Tamper Detection for Safeguards and Treaty Monitoring: Fantasies, Realities and Potentials
Roger G. Johnston
Non-Proliferation Review/ Spring 2001

Устройства индикации вмешательства и их применение для учета и контроля ядерных материалов: фантазии, реальность и возможности

Роджер Дж. Джонстон

Обнаружение несанкционированного вмешательства играет важную роль как в отечественных, так и в международных программах защиты, контроля и нераспространения ядерных материалов. К сожалению, представления о нем зачастую основаны на неправильном понимании данного определения, нечетко поставленных задачах и попытках выдать желаемое за действительное. Существующие программы защиты от несанкционированного вмешательства страдают как от указанных недостатков, так и от нехватки квалифицированного персонала, ограниченности анализа, нечеткости (или отсутствия) нормативов, идеализации возможностей оборудования и преувеличения его универсальности, а также их очевидной уязвимости. Для успешного применения устройств индикации вмешательства как в настоящее время, так и в дальнейшем требуется совершенствование и детализация подхода, модернизация оборудования и уяснение принципов его функционирования.

В данной работе рассматриваются устройства индикации вмешательства, в частности, пломбы и маркировки, а также затрагивается вопрос об ошибочном представлении, касающемся эффективности этих устройств со стороны ряда специалистов по учету ядерных материалов. Далее излагаются общие проблемы, которые возникают при применении пломб и других устройств индикации вмешательства в Соединенных Штатах и других странах, а затем более детально рассматриваются программы учета и контроля ядерных материалов (УК ЯМ) в США и России, а также программы маркировки и установки пломб Международного агентства атомной энергии (МАГАТЭ). В заключительной части работы описываются новые возможности в части применения устройств индикации вмешательства как на территории США, так и в рамках международных программ контроля соглашений и нераспространения ядерных материалов. В данной работе представлен более реалистичный подход к оценке возможностей и слабых сторон устройств индикации вмешательства.

МЕРЫ ПО ИНДИКАЦИИ ВМЕШАТЕЛЬСТВА

Обнаружение несанкционированного вмешательства, как правило, подразумевает применение маркировок и/или пломб. Маркировка используется для обозначения характерных признаков и идентификации объекта или контейнера. Типичными примерами маркировки в повседневной жизни являются номерные знаки автомобилей и голографические изображения, наносимые на кредитные карточки. Пломбы представляют собой устройства индикации вмешательства, предназначенные для обнаружения несанкционированного доступа к дверям, контейнерам или упаковкам изделий. Типичными примерами пломб являются запечатанные упаковки лекарств, отпускающихся в аптеках без рецепта, а также недорогие пластиковые или проволочные пломбы, которыми опечатываются домашние или промышленные счетчики в США для предотвращения хищений.

В настоящее время имеются тысячи различных типов пломб, в том числе устройства активного и пассивного типов. Пассивные пломбы представляют собой невосстановимые механические конструкции,

тонкую фольгу или пленку, липкие ярлыки, проволоку или провод, оптическое волокно и другие материалы и приспособления, которые повреждаются или изменяются в случае разрыва или другого воздействия. В настоящее время существует также два вида активных пломб: электронные и оптоволоконные. С помощью электронных пломб осуществляется непрерывный контроль изменений, происходящих в результате вмешательства. Активные оптоволоконные пломбы периодически или произвольно посылают световые импульсы по оптоволоконному пучку (или одному волокну) для проверки непрерывности линии.

Важно помнить, что пломбы, в отличие от замков, не предназначены для защиты от несанкционированного вмешательства или доступа. Они предназначены лишь для фиксации факта такого доступа. Некоторые пломбы выполнены из легко рвущейся бумаги или пластика; однако это не делает их менее эффективными для обнаружения вмешательства. Другой вопрос, иногда приводящий к смешению понятий, касается частичной взаимозаменяемости маркировок и пломб. Надежная пломба должна иметь признаки, свойственные маркировке, и наоборот. Как следствие, устройство, используемое главным образом как пломба, может также выполнять функцию маркировки, в то время как маркировка может служить для обнаружения вмешательства.

