ПОРТФЕЛЬ РЕДАКЦИИ

БИТ

В. К. Аблеков, А. А. Краснопевцев, А. А. Модестов

РАЗРАБОТКА МАСШТАБИРУЕМЫХ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время обострилась проблема обеспечения сохранности и безопасности объектов и ценностей, имеющихся на объектах [1]. Особенно важной стала проблема обеспечения безопасности средств и систем, связанных с обработкой и передачей информации, ввиду автоматизации всей информационной инфраструктуры объектов и массового подключения систем обработки и передачи информации к локальным и глобальным сетям.

Проблемы обеспечения безопасности и охраны объектов приобретают одно из важнейших значений в выборе системы безопасности. Связано это с преступностью, коммерческим и промышленным шпионажем, а также с нестабильной политической и экономической ситуацией. Все вышеперечисленные факторы требуют осуществления мероприятий по противодействию нарушителям и обеспечению безопасности на всех уровнях, из которых исходит угроза.

На сегодняшний день многие предприятия имеют множество филиалов, которые могут быть удалены друг от друга. В каждом филиале обеспечение безопасности объекта осуществляет охранная система, включающая в себя различные датчики, сервер с данными, каналы передачи информации, сотрудников безопасности. Для предотвращения вторжения нарушителя в контролируемую зону существующие охранные системы используют обычные датчики, такие как датчики движения, открытия двери, разбития окна, различные пожарные датчики, камеры и другие. Все датчики являются независимыми — каждый из них принимает решение о возможной тревоге самостоятельно, в соответствии с заложенной логикой. После принятия решения датчик отправляет свое решение на сервер, используя сработку на основании сопротивления цепи (передача 1 бита) или канал GPRS и в некоторых случаях радиоканал. Такие каналы передачи информации не защищены. Например, отдельно стоящий датчик не защищен от подмены. Нарушитель может воспользоваться данной уязвимостью и осуществить вторжение. Использование подобных датчиков влечет за собой множество ложных сработок, затрудняющих распознавание действительного нарушения. Можно говорить о том, что такие охранные системы не могут обеспечить должный уровень защиты. Поэтому остро стоит вопрос обеспечения безопасности объектов. Следует отметить, что в подобных системах затруднено проведение перемонтажа и модификации архитектуры системы, а также невозможна интеграция с другими системами защиты. В условиях современной конкуренции возникает требование в минимизации издержек при различных модификациях архитектуры системы и добавлении возможности интеграции с другими системами защиты.

В результате проведенного анализа возможных атак на целевую ИС, анализа рисков информационной безопасности и построенной модели нарушителя была разработана архитектура системы безопасности [2], которая состоит из следующих компонентов:

1. Архитектура сервера

Сервер состоит из нескольких модулей: приема данных, обработки данных, принятия решений, простых команд, управления, оповещения и архивации. Каждый из модулей может быть размещен удаленно, что добавляет гибкость в систему — доступность. Предлагаемая в работе система реализует сервис-ориентированную архитектуру (SOA) и представлена на рис. 1. Каждый из модулей может быть реализован на своем сервере или серверном кластере. Благодаря этому вся система поддается масштабированию и способна обрабатывать данные на объектах с большим числом датчиков. Модули взаимодействуют друг с другом через очереди шифрованных сообщений, это обеспечивает целостность, конфиденциальность и доступность. Введение очередей сообщений в систему позволяет производить программное обновление, модификацию архитектуры без остановки сервера, тем самым достигается непрерывная защита объекта.

2. IP-датчики

Существующие датчики безопасности были модернизированы путем добавления микроконтроллера для съема первичных данных с датчика и модуля преобразования в Ethernet для возможности передачи данных посредством сетевых протоколов TCP/IP. Для снижения стоимости датчика сняты модули, отвечающие за принятие решений. Оставлена только та часть датчика, которая отвечает за съем первичных данных. Подобная модификация не увеличивает геометрические размеры и может быть внедрена в датчик любого типа. Предполагается использование датчиков, осуществляющих многокритериальное получение первичной информации для увеличения точности определения тревоги.

