

УДК 004.75

**ИССЛЕДОВАНИЕ МЕТОДИК ЗАЩИТЫ СИСТЕМ «УМНЫЙ ДОМ»
НА БАЗЕ АРХИТЕКТУРЫ ПРОГРАММНО-ОПРЕДЕЛЯЕМОЙ СЕТИ**

Богомолов Д.М. (Университет ИТМО)

Научный руководитель – к.т.н., доцент, Донецкая Ю.В. (Университет ИТМО)

Проведен анализ методики защиты систем «умный дом», приведены причины выбора архитектуры программно-определяемой сети для разработки методики защиты информации. Работа содержит описание защищенной системы «умный дом», которая обеспечивает повышенную степень безопасности данных.

Введение. На сегодняшний день ключевой задачей в развитии и использовании технологий интернета вещей является интегрирование всех несвязанных технологий в одну доверенную сеть, которая позволит большому объему информации и сервисов безопасно и эффективно взаимодействовать как в концепции устройство-устройство, так и в концепции устройство-человек. В работе предлагается методика проектирования систем «умный дом» с целью повышения защищенности подобных систем, которая подразумевает возможность масштабирования предлагаемой концепции для «умных домов» различной конфигурации устройств.

Основная часть. Концепция программно-определяемой сети проста и её достоинство состоит в том, что данная архитектура предлагает не просто создавать централизованный узел в сети, но и управлять всей плоскостью передачи данных из одного центра, именуемый контроллером, на базе уже реализованных протоколов. Использование подобной архитектуры позволяет вынести контрольную плоскость сети на программно-аппаратную базу, избегая разделение её на процессы. Таким образом, контроллер определяет конечное место назначения пакетов, что позволяет встроить в подобную архитектуру эффективную систему защиты информации.

Когда пользователь системы посылает запрос к системе, формируется контейнер, который передается через интернет или по сетевому каналу, где возможно наличие различного рода атак. Для подтверждения подлинности запроса между устройствами умного дома и интернетом устанавливается сервер-контроллер, на котором запущена программа фильтрации запросов. В начале вход системы поступает поток данных и после передачи на уровень контроля, обслуживаемый сервер-контроллером, он будет проверен на новизну для системы. При обнаружении известной атаки система входит в режим повышенной защиты и не позволяет пропускать скомпрометированный поток информации. Если поток оказывается новым и неизвестным то, система пропускает его через анализатор. Затем все данные о проанализированных запросах или атаках будут сохранены, после чего система обновит правила, в случае обнаружения новых атак. А так, как в системах умный дом запросы пользователя и устройств между собой будут однотипны, такая система не будет существенно замедлять нормальную работу устройств «умного дома».

Выводы. В работе рассмотрена методика, позволяющая увеличить защищенность системы от внешних атак, а реализация системы может быть применена на системах типа «умный дом» любого масштаба без потери скорости работы.

Богомолов Д.М. (автор)

Донецкая Ю.В. (научный руководитель)