вышеперечисленных функций безопасности. Подсистема безопасности Infinity SCADA позволяет осуществлять контроль прав и аудит доступа к следующим защищаемым ресурсам АСУ ТП:

- оперативным значениям параметров технологического процесса (чтение, запись);
- оперативным сообщениям об авариях и отклонениях в ходе технологического процесса (чтение, квитирование);
- истории изменения значений параметров и возникновения сообщений об авариях в ходе технологического процесса (чтение, добавление, изменение, удаление);
- мнемосхемы (чтение, добавление, изменение, удаление);
- конфигурационные данные технологических серверов (чтение, изменение);
- функции администрирования и конфигурирования технологических серверов (выполнение).

В системе имеется возможность настройки прав доступа и правил аудита отдельно для каждого защищаемого ресурса системы.

Подсистема безопасности Infinity SCADA позволяет осуществлять контроль прав и аудит доступа к оперативным зна-

защита информации

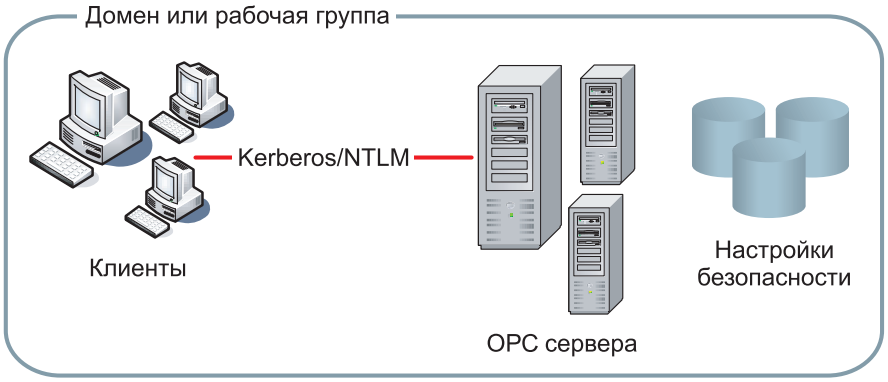

Рис. 1. Схема построения подсистемы безопасности Infinity SCADA в рамках одного диспетчерского пункта

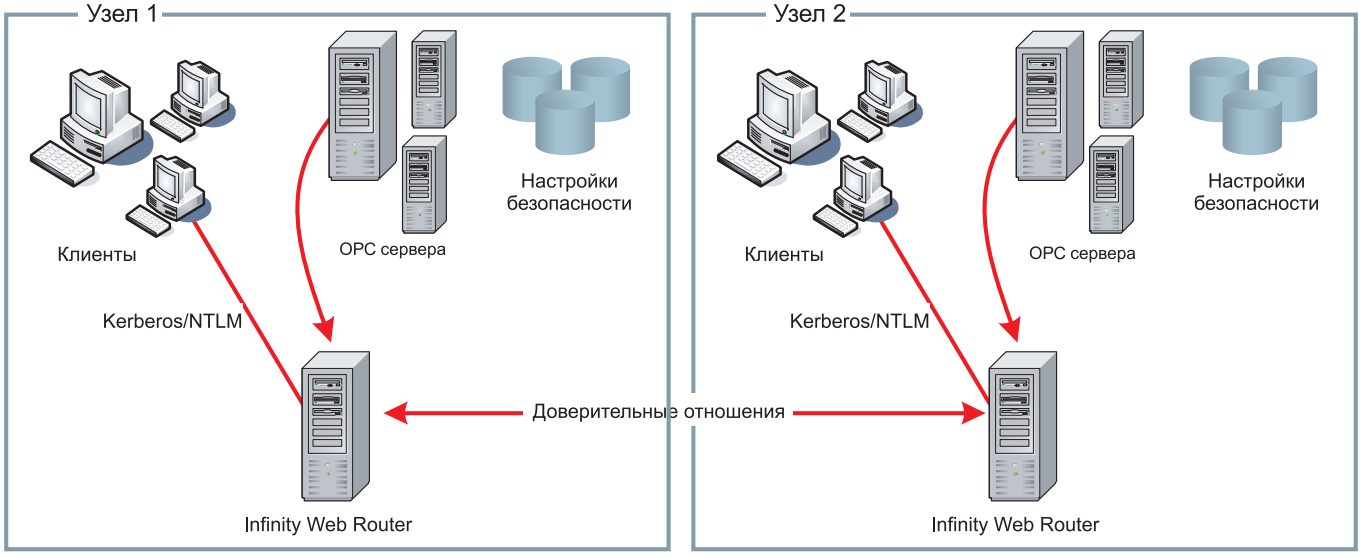

Рис. 2. Схема построения распределенной подсистемы безопасности Infinity SCADA

обеспечение информационной безопасности АСУ ТП

чениям параметров технологического процесса с высокой степенью детализации (на уровне OPC-тегов и их свойств).

В системе реализованы удобные средства просмотра журналов аудита, обеспечивающие возможность поиска и фильтрации данных аудита.

Подсистема безопасности Infinity SCADA ориентирована на использование в распределенных системах, состоящих из нескольких территориально удаленных диспетчерских пунктов. В Infinity SCADA реализована поддержка обмена технологическими данными между распределенными узлами системы в зашифрованном виде.

Принципы построения подсистемы безопасности Infinity SCADA

Рассмотрим основные принципы реализации функций безопасности в программном комплексе Infinity SCADA. Обеспечение безопасности в Infinity SCADA базируется на решениях компании Microsoft, применяемых в подсистеме безопасности ОС Windows. Ниже перечислены основные принципы построения подсистемы безопасности Infinity SCADA:

1. Пользователями системы Infinity SCADA являются пользователи ОС Windows.

