Несанкционированное вмешательство в работу приборов учета

Дмитрий Анисимов,
главный специалист
ООО «Диамер»,
автор сайта «Теплопункт»

Несанкционированное вмешательство в работу приборов учета – одна из основных проблем в сфере учета потребляемых ресурсов. Кто виноват в возникновении этой проблемы, и что необходимо сделать для ее решения?

Десять лет назад и позже мы неоднократно писали о несанкционированном вмешательстве в работу приборов учета, искажении показаний расходомеров и «взломе» тепловычислителей. Тогда эта тема уже использовалась кем-то для «наезда» на конкурентов, но далеко не в тех масштабах, в каких это произошло нынче. И вот мы снова пишем о несанкционированном вмешательстве. Но можем ли мы добавить что-либо новое к тому, что было уже когда-то рассказано?

Немного истории (ибо это – уже история). Весной 2013 г. группа российских производителей приборов учета неожиданно провела «испытания» ряда приборов, в ходе которых «выяснилось», что некоторые из этих приборов можно «взломать». То есть при помощи неких инструментов (среди них назывались изогнутая проволока и таинственная «флэшка» с не менее таинственным программным обеспечением) можно незаметно изменить метрологические характеристики. Но почему слова «испытания» и «выяснилось» мы берем здесь в кавычки?

Вообще-то мы всеми руками за подобные мероприятия, доказательством чему – наша статья 2005 г., в которой было написано следующее: «...Мы же – специалисты по приборному учету – можем сделать кое-что и, как говорится, на общественных началах. Это "кое-что" можно назвать "диверсионным анализом теплосчетчиков". Суть его состоит в том, что берется теплосчетчик конкретного типа, и далее с пристрастием изучается его документация, его устройство и его конструкция... Задача проверяющего – "устроить диверсию", найти лазейки, случайно или вполне преднамеренно оставленные производителем для "фальсификаторов". Для того чтобы результаты анализа различных приборов разными людьми были объективны и сопоставимы, необходима некая универсальная методика...

Так вот, мы предлагаем специалистам в области теплоучета заняться диверсионным анализом теплосчетчиков различных типов... И не нужно воспринимать диверсионный анализ как диверсию против производителей приборов. Напротив, предлагаемый проект поможет "на общественных началах" решить общую проблему достоверности учета, другими словами – снять сомнения в достоверности учета при использовании тех или иных приборов. Одновременно будут решаться и некоторые частные проблемы:

- будут обнаруживаться и устраняться случайные "проколы" разработчиков приборов по части их "безопасности";
- станут бессмысленными те распространяемые через интернет анонимки, от которых уже пострадал кое-кто из производителей;
- станут очевидны и будут обоснованы предпочтения потребителей по части устройства и конструкции теплосчетчиков».

Главное – методика

Итак, испытания нужны, их стоит всецело приветствовать. Но главное при их проведении – это методика. А какая методика легла в основу весенних испытаний в 2013 г.? Почему в одни приборы вставляли инструмент под названием «изогнутая проволока», а в другие не стали? Откуда для приборов одного типа появился «ключ авторизации» («флэшка»), внешне похожий на ключ для сервисных центров? Кто его изготовил? И как можно быть уверенным в том, что подобного ключа не существует для приборов других типов?

Так, может, это были вовсе не «испытания на защищенность от несанкционированного доступа» приборов разных производителей, а проверка поступившей из неких источников информации о конкретных способах вмешательства в работу приборов конкретного типа? Другими словами, кто-то сообщил, кто-то продемонстрировал. Дело, безусловно, тоже важное и полезное – но зачем преподносить его как некие сравнительные испытания, в результате которых что-то вдруг выяснилось?

