Блок контроля от несанкционированного доступа — защита копирования электронных ключей

НТ ЗАО «Аларм» заканчивает опытную эксплуатацию нового элемента систем охранной сигнализации — Блока контроля от несанкционированного доступа (БК НСД). О новом устройстве мы беседовали с зам. главного конструктора НТ ЗАО «Аларм» Дмитрием Шелюто.

Справка ТБ: *Компания Dallas Sem. (Dallas Semiconductor) занимается разработкой, производством и сбытом интегральных микросхем и законченных микромодулей на их основе. Dallas Semiconductor поставляет свою продукцию изготовителям комплексного оборудования в области контрольно-измерительной аппаратуры, систем автоматизации производственных процессов, персональных ЭВМ, систем связи, медицинской техники, торгового оборудования, систем автоматической идентификации, а также больших ЭВМ.*

В настоящее время Dallas Semiconductor является ведущим поставщиком энергонезависимой памяти, микросхем часов реального времени, приборов автоматической идентификации в миниатюрном металлическом корпусе (iButton). Энергонезависимая память является ключевым элементом большинства выпускаемых компанией электронных компонентов.

Для чего была произведена разработка нового устройства?

Работы по разработке былипроведены в соответствии с требованиями Департамента Охраны МВД. Задача БК НСД — защита от подделки имеющихся ключей доступа. На сегодняшний день в 90% объектов сданных под охрану используют ключи доступа типа Dallas (DS1990A). Эти ключи легко дублируются, многие сами имеют дубликаторы, т.е. за короткое время ключ можно «считать» и прибор совершенно корректно снимается с охраны. Поэтому Департамент охраны вынужден принимать меры организационного характера, которые, к сожалению, из-за халатности «хозоргана» не всегда срабатывают.

Мы предлагаем использовать другой ключ доступа с совершенно иным уровнем защиты. На рынке существует серия ключей Touch Memory (Dallas Sem.) DS1961S, которые имеют кроме классической открытой части, еще закрытую область.

В эти ключи встроен алгоритм шифрования стандарта SHA-1 (Secure Hash Algorithm http://www.gaw.ru/pdf/Dallas_Sem/ibutton/app/app157ru.pdf, http://www.digital-evolution.ru/content/6-ibutton-info). Этот алгоритм был рекомендован в качестве основного для государственных учреждений в США (до 2011 г., в настоящий момент используется как цифровая подпись). Данный алгоритм при его серьезном уровне защиты находится в свободном распространении, т.е. за его использование не надо платить.

На каком количестве приборов планируется применение БК НСД?

Парк приборов в Беларуси достаточно большой. Приборы уже стоят в банках, пунктах обмена валюты, квартирах, ларьках. Необходимо было сделать какое-то небольшое устройство с отдельными защищенными ключами, исключающими дублирование. Устройство само небольшое, ставится либо в сам прибор, либо рядом, имеет собственную защиту и к нему подключается наружное устройство доступа (УД).

Какие основные принципы работы устройства и его особенности?

БК НСД считывает ключи доступа, прикладываемые к внешнему устройству доступа, определяет их тип («незащищенные» — DS1990A и 100% аналоги, либо «защищенные»-DS1961S) и, в зависимости от параметров настройки и программирования изделия, выполняет следующие функции:

– определяет тип ключа, установленного в УД (DS1990A, либо DS1961S);

– обрабатывает данные с защищенного ключа DS1961S по алгоритму SHA-1, перекодирует в формат данных ключа DS1990A и транслирует их в прибор, если данный ключ содержится в памяти БК НСД;

– формирует и отправляет в прибор признак «чужого» ключа при установке незапрограммированного в БК НСД ключа DS1961S;

– транслирует (режим работы 1) коды ключей DS1990A в прибор, если в БК НСД установлен признак «не контролировать», и код ключа DS1990A не совпадает с «открытой» частью кодов ключей DS1961S, записанных в БК НСД, либо формирует и отправляет в прибор признак «чужого» ключа, если открытый код ключа DS1990A совпадает с каким либо кодом ключа DS1961S, хранящегося в памяти БК НСД ;

– транслирует коды ключей (режим работы 2) DS1990A в прибор, если в БК НСД установлен признак «контролировать», и код ключа DS1990A совпадает с кодом, записанным в БК НСД, либо формирует и отправляет в прибор признак «чужого» ключа, если данный код не занесен в память БК НСД;

– формирует и отправляет в прибор признак «чужого» ключа, если установленный ключ «нулевой» (т.е. в код ключа содержит одни нули);

Ключ может быть привязан только к конкретному изделию БК НСД. Человек, получив ключ в руки, не может его скопировать.

В настоящий момент изделия проходят эксплуатацию, и в середине августа планируется установка БК НСД на реальные объекты..

Какие еще есть варианты защиты объекта ?

Для повышения защищенности объекта можно дополнительно применять клавиатуру МДВ-7К. Во всех приборах есть программируемая функция «подтверждение снятия», т.е после снятия объекта ключом, в течение определенного времени необходимо нажать скрытую кнопку. Сейчас вместо кнопки рекомендуется ставить клавиатуру, чтобы можно было набрать дополнительный код и защититься как от потери ключа, так и от снятия «под принуждением». Клавиатура может работать в двух режимах: как устройство доступа (вместо ключа набирается код и сохраняется при программировании в памяти прибора;далее, при наборе кода, он транслируется в прибор и воспринимается как ключ DS1990A.) Код может содержать от 1 до 12 цифр. Второй режим — в качестве кнопки снятия. В этом случае коды сохраняются в самой клавиатуре. При наборе данного кода формируется сигнал на подтверждение снятия прибора с охраны. Также есть код, так называемый «паника»: при наборе правильного кода и лишней цифры, она реагируют корректно, а на самом деле на

МДВ-7К

БК НСД

пульт поступает сигнал экстренного вызова. Такая комбинация ключ плюс клавиатура достаточно надежна.

Как будет осуществляться модернизация существующих охранных систем, какова сложность установки?

У нас возникли сложности на этапе эксплуатации с точки зрения программирования изделия, т.к. мы реализовали программирование с пульта ввода. Были моменты, которые сейчас упростили, устранили при программировании. Модернизация устройствами БК НСД и МДВ-7К охранных приборов мы реализовали вначале только под наши приборы (пр-ва «Аларм»), а стояла задача совместимости со всеми приборами. При решении проблемы у нас возникли вопросы по совместимости изделий с приборами и пультами различных производителей. Приборы похожи, но алгоритмы считывания ключей немного разные, даже считывание ключа происходит по-разному. Например, в свое время мы дорабатывали наши приборы, для возможности относить считыватели на 300 метров от приборов, мы очень жестко выдержали этот протокол и когда мы попытались работать с другими приборами в другом формате, они этого не «понимают». Пришлось немного «ухудшить» параметры, чтобы любые пульты и приборы других производителей могли иметь возможность работы с изделиями БК НСД и МДВ-7/К.

На сегодняшний день с какими приборами работает БК НСД?

Практически со всеми установленными на объектах приборами: ПКП -4М, А-606, Агат21, (т.е. приборами производства компаний Ровалэнт, Новатех, Агат-систем).

Беседовал Сергей ДРАГУН

НТ ЗАО «Аларм»
220141, г. Минск, ул.Ф.Скорины 51, литер Ж, к.308а
Тел./факс: (017) 285-93-59; 285-94-01, 640-14-22, 265-94-47
E-mail: alarm@alarm.by

УНП: 100435764