2. Для идентификации пользователей в системе используются стандартные протоколы аутентификации ОС Windows: Kerberos, NTLM.

3. При настройке прав доступа к защищаемым ресурсам системы используются учетные записи пользователей доменов и групп ОС Windows.

Можно отметить следующие достоинства интеграции с подсистемой безопасности ОС Windows:

- Упрощается процедура администрирования в диспетчерских пунктах: применяются единые принципы управления учетными записями пользователей; отсутствует необходимость в дублировании учетных записей, использование групп пользователей ОС Windows позволяет снизить трудоемкость процедуры настройки прав доступа к защищаемым ресурсам.
- Возможность использования механизмов однократного ввода идентификационных данных при входе пользователей в систему.
- Применение решений, проверенных многолетней практикой использования и доказавших свою состоятельность.
- Возможность использования альтернативных программно-технических средств аутентификации сторонних производителей - таких как смарт-карты, биометрические устройства, которые интегрированы с подсистемой безопасности ОС Windows.

Схема построения подсистемы безопасности Infinity SCADA в рамках одного диспетчерского пункта, все компьютеры которого объединены в сеть с использованием рабочих групп Windows или доменов Windows 2000, связанных доверительными отношениями, представлена на рис. 1.

В системе Infinity SCADA владельцами защищаемых ресурсов являются OPC-сервера. Каждый OPC-сервер имеет свою базу данных с настройками безопасности, в которой хранятся права доступа пользователей к защищаемым ресурсам сервера и данные аудита. Процесс доступа к защищаемым ресурсам OPC-сервера в общем случае выглядит следующим образом:

1. Клиент проходит аутентификацию на сервере.

2. Клиент передает серверу запрос на доступ к защищаемому ресурсу.

3. Используя информацию из базы данных с настройками безопасности, сервер определяет возможность доступа клиента к защищаемому ресурсу и необходимость регистрации попытки доступа клиента к защищаемому ресурсу.

В распределенных АСУ ТП, состоящих из нескольких территориально удаленных диспетчерских пунктов (узлов), в которых применяются разные принципы организации локальных вычислительных сетей (рабочие группы Windows, домены Windows 2000), возникают проблемы с идентификацией пользователей одного узла в другом узле. Эта проблема может быть решена средствами ОС Windows путем дублирования учетных записей пользователей в других узлах системы и использования протокола аутентификации NTLM либо путем построения сети предприятия с использованием служб Microsoft Active Directory. Однако на практике предложенные решения не всегда могут быть применены в силу большого числа диспетчерских пунктов и использования на предприятиях политики регулярной смены паролей, либо в силу больших финансовых затрат на модернизацию вычислительных сетей предприятий. Поэтому построение подсистемы безопасности для распределенной АСУ ТП требует специализированных решений.

Рассмотрим, каким образом проблема идентификации пользователей решается в подсистеме безопасности Infinity SCADA при использовании ее в гетерогенной распределенной среде функци-

онирования. В Infinity SCADA информационное пространство распределенной АСУ ТП строится путем объединения адресных пространств OPC-серверов всех диспетчерских пунктов с использованием программных компонент Infinity Web Router. Компоненты Infinity Web Router объединяются в единую сеть и позволяют OPC-клиенту любого диспетчерского пункта получать доступ к данным OPC-серверов других диспетчерских пунктов распределенной системы. Компоненты Infinity Web Router также участвуют в построении распределенной подсистемы безопасности, они осуществляют передачу идентификационных данных пользователя между узлами системы. На рис. 2 представлена схема построения распределенной подсистемы безопасности Infinity SCADA.

Идентификация пользователей в удаленных узлах основана на использовании доверительных отношений между компонентами системы, которые позволяют гарантировать, что запросы на доступ к защищаемым ресурсам получены от клиентов, которые прошли аутентификацию в одном из узлов системы. Между OPC-серверами и Infinity Web Router одного узла устанавливаются односторонние доверительные отношения, между компонентами Infinity Web Router разных узлов устанавливаются двусторонние доверительные отношения. При этом доверительные отношения являются транзитивными. Компоненты Infinity Web Router вместе с запросами на доступ к защищаемым ресурсам передают контекст безопасности клиента, который однозначно идентифицирует пользователя в распределенной системе. Контекст безопасности клиента может использоваться компонентом-получателем запроса для проверки прав доступа к защищаемым ресурсам. При этом компонент-получатель может доверять информации, содержащейся в контексте безопасности, поскольку она получена от компонента, с

которым установлены доверительные отношения. В распределенной АСУ ТП процесс доступа к защищаемым ресурсам OPC-сервера узла 2 клиентом из узла 1 выглядит следующим образом:

1. Клиент узла 1 проходит аутентификацию в компоненте Infinity Web Router узла 1.

2. Клиент узла 1 передает компоненту Infinity Web Router узла 1 запрос на доступ к защищаемым ресурсам OPC-сервера узла 2.

3. Infinity Web Router узла 1 формирует контекст безопасности клиента и передает его вместе с запросом компоненту Infinity Web Router узла 2.

4. Infinity Web Router узла 2 передает запрос вместе с контекстом безопасности соответствующему OPC-серверу узла 2.

5. Используя информацию из базы данных с настройками безопасности, OPC-сервер узла 2 определяет возможность доступа клиента к защищаемому ресурсу и необходимость регистрации попытки доступа клиента к защищаемому ресурсу.

В рамках подсистемы Infinity SCADA компоненты Infinity Web Router также используются при настройке прав доступа к защищаемым ресурсам системы. Они позволяют получать список пользователей других узлов системы, с тем чтобы доступ к защищаемым ресурсам узла мог быть предоставлен пользователям других узлов.