УДК 003.26

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМЫ «УМНЫЙ ДОМ»

И.В. ИСАКОВ
(Представлено: канд. физ.-мат. наук, доц. Ю.Ф. ПАСТУХОВ)

В данной работе рассмотрим и проанализируем систему «Умный дом», её информационную безопасность.

Концепция умного дома включает в себя объединение различных современных технологий и решений, способных обеспечить комфорт и удобство получения услуг, безопасность граждан, рациональное потребление ресурсов. Вместе с тем из поля зрения приверженцев концепции умного дома часто выпадает безопасность самих элементов умного дома. Зачастую инфраструктура системы «умный дом» развивается намного быстрее, чем средства ее защиты, что вызывает живой интерес и оставляет большой простор для деятельности как исследователей, так и злоумышленников. Исходя из основной концепции системы умный дом, практики ее применения, а также необходимого и должного уровня безопасности и защищенности, как всей системы, так и ее компонентов антивирусное средство «умного дома» должно обеспечивать выполнение следующих важных функций:

– контроль появления на сервере умного дома любых посторонних файлов или программ;

– контроль несанкционированных подключений устройств к сети;

– контроль подключения устройств к беспроводным каналам передачи данных;

– контроль трафика между локальными сетями интеллектуального здания и непосредственно сервером автоматизированного управления;

– контроль взаимодействия сервера с сетью Интернет на предмет проникновения вирусного программного обеспечения;

– контроль сетевого оборудования на предмет DoS-атак;

– обеспечение проверки файлов, передаваемых в проводных и беспроводных сетях;

– выполнение эвристического поиска и наличия на сервере вирусных программ;

– контроль целостности системы умного дома, которая должна заключаться в проверке текущей конфигурации, управляющих процессов и хранимых данных.

На основе проведенного анализа существующих программных антивирусных средств можно сделать выводы, что создание антивирусной системы, способной обеспечивать комплексную защиту системы автоматизированного управления зданием является актуальной и важной задачей в краткосрочный период.

Решить данную задачу возможно с помощью целостного и системного похода используя средства анализа контента и системы обнаружения атак. Средства анализа контента предназначены для контроля сетевого трафика с целью выявления нарушений политики безопасности. В настоящее время можно выделить два основных вида средств контентного анализа - системы аудита почтовых сообщений и системы мониторинга Интернет-трафика. Системы аудита почтовых сообщений предполагают сбор информации о SMTP-сообщениях, циркулирующих в АС, и её последующий анализ с целью выявления несанкционированных почтовых сообщений, нарушающих требования безопасности, заданные администратором. Так, например, системы этого типа позволяют выявлять и блокировать возможные каналы утечки конфиденциальной информации через почтовую систему. Системы мониторинга Интернет-трафика предназначены для контроля доступа пользователей к ресурсам сети Интернет. Средства защиты данного типа позволяют заблокировать доступ пользователей к запрещённым Интернет-ресурсам, а также выявить попытку передачи конфиденциальной информации по протоколу HTTP. Системы мониторинга устанавливаются таким образом, чтобы через них проходил весь сетевой трафик, передаваемый в сеть Интернет.

Системы обнаружения атак представляют собой специализированные программные или программно-аппаратные комплексы, предназначенные для выявления информационных атак на ресурсы системы посредством сбора и анализа данных о событиях, регистрируемых в системе. Система обнаружения атак включает в себя следующие компоненты:

– модули-датчики, предназначенные для сбора необходимой информации о функционировании системы. Иногда датчики также называют сенсорами;

– модуль выявления атак, выполняющий анализ данных, собранных датчиками, с целью обнаружения информационных атак;

– модуль реагирования на обнаруженные атаки;

– модуль хранения данных, в котором содержится вся конфигурационная информация, а также результаты работы средств обнаружения атак;

– модуль управления компонентами средств обнаружения атак.

Для решения проблемы обеспечения информационной безопасности «Умного дома» необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации.

ЛИТЕРАТУРА

1. Кусакин, И.И. Программно-аппаратный комплекс автоматизированного контроля целостности инфраструктуры жилых помещений для социального обеспечения. XV Международная телекоммуникационная конференция молодых ученых и студентов «МОЛОДЕЖЬ И НАУКА». Тезисы докладов. В 3-х частях. Ч. 3 – М.: НИЯУ МИФИ, 2012. – С. 156 – 157.