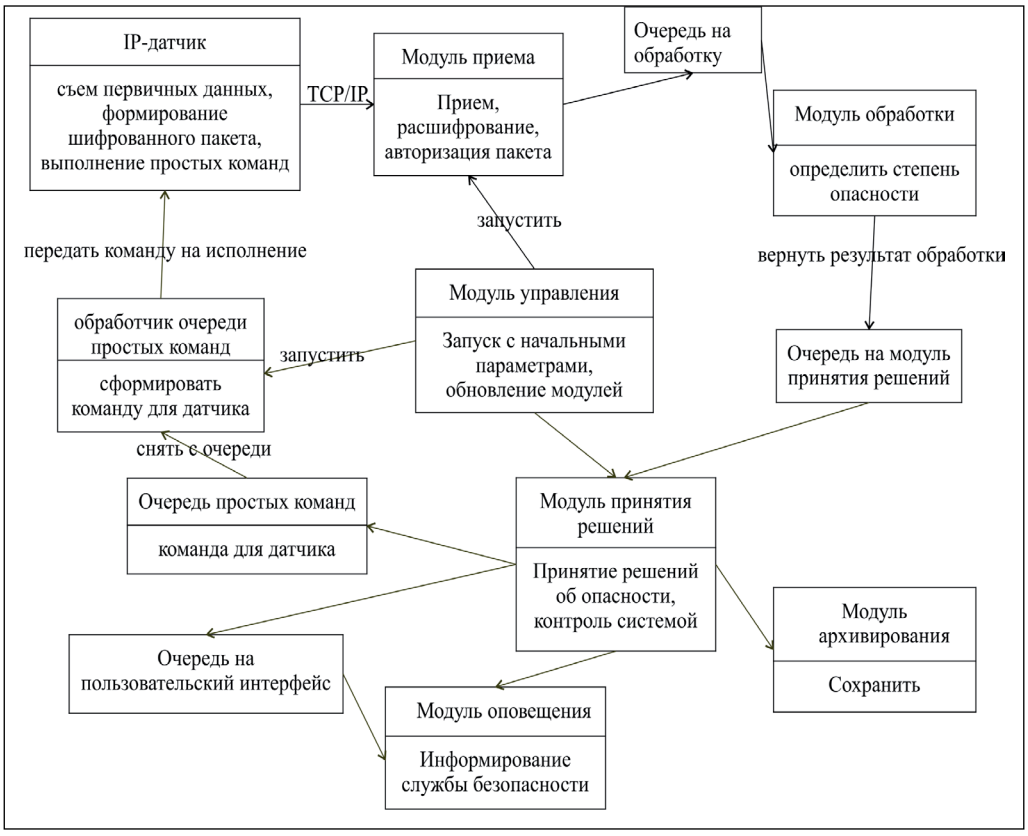

Рис. 1. Архитектура системы

3. Протокол взаимодействия датчика и сервера

Разработан протокол общения «датчик — сервер». Микроконтроллер на основании выходных значений датчика формирует пакет, добавляет идентификационные данные датчика, после чего пакет шифруется и передается на сервер посредством сетевых протоколов TCP/IP. Сервер принимает пакет, расшифровывает его, проверяет идентификатор датчика (авторизует) и начинает обработку пакета в соответствии со структурой, описанной в п. 1.

Рассмотрим основные отличительные преимущества разрабатываемой системы.

1) Обработка первичных данных, полученных с IP-датчика, на сервере позволяет:

• интегрировать датчики различного типа (пожарные, безопасности, видеокамер и т. д.) для комплексного обеспечения безопасности;

• использовать специализированные датчики и датчики с большим объемом выходных данных для повышения точности определения факта тревоги;

• иметь возможность обработки группы датчиков одного типа, взаимодействия различных типов датчиков для повышения точности определения тревоги и уменьшения процента определения «ложной тревоги», возможность конфигурирования групп датчиков и выполнения заранее заданных действий в случае сработки отдельных датчиков или групп датчиков.

2) Повышение надежности канала передачи данных за счет контроля целостности, обеспечения конфиденциальности и сохранения доступности.

3) Разработанная архитектура представляет собой набор модулей, что позволяет добиться «гибкости» реализации, то есть возможности изменения элементов системы без изменения всей системы целиком.

4) Построение единой распределенной системы обеспечения информационной безопасности, содержащей множество объектов, удаленных друг от друга. Информация о возникновении нарушения на одном из объектов будет распространена по всей системе и приняты соответствующие меры предосторожности.

В результате работы получена распределенная система, осуществляющая обеспечение информационной безопасности автоматизированных систем, способная функционировать посредством существующих сетевых каналов передачи данных. Введение протокола TCP/IP в общение «датчик — сервер» позволяет осуществлять шифрование и авторизацию передаваемых пакетов, что, в свою очередь, позволяет обеспечить защиту от таких атак, как подмена датчика. Разработанная система обладает возможностью подключения различных типов устройств и извещателей, интеграции с существующими системами защиты автоматизированных систем. Основным преимуществом является значительное повышение надежности при одинаковой стоимости внедрения в сравнении с существующими системами.

СПИСОК ЛИТЕРАТУРЫ:

1. *Белов С. В.* Автоматизированная система анализа физической защищенности объектов обработки информации. М.: МИФИ, 2005. — 169 с.

2. *Малюк А. А.* Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. М.: Горячая линия—Телеком, 2004. — 280 с.