Одним из важных моментов обнаружения вмешательства является вопрос о том, существует ли вероятность фальсификации пломбы или печати и, если существует, то насколько велика эта вероятность. Под фальсификацией пломбы имеется в виду её подделка. Несмотря на наличие других видов вмешательства, как правило, фальсификация пломбы подразумевает ее вскрытие, а затем восстановление *без внешних признаков вскрытия*, с использованием либо оригинальной, либо поддельной пломбы. Если используется оригинальная пломба, она может быть вскрыта без повреждений или признаков взлома, либо повреждения/признаки взлома могут быть уничтожены или скрыты. Аналогичным образом нарушение маркировки подразумевает либо подделку маркировки без обнаружения, либо снятие маркировки и ее нанесение на другой объект или контейнер, также без обнаружения. "Вмешательство" означает серию действий, направленных на нарушение пломбы или маркировки.

Любая пломба или маркировка потенциально подвержена сотням возможных типов вмешательства. В случае нарушения пломб, возможные виды вмешательства могут быть сгруппированы следующим образом:

- Вмешательство в конструкцию пломбы еще до ее использования с целью определения способа ее несанкционированного вскрытия;
- Вскрытие, а затем закрытие пломбы без ее повреждения или признаков вскрытия;
- Восстановление пломбы или скрытие повреждений после вскрытия пломбы;
- Скрытие или уничтожение признаков доступа после вскрытия пломбы;
- Замена пломбы (или ее частей) на поддельную или дубликат;
- Изменение даты, указанной на пломбе;
- Вмешательство в процедуры установки, контроля и проверки пломбы;
- Фальсификация пломбы и взлом непосредственно контейнера или замка;
- Ложная тревога и дискредитация;
- "Психологическая атака": подкуп или запугивание;
- Комбинированные или альтернативные методы.

Кроме пломб и маркировок, обнаружение вмешательства может предполагать использование датчиков вторжения, портальных мониторов, информационных барьеров и видеонаблюдения. Датчики вторжения (по сути, охранная сигнализация) часто используются в сочетании с пломбами; их отличие заключается в том, что они сигнализируют о вмешательстве в реальном времени, а не позднее, в момент проверки. Такие датчики дают преимущество более быстрого реагирования сил охраны на вторжение. Их типичными недостатками по сравнению с пломбами является большое количество ложных тревог, высокая стоимость, необходимость использования электропитания и дополнительная уязвимость,

связанная с необходимостью отправки сигнала на удаленный пульт и его расшифровки. Портальные мониторы (такие, как датчики радиоактивного излучения и металлоискатели) используются для контроля доступа (входов и выходов) через двери, коридоры и подъездные пути, а также способствуют сохранению защитных барьеров. Информационные барьеры представляют собой аппаратные или программные средства, предназначенные для блокировки или фильтрации некоторых видов информации. Они рассматриваются в качестве способа предупреждения доступа к секретной информации радиационных датчиков, в то же время предоставляя необходимые данные инспекторам по ядерной безопасности. Для снижения риска вмешательства и уменьшения потребности в персонале, обеспечивающем охрану безопасности и контроль, как правило, используются видеокамеры наблюдения. В то время как датчики, контрольные устройства, информационные барьеры и видеокамеры применяются вместо маркировок и пломб, они сами также нуждаются в защите от несанкционированного вмешательства. Это можно обеспечить при помощи дополнительных маркировок и пломб.

ЗАБЛУЖДЕНИЯ, КАСАЮЩИЕСЯ МАРКИРОВОК И ПЛОМБ

Многие аналитики высказывают реалистичные предположения по поводу недостатков и погрешностей в работе устройств индикации вмешательства, маркировок и пломб. Звучат также убедительные призывы к совершенствованию международных процедур и стандартов в части сохранности ядерных материалов. Тем не менее, среди многих специалистов в области охраны ядерных материалов и установок, а также среди теоретиков ядерного разоружения и нераспространения ядерного оружия бытует ошибочное мнение о существовании якобы защищенных от вмешательства пломб, маркировок и других технологий контроля или их появлении в ближайшем будущем. Это чистая фантазия.

Само понятие "защищенный от вмешательства" нереально и даже бессмысленно. Большинство пломб разобьётся, если их достаточно сильно ударить молотком. Это, конечно, наиболее грубый способ вмешательства. Под понятием "защищенный от вмешательства" обычно подразумевают неповрежденные пломбы или маркировки. Однако даже в этом контексте выражение "защищенный от вмешательства" проблематично, поскольку обычно сложно доказать изначально отрицательное утверждение. Как можно доказать, что пломба или маркировка защищена от всех существующих и потенциально возможных видов, приемов и способов вмешательства? Любая оценка уязвимости может не обнаружить никакой уязвимости, хотя это само по себе должно рассматриваться как очень подозрительный результат. Это может означать лишь то, что при оценке уязвимости не хватило финансовых средств, времени, персонала или отсутствовали технологии, опыт, мотивация, умения, необходимые для неизбежного обнаружения уязвимости. Часто дело в том, что сами оценщики не слишком стремятся находить погрешности. Оценка часто выполняется самими разработчиками или продавцами пломб и маркировок, либо на оценщиков оказывается скрытое (или явное) давление с требованием "сертифицировать" маркировку или пломбу для реальной эксплуатации после того, как на их разработку и/или закупку были потрачены значительные суммы. Обнаружение нежелательной уязвимости может вызвать настоящий ужас.

Выражение "защищенный от вмешательства" часто оправдывается тем, что оно не используется в буквальном смысле. Мой опыт, однако, свидетельствует о том, что многие используют его *именно* буквально. Тем же, кто все-таки не подразумевает его буквально, следует избегать подобной невнятной терминологии. Когда речь идет о ядерном оружии, терроризме и национальной безопасности, а программы разоружения и нераспространения ядерного оружия требуют участия международной дипломатии и переводов на различные языки, необходимо оперировать однозначными терминами. Слова имеют силу. Выражение "защищенный от вмешательства" стало настолько распространенным, что люди начали

воспринимать его буквально. Мне неоднократно приходилось слышать от специалистов в области безопасности, в том числе от занятых в охране отечественных ядерных объектов, заявления: "Наши пломбы защищены от вмешательства" – видимо, на том лишь простом основании, что они называются "защищенными пломбами".

Вопрос уязвимости имеет большое значение, поскольку теоретики START III и других программ разоружения, нераспространения и гарантий часто полагаются на защищенные от фальсификаций маркировки, пломбы, видеокамеры и другие средства контроля. (Эти неуязвимые устройства могут называться или не называться "защищенными" самими этими теоретиками). В некоторых случаях, неуязвимые маркировки, пломбы или другие контрольные устройства рассматриваются в качестве единственных или важнейших элементов, подтверждающих выполнение соглашений, при условии, что обязательность контроля часто считается необходимым условием соблюдения режима.

Воображаемые "защищенные" маркировки и пломбы, на которые ссылаются теоретики, часто не называются конкретно. Если же называются, то под ними обычно подразумеваются электронные или оптоволоконные пломбы, принцип работы которых основан на микроскопической неровности поверхности или других свойствах сложнопрофильной поверхности. Часто они посылают удаленные сигналы либо контролируются раз в несколько месяцев или лет во время периодических инспекций на месте. В любом случае проверяющие убеждены, что эти марки и пломбы покажут следы диверсии или несанкционированной деятельности, поскольку они "защищены от вмешательства". Тот же факт, что маркировки и пломбы остаются недоступными для инспекторов в течение длительного времени и находятся полностью под контролем инспектируемого государства (со всеми его огромными ресурсами) проблемой не считается.

Некоторые их этих гипотетических маркировок и пломб, по всей видимости, имеют поразительную силу, даже большую, чем просто "защита от вмешательства". Они даже могут повышать эффективность защиты самих объектов и контейнеров, на которые они нанесены. То есть, если "защищенная от вмешательства" маркировка имеется, например, на ракете, то нам, по всей видимости, можно не беспокоиться о попытках доступа к содержимому ракеты в другом месте, где маркировки нет. Защитная "аура" маркировки должна каким-то образом предотвратить такие попытки. Аналогично, "защищенные" пломбы должны каким-то образом усилить защиту целого контейнера или замка, на котором стоит пломба.

Справедливости ради, нужно отметить, что некоторые теоретики хотя бы пытаются разработать механизмы такой пространственной защиты. К примеру, предполагается, что из нескольких оптоволоконных кабелей может быть сформирована сеть вокруг защищаемого объекта. Не очень понятно только, что защищает узлы этой сети от повреждений, перемещения и физического вмешательства.