Отсюда и кавычки: в данном конкретном случае никаких испытаний не было. Была публичная демонстрация заранее известной (и, вероятно, заранее проверенной) информации о возможности фальсификации показаний определенных приборов учета путем изменения их метрологических характеристик без нарушения пломб. «Испытатели» действовали по заранее изученной (и, вероятно, опробованной) инструкции, используя заранее подготовленные (и, вероятно, опробованные) инструменты. А для чего они это делали? Очевидно, лишь для того, чтобы опорочить

и, если повезет, на какое-то время вывести из игры конкурента. Ведь если бы «в доме был порядок», и испытания были бы настоящими, то в их результате, во-первых, производитель поблагодарил бы коллег и взялся устранять обнаруженные конструктивные недостатки приборов, а во-вторых, коллеги занялись бы поиском тех, кто изготавливает специнструменты и занимается взломом существующих приборов (имеющих те самые конструктивные недостатки). А то, как был сформулирован протокол весенних испытаний, как он был преподнесен, как на него отреагировали стороны, – все это свидетельствует о том, что имел место некий заказ, который хоть и неуклюже, но старательно отрабатывался.

Но уйдем от дрязг реальной жизни в сугубо теоретические сферы. Итак, имеется некий прибор учета. Некоторые его настройки, определяющие метрологические характеристики, можно менять. Это объективная необходимость, обеспечивающая возможность эксплуатировать прибор долго и эффективно. Время от времени он проходит поверку, и если выясняется, что его характеристики в силу естественных причин (таковых много, но можно условно объединить их понятием «старение») непозволительно изменились, то прибор калибруют. То есть меняют те самые настройки, а изменения фиксируют в документации, заверяя подписями и печатями.

Однако ясно: то, что можно изменить «легально», можно изменить и «преступным путем». Зачем – тоже понятно: установлен прибор, который выдает честные показания; тайно меняем настройки, и показания смещаются в нашу пользу. Чтобы защититься от этого, можно (нужно) скрыть «органы управления» прибора под пломбируемыми крышками, программную часть защитить паролем, все изменения настроек фиксировать в отдельном нестираемом архиве – и т.д., и т.п. Все производители говорят о том, что вот тут у них пломбы, там – пароли, а здесь – фискальные архивы. Но... на каждый сейф найдется свой взломщик. А если можно вскрыть сверхнадежный сейф или, скажем, взломать сверхзащищенный сервер, то почему нельзя сделать то же самое с механическими и программными защитами прибора учета?

Другой вопрос, стоит ли овчинка выделки, то есть окупятся ли трудозатраты? Ведь если найти в корпусе прибора щель, в которую можно засунуть проволочку, которой нажать на кнопку, скрытую под пломбой (что дешево и доступно практически каждому желающему), то работа по вторжению в программную часть требует большого времени и высокой квалификации. Вот почему с изрядной долей уверенности можно сказать: если «немеханическое» несанкционированное вмешательство в работу прибора учета возможно, то, во-первых, эту возможность случайно или осознанно заложил сам производитель, а во-вторых, организацией вмешательства занимались (разрабатывали методики, изготавливали инструмент) люди, досконально (читай: на уровне разработчика) знающие прибор.

Да, у производителя может быть множество резонов предусмотреть в своих приборах «тайные входы». Мы уже писали об этом в одной из своих статей в 2003 г. (на примере тепловычислителей):

«А корни таких фальсификаций известны. Давайте обратимся к истории, точнее, к тому ее периоду, когда учет стал “входить в моду”, и в стране появилась масса небольших, но очень амбициозных фирм, разрабатывающих и выпускающих тепловычислители... Изначально та маленькая фирма, которая взялась делать вычислители, не имеет никаких злых помыслов и декларирует “честность” своих приборов. И первые из этих приборов не имеют никакого “хитрого” интерфейса и не позволяют над собою никаких фальсификаций. Но производитель на начальной стадии мал, слаб и неопытен: то программист ошибку в программе допустит, то схемотехник не тот транзистор применит, то радиомонтажник “соплю” на плате посадит, то компоненты закупят по дешевке, но сомнительного качества... А времени на эмуляцию всех ветвей программы и длительные ресурсные испытания, понятное дело, нет – вот и всплывают все оплошности уже в процессе коммерческой эксплуатации проданных приборов.

Разумеется, такие сбои, отказы и провал учета могут поставить крест на репутации и дальнейшем развитии фирмы. Однако пока вычислителей выпущено и выпускается немного, и все они находятся в поле зрения производителя, возникает соблазн – излечивая “детские болезни” приборов, стирать из их памяти признаки этих “болезней”. Другими словами, позвонил

мне потребитель и сказал, что вычислитель "умер" и вот уже дня три, как ничего не считает. Я приезжаю, ремонтирую прибор, а в его память вписываю архивы, будто бы он и не "умирал" вовсе. Потребитель меня не выдаст – не в его интересах. Я же извлекаю урок из случившегося и говорю своему программисту: слушай, Василий, а давайка переделаем "софт" нашего прибора так, чтобы я мог с ноутбука или вообще с клавиш, введя определенный пароль, "восстанавливать" архивы, менять данные – и т.д., и т.п., и чтобы прибор такого несанкционированного доступа никак не фиксировал.

Так и появляется программное обеспечение со "скрытыми входами", и входы эти реально спасают производителя, помогают ему раскрутиться на рынке, маскируя неизбежные ошибки и экономя время на испытания приборов, которые проходят непосредственно в "боевых условиях". А вот после – два варианта развития. Если производитель раскрутился, в душе оставшись честным, он уберет из ПО своих приборов все эти тайные входы и постарается забыть о том, что творил в начале своего пути, как о страшном сне. И общество должно его простить: это, знаете, что-то типа "налоговой амнистии", когда помнят, что "все большие капиталы в мире нажиты нечестным путем", но понимают, что дальше-то жить надо и желательно – честно, а значит, должна быть какая-то "точка легализации". Другой вариант – производитель раскрутился, но честным стать не захотел, так как обманом жить всегда проще».

Кто виноват, и что делать?

Однако, как ни парадоксально это звучит, даже если производитель сознательно оставил (сделал) в своих приборах «закладки» или «входы» для тайного вмешательства в их работу, он не преступник до тех пор, пока этими входами не воспользовался. Другими словами, судят не того, кто оставил дверь открытой, а того, кто из-за этой двери что-то украл. Исключение – случай, когда дверь была оставлена открытой по предварительному сговору. А уж если дверь была заперта, то все еще яснее: изготовитель замка не виновен в том, что к замку оказалось возможным подобрать отмычку. Однако если это ответственный производитель, заботящийся о своих клиентах (и о своей репутации, что в данном случае одно и то же), то он будет анализировать все случаи взломов своей продукции и принимать соответствующие меры.

Кроме того, меры может принять и потребитель. Например, повесить на дверь дополнительный замок. Или, в случае с приборами, дополнительно их опломбировать, надежно закрыть все неиспользуемые разъемы, ограничить доступ в узел учета и т.д. Если же потребитель, узнав каким-то образом о возможностях тайного доступа в приборы определенной марки специально приобретает именно их, то... кого от кого мы защищаем, когда говорим о том, что эти приборы можно «взломать» при помощи скрепки или какого-то более изощренного инструмента?

Итак, ничего нового. Популярная в этом сезоне тема о несанкционированном вмешательстве в работу (некоторых) приборов учета раскладывается на следующие вопросы, которые не раз уже задавались, и ответы, которые столько же раз звучали:

- возможно ли такое вмешательство в принципе? – Да, несомненно;
- кто виноват в возможности такого вмешательства? – Очевидно, что вмешательство возможно только тогда, когда разработчик/производитель либо не предусмотрел защиту от него, либо, наоборот, специально предусмотрел возможность вмешательства. Но даже предусмотреть возможность вмешательства – не значит иметь преступные намерения, ибо причины и цели тут могут быть разные. Вот почему правильней говорить не о вине, и уж тем более не о вине в юридическом смысле, а об этике, уровне профессионализма, инженерной культуре и других подобных материях;
- кто виноват в конкретных случаях вмешательства? – Тут ответ совершенно однозначный: кто вмешался (кто пойман), тот и виноват. Причем вот здесь уже – именно юридически;
- что делать, чтобы не допустить вмешательства в работу приборов учета? – Если в этом заинтересован производитель, он должен совершенствовать приборы и способы их защиты. Если речь идет об интересах потребителя (а потребители приборов – это обе стороны рынка учета энергоресурсов, то есть и ЭСО, и их абоненты), то ограничивать доступ в узлы учета (двери,

сигнализация, ключи под роспись), пломбировать все «открываемые» элементы конструкции приборов, блокировать каким-либо способом доступ к диагностическим, технологическим и другим не используемым в «повседневной учетной работе» разъемам и переключателям.