Реальность, к сожалению, такова, что убедительные доказательства существования "защищенных от вмешательства" пломб и маркировок отсутствуют. Зато имеется целый ряд причин полагать, что их существование невозможно. Более того, отсутствуют должное теоретическое понимание процесса обнаружения вторжения, стандарты испытаний пломб/маркировок на уязвимость, и (как указано выше) отсутствует даже способ доказать, что та или иная пломба или маркировка действительно защищена от вмешательства. Фактически, ВСЕ пломбы, которые подвергались *полной* и *эффективной* оценке уязвимости специалистами, которые действительно хотели найти проблемы (а не просто "сертифицировать" пломбу), показали значительную уязвимость, хотя в протоколах, фиксирующих их конкретное применение, и продемонстрированы высокие результаты. Более того, в последние шесть лет выполнялось поразительно мало правительственных и частных исследований в области разработки новых пломб и маркировок повышенной защиты, особенно для применения в рамках программ нераспространения ядерного оружия. Все это

происходит, несмотря на тот факт, что существует потребность в значительно усовершенствованных пломбах и маркировках, и что призывы к дополнительным исследованиям в части технологий контроля звучали за эти годы неоднократно.

Общее предположение, что лучшие пломбы всегда должны быть высокотехнологичными, тоже сомнительно. Лос-Аламосская национальная лаборатория после детального исследования 135 пломб обнаружила, что высокотехнологичные пломбы часто легче фальсифицировать, чем простые. Этому имеется целый ряд причин, в том числе и то, что несложные, практические методы контроля часто оказываются более результативными и их легче согласовать. Хотя современные пломбы и показывают отличное результаты по обнаружению вмешательства, они могут не подходить для применения в некоторых условиях (например, в России) ввиду сложностей с обслуживанием и обеспечением работоспособности, подверженности непредсказуемым отказам оборудования и радиационным повреждениям, а также подозрений (со стороны контролируемой страны) в использовании данных для шпионажа и нарушении безопасности.

Существует также связанное с предыдущим предположение, что вмешательство лучше обнаруживается, если информация с пломбы (даже простой) считывается высокотехнологичным устройством. Считывающими являются электронные или оптические устройства (часто с ручным управлением), используемые в конкретном месте для обнаружения факта вмешательства. Реальность же такова, что высокотехнологичные считывающие устройства (по крайней мере, те, что обычно применяются) часто ухудшают безопасность. Несмотря на то, что высокотехнологичные считывающие устройства часто применяются для экономии средств и времени, пломбы, которые читаются при помощи таких устройств, часто требуют больше времени и усилий для надежного обнаружения вмешательства, чем контролируемые вручную, Еще одна фантазия, которой подвержены некоторые теоретики ядерного разоружения, заключается в использовании высокотехнологичных "черных ящиков" для контроля выполнения условий соглашения. "Черные ящики" представляют собой такие контрольные устройства, установленные инспекторами на месте проверки, принципы и механизмы работы которых, как и метод шифровки и/или детальные технические характеристики не известны инспектируемой стороне в подробностях. Однако в настоящее время при наличии тщательно разработанных и обязательных для соблюдения требований о согласовании с ведомствами охраны и ядерной безопасности любого оборудования, доставляемого в зоны УК и ЯМ на ядерные объекты США, а также ввиду неизбежных опасений инспектируемой стороны, связанных с утечкой секретной информации, представляется крайне маловероятным, что тайное оборудование, методы шифровки или "ловушки" (скрытые пломбы) будут допущены на засекреченные ядерные объекты или в районы расположения ядерных боеголовок.

ОБЩИЕ ПРОБЛЕМЫ

Современные методы применения пломб в США и за рубежом в области ядерной безопасности и других областях далеко не идеальны. Пломбы для конкретных задач часто выбираются без внимательного анализа, иногда на основе устных рекомендаций. Уязвимость пломбы при этом редко берется в расчет, а контрмеры обычно не предпринимаются. При обучении инспекторов, осматривающих пломбы, как правило, подчеркивается необходимость строгого соблюдения формальностей и почти не уделяется внимания таким качествам, как гибкость и наблюдательность, которые обеспечивают эффективную и практическую безопасность. Инспекторам обычно дается мало полезной информации о том, как обнаружить факт вмешательства, и не сообщаются сведения об уязвимости пломб и наиболее распространенных способах их фальсификации, а также отсутствует практическое обучение навыкам обнаружения вскрытых (явно или незаметно) пломб. Эффективные, независимые и регулярные

оценки уязвимости программ обнаружения или устройств индикации вмешательства проводятся редко; интенсивная внешняя поддержка и проверка – еще реже. Даже когда оценки уязвимости проводятся, их результаты и рекомендации часто игнорируются.

Еще менее эффективными, по крайней мере, с точки зрения эксперта по оценке уязвимости, являются попытки оказать давление на результаты оценки или даже на самих экспертов. В моей практике были неоднократные случаи, когда после того, как уязвимость пломбы была продемонстрирована сотрудникам службы безопасности, они просили (или даже требовали), чтобы "об этом не сообщалось руководству". Это – не показатель жизнеспособности программы безопасности! Слабые места есть всегда. Их обнаружение должно восприниматься положительно, поскольку тогда появляется возможность повысить безопасность.

Многие нынешние пользователи пломб полагают (ошибочно), что их пломбы полностью или почти полностью защищены от несанкционированного вмешательства. Мой опыт свидетельствует о том, что они обычно быстро меняют свою точку зрения, если им показать один или более способ обхода их пломб. Они даже начинают задумываться о полном отказе от применения пломб. Это пример того, что Кевин Дж. Су Ху называет (в контексте компьютерной безопасности) "двояким" подходом к безопасности: "…[считается, что] системы либо безопасны, то есть вообще не имеют слабых мест, либо небезопасны…". Более реалистичный и конструктивный подход заключается в том, что безопасность представляет собой континуум. Пломбы (как и все остальное в этом мире) представляют собой неидеальные компромиссы с реальностью и всегда будут уязвимы. Некоторые уязвимые участки могут быть очень серьезными, другие можно исправить или устранить при помощи необходимых мер, а о существовании третьих пользователь так никогда и не узнает.

К сожалению, в программах обнаружения несанкционированного вмешательства на ядерных объектах часто утверждается – в политических целях либо в целях сохранения репутации или позитивного общественного мнения – что их пломбы были, есть и останутся неуязвимыми. Такая позиция безответственна. От пользователей пломб часто можно услышать, что случаев фальсификации пломб никогда не было. Это очень спорный вывод. Без независимого подтверждения отсутствия факта диверсии или вмешательства, то есть без баланса материала, на основании только осмотра пломбы, такие утверждения безосновательны. По определению, фальсифицированные пломбы никогда не обнаруживаются.

Не редкость, когда руководители служб безопасности мало заинтересованы проблемами уязвимости применяемых ими пломб. Причиной этого (наряду с "защищенностью" пломб) обычно называется существование нескольких других уровней физической защиты на случай фальсификации пломбы. Существует пять серьезных причин сомневаться в правильности этой точки зрения. Во-первых, пломбы не должны рассматриваться как составная часть системы физической защиты ядерных материалов, как это часто происходит; они в большей степени являются частью функции контроля и учета. Во-вторых, представление о том, что отказ сигнализации и других средств охраны на одном уровне будет автоматически компенсирован другими уровнями, является верным способом ослабления безопасности. Каждый уровень должен рассматриваться и оптимизироваться без привязки к другим уровням. В-третьих, пломбы (и маркировка) часто являются элементом безопасности, находящимся физически ближе всего к контролируемому ядерному материалу или боеголовке. Поэтому они определенно заслуживают серьезного внимания. В-четвертых, игнорирование уязвимости пломб могло бы быть понятным, если бы для принятия корректирующих мер требовались значительные средства или усилия. Во многих случаях, однако, уязвимость пломб может быть снижена или устранена относительно дешевыми и простыми способами.

Пятая причина, по которой опасно предполагать, будто вмешательство с фальсификацией пломбы будет зафиксировано другими средствами охраны, заключается в том, что потенциальным нарушителям может

быть и не обязательно проходить через внешние уровни охраны. Работник самой организации, например охранник, пытающийся похитить ядерные материалы или организовать диверсию, уже будет иметь допуск через многие или даже все внешние уровни физической защиты. Внешние инспекторы для выполнения своих задач обычно также проводятся через один или несколько уровней охраны. Если же речь идет о контроле использования и нераспространения ядерных материалов, государство, в котором находится контролируемый объект, является *собственником* объекта и большинства или всех его уровней безопасности. Это значит, что, по меньшей мере, некоторые из этих уровней безопасности не могут использоваться в качестве "дополнительных" к пломбам индикаторов вмешательства, поскольку работники, контролирующие эти уровни безопасности, и являются теми потенциальными нарушителями, против которых устанавливаются пломбы!

Одна из постоянных проблем в применении средств контроля вмешательства в рамках программ нераспространения ядерных материалов заключается в непонимании отличия такой программы от внутренних программ безопасности и охраны. Часто предполагается, что меры, применяемые для обеспечения безопасности и гарантий внутри страны (в т.ч. пломбы), могут быть просто заимствованы с небольшими модификациями для применения в международных программах контроля и нераспространения ядерных материалов. В реальности же, отечественные "меры безопасности" сильно отличаются от международных (например, мер безопасностей МАГАТЭ) с точки зрения целей, кадров, экономических подходов, среды, видов нарушений, секретности, степени уверенности в предшествующих и последующих этапах процесса, оптимально возможного оборудования, структур, которые имеют/устанавливают/эксплуатируют контрольное оборудование, и последствий неудачного применения таких мер. Эти различия часто игнорируются. Нас уверяют, например, что организовать мониторинг периметра на зарубежных ядерных установках будет "проще, чем кажется сначала, поскольку предполагается, что ядерные объекты уже оснащены системой охраны периметра". При этом не обращается внимания на тот факт, что существующая система охраны периметра ориентирована на совершенно другие цели, других потенциальных нарушителей и принадлежит, эксплуатируется и контролируется самой проверяемой страной. Аналогично, при обсуждении способа применения START III на американском складе и заводе по демонтажу боеголовок Пантекс в Техасе часто предполагается, что международные инспекторы могут просто использовать имеющиеся на Пантексе пломбы и базу данных по пломбам для своих проверок. Но это бессмысленно, поскольку отечественные пломбы ориентированы на один тип возможных нарушителей – лицо или группу лиц, имеющих враждебные объекту намерения, – в то время как пломбы для контроля выполнения международных соглашений предназначены для обнаружения попыток несанкционированного вмешательства со стороны самой страны-владельца объекта. Страна-нарушитель будет иметь на 6-9 порядков больше ресурсов, чем злонамеренное лицо или группа лиц, против которых направлены внутренние меры ядерных "систем безопасности".

Пломбы для контроля выполнения межгосударственных соглашений должны обладать совершенно иными свойствами, чем те, что применяются внутри США в целях контроля и обеспечения безопасности. Существующие пломбы для применения внутри страны, например, не предназначены для того, чтобы предоставлять наблюдателям (или видеокамерам) хороший обзор при установке, осмотре и снятии пломбы. Между тем, такой обзор может быть необходим для двустороннего или трехстороннего контроля работ по демонтажу ядерных боеголовок. Причина в том, что международным инспекторам вряд ли будет дано разрешение на прямой доступ к контейнерам с ядерными боеголовками или на установку пломб непосредственно на них по соображениям ядерной безопасности и охраны материалов. Вместо этого, пломбы обычно устанавливаются персоналом организации-

владельца объекта под пристальным наблюдением инспекторов. Даже если иностранным инспекторам когда-нибудь и будет дано разрешение самим устанавливать пломбы на контейнерах с боеголовками, все-таки, нынешние конструкции пломб и протоколы использования для внутренних целей рассчитаны на то, что у устанавливающего пломбу лица нет враждебных намерений. Однако это не обязательно относится к международному контролю.

Другой проблемой нынешних средств обнаружения вмешательства является то, что, несмотря на их 7000-летнюю историю, эта область остается слабо изученной. Отсутствует теоретическое обоснование и существует удивительно мало публикаций (открытых и закрытых) о пломбах и маркировке. Лишь некоторые из руководств по безопасности и физической защите посвящают пломбам больше, чем один абзац, а маркировке уделяется еще меньше внимания. Отсутствуют общие описания на тему контроля вмешательства. Те немногие нормативы, которые относятся к пломбировочным устройствам, не отличаются подробностью и обоснованностью в части выбора и эксплуатации пломб, а также испытаниях на уязвимость. Ведется активное обсуждение "международных норм или стандартов" в области общей физической защиты ядерных материалов, а также имеется большой интерес к американскому "Стандарту хранения вооружений" и рекомендациям МАГАТЭ (INFCIRC/225 ред. 4) по защите ядерных материалов. Однако в них не говорится почти ничего о маркировке, пломбах и обнаружении вмешательства.

КОНКРЕТНЫЕ ПРОБЛЕМЫ

Как хорошо известно, в области учета и контроля российских ядерных материалов, в том числе и в проектах международной технической помощи, организуемых США, имеется ряд серьезных проблем. В России обычно используются устаревшие пломбы, пломбы, которые легко фальсифицировать, или же пломбы вообще не используются. Россияне также обычно демонстрируют слабый интерес к внутренней угрозе. Отсутствует комплексная программа испытаний системы УК ЯМ, и Министерство энергетики США не предпринимает шагов по ее созданию, хотя такая программа необходима для эффективной работы. Общее руководство программами поддержки УК ЯМ в России со стороны Министерства энергетики было далеко не идеальным, а программы по снижению ядерной угрозы, которые проводит Министерство обороны США, сталкиваются с постоянными трудностями. В случае с хранилищем делящегося материала на заводе "Маяк", например, Министерство обороны не уверено, что именно Соединенные Штаты должны там контролировать: эффективность собственной российской программы УК ЯМ или выполнение российской стороной условий международных соглашений, либо и то, и другое. Ни Министерство обороны, ни Министерство энергетики не видят различия между внутренней программой безопасности и наблюдением за выполнением международных соглашений, и не понимают, какое охранное или контрольное оборудование должно применяться в России, кто должен им владеть и эксплуатировать.

В отличие от России, американская программа УК ЯМ обычно считается наиболее проработанной и эффективной в мире. Существуют, однако, проблемы и критические замечания в её адрес, что создает очевидную необходимость в совершенствовании этой программы. Что касается вопроса об индикации вмешательства, МЭ США демонстрирует полное отсутствие специальных знаний в области пломбировочных устройств и их применения. Многие руководители МЭ США считают, что их ведомство использует "защищенные" пломбы. Поразительно, что в основном Руководстве Министерства энергетики по гарантийным пломбам не содержится никакой полезной информации о пломбах и не упоминается о необходимости специальной подготовки, которая дала бы инспекторам возможность познакомиться с видами уязвимости пломб и наиболее распространенными типами вмешательства. Более того, в МЭ США утверждают, что пломбы способствуют снижению

радиационного воздействия на персонал. В действительности же способы использования многих пассивных пломб ведут как раз к обратному. Установка, осмотр и снятие пломб МЭ часто требуют выполнения длительных манипуляций, вызывающих облучение персонала, в которых не было бы необходимости, если бы пломбы не использовались. Частые двойные проверки пломб МЭ США, а также заказы на замену пломб в условиях, когда приняты недостаточные меры безопасности, тоже являются причиной дополнительного облучения персонала.

Для обеспечения ядерной безопасности и охраны объектов в США используются пломбы, которые никогда не проходили оценку уязвимости, а также пломбы, которые прошли лишь поверхностную оценку уязвимости или "сертификационные" испытания (зачастую выполненные самим же разработчиком или продавцом пломбы), либо пломбы, прошедшие оценку уязвимости, результаты которой игнорируются или не сообщаются пользователям пломбы. По всей видимости, лишь немногие пользователи пломб и руководители служб безопасности в ядерном комплексе США имеют хотя бы элементарное представление о уязвимости пломб и протоколах её оценки.

Особенно неудачной практикой в последние годы стал преждевременный перенос методов и оборудования УК ЯМ, применяемых для внутренних программ США, на аналогичные международные программы. Передача технологий может быть вполне оправданна, если свойства оборудования и его слабые места хорошо известны, либо когда оборудование явно обеспечивает лишь средний уровень безопасности, либо не применяется на ядерных установках США. Однако передача ключевых систем УК ЯМ не представляется целесообразной в то время, когда у самих США имеется только поверхностное понимание проблем, связанных с их применением. Это не только ставит под потенциальную угрозу национальную безопасность США, но и свидетельствует о серьезном непонимании разницы между внутренней безопасностью и контролем над выполнением международных соглашений. Ни одна система или устройство безопасности не могут быть оптимизированы для обоих типов применения одновременно.

Если обратиться к МАГАТЭ, то будет очевидно, что этому агентству приходится решать ряд сложных проблем и испытывать трудности, среди которых "бюджет с нулевым ростом", задержки финансирования, ограниченность ресурсов, сложности морального характера, культурные и языковые различия, непростые, а иногда и неблагоприятные условия на местах, необходимость тесно сотрудничать с бюрократическими правительственными структурами, различные цели, которые преследуют страны-члены МАГАТЭ и их различные подходы к безопасности, а также нереалистичные ожидания со стороны некоторых критиков. Несмотря на все эти трудности, МАГАТЭ ведет программу обеспечения безопасности, которая достойна всяческих похвал в части ее профессионализма, качества и эффективности. У МАГАТЭ имеется сложная программа применения маркировок и пломб и достаточное понимание практических проблем при обнаружении вмешательства. Агентство производит первоклассный анализ пломб после их эксплуатации на местах. МАГАТЭ также обладает группой высокообразованных, преданных своему делу инспекторов, которым нет равных в мире в части их квалификации и мотивации.

В то же время, МАГАТЭ сталкивается и с некоторыми недостатками и проблемами, касающимися, в частности, обнаружения вмешательства. Агентство имеет "двоякий" подход к мерам безопасности (он изложен выше) и обычно настаивает – без убедительных доказательств – что его пломбы защищены от вмешательства. МАГАТЭ также обвиняют в том, что его программа безопасности недостаточно прозрачна, а также в том, что оно отказывается от проведения независимых внешних проверок, результаты которых могут быть не всегда положительны. Беспокоит также, что Агентство имеет склонность к достаточно агрессивному способу доведения до всеобщего сведения фактов вмешательства или попыток сокрытия несанкционированных действий, а также то,

что Агентству не хватает возможностей в части сбора информации, и в обществе существует неверное понимание сути его деятельности.

МАГАТЭ в целом добросовестно подходит к организации проверок большинства своих пломб на уязвимость. Агентство часто начинает тщательные проверки уязвимости пломб только после того, как возьмет на себя обязательство (по крайней мере, неофициальное) использовать пломбу конкретной конструкции. У Агентства отсутствует собственная реальная программа исследований пломб и маркировок и внутренняя программа оценок уязвимости и оптимизации применения пломб. Вместо этого, МАГАТЭ полагается на специальную техническую поддержку со стороны своих членов, которая отличается по качеству и часто выполняется неэффективно, под политическим давлением, при ограниченном и нестабильном финансировании. Непонятно, полностью ли результаты оценок уязвимости учитываются в протоколах, при обучении и исследованиях использованных пломб и оптимально ли подобраны сами пломбы для конкретного применения. Несмотря на высокую мотивацию и тщательную подготовку, инспекторы МАГАТЭ часто не знакомы со слабыми сторонами применяемых ими пломб и наиболее вероятными сценариями их взлома. Это существенно сокращает их возможности в части обнаружения вмешательства. Также существует мнение, что подход инспекторов МАГАТЭ часто не отличается целостностью, активностью и способностью к критическому наблюдению, и что им не разрешается применять требуемую гибкость и личную инициативу.

В рамках своей программы, МАГАТЭ выполняет слепой (не двойной) тест эффективности обнаружения признаков вмешательства в пломбу. Эти проверки, однако, ориентированы скорее на контроль качества, чем на оценку вероятности обнаружения реальной фальсификации пломбы. Пломбы, подвергающиеся таким проверкам, обычно подложные или имеющие очевидные повреждения, а не подвергшиеся вмешательству с применением более изощренных и реально существующих методов.

Еще одна проблема, которая становится предметом значительного беспокойства любой инспекционной программы безопасности, заключается в надежности персонала служб безопасности и самих инспекторов. Рекомендации МАГАТЭ по проверкам персонала, содержащиеся в стандарте INFCIRC/255, достаточно расплывчаты, и сами инспекторы МАГАТЭ, по всей видимости, также не проходят основательной проверки