Очевидно, что принятие этих совсем несложных мер может защитить даже тот прибор, который изначально вообще никак не был защищен производителем, и даже тот, в котором производитель осознанно предусмотрел «тайные входы». А раз так, то вопросы о несанкционированном вмешательстве... теряют свою актуальность? Для добросовестного потребителя – да, но в целом картина несколько сложнее.

Проблема решаема

Когда-то (в 2010 г.) мы писали:

«...В сфере теплоучета видим четыре стороны, каждая со своими интересами. Это поставщик тепла, который заинтересован получить за тепло больше, и потребитель тепла, который желает заплатить за тепло меньше. Это производитель приборов учета (или его представитель, дилер), задача которого – убедить и поставщика, и потребителя покупать именно его продукцию, а не продукцию конкурентов. И, наконец, государство, которое контролирует качество производимых приборов учета и вынуждает поставщиков и потребителей тепла применять для учета не любые «изделия», а только сертифицированные средства измерений. Можно было бы упомянуть здесь и монтажные фирмы, но они, хотя часто и бывают самостоятельны, в каждом конкретном проекте все же выражают интересы либо поставщика тепла, либо потребителя (монтируют и/или обслуживают теплосчетчики для того или другого), либо производителя приборов (продвигают его продукцию)... Очевидно, что для соблюдения баланса интересов поставщиков и потребителей тепла необходимо применять как можно более технически совершенные приборы учета».

Если придерживаться этой схемы, то поставщики и потребители энергоресурсов сами в состоянии принять меры по защите своих приборов, даже если эти приборы не защищены изначально, конструктивно, «идеологически». Но они не могут защитить «чужие», то есть не могут ничего поделать, если со своими приборами «мухлюет» другая сторона. А та, опять же, может «мухлевать» и с приборами, которые производитель искренне считает защищенными. Производителя приборов данная тема волнует только тогда, когда он узнает, что конкурент получает преимущество за счет «нечестной игры».

За честность и равновесие должно отвечать государство: при сертификации приборов учета вопросы их защиты от несанкционированного доступа должны стоять сразу после вопросов метрологии. Но нам следует признать, что если производитель пожелает сделать «закладки» или «тайные входы», обеспечивающие несанкционированное изменение характеристик своих приборов, то он это сделает, и найти их (как при сертификации, так и при любых других испытаниях), не зная о них заранее, будет крайне сложно. А уж доказать злой умысел производителя – вообще практически невозможно. Зато возможно вскрывать конкретные случаи несанкционированного вмешательства, фальсификаций – и наказывать виновных, чтобы ни у кого более не было соблазна заниматься этим. Это тоже задача государства, но не метрологической службы, а правоохранительных органов. Помогать им, разумеется, может и должна общественность.

Таким образом, защита приборов учета от несанкционированного доступа наиболее эффективно обеспечивается не на уровне приборов, не на уровне производителей и не на уровне метрологической службы. Это – вопрос правопорядка. Конечно, важную роль могут играть испытания на предмет «взлома» по единым для всех методикам (см. выше о диверсионном анализе) и информирование всех заинтересованных сторон об их результатах. Но очевидно, что проводиться такие испытания должны независимыми лабораториями. Если же (вернемся к началу данной статьи) испытания проводит конкурент, и они больше напоминают заранее отрепетированную демонстрацию, а результаты преподносятся под лозунгом «держи вора»... нет, извините, это не забота об общем благе, а всего лишь пиар-акция, затеянная ради собственной выгоды.

Итак, проблема есть, но ее преподносят в неверном ключе. И проблема решаема, но не органами метрологии, а силами правопорядка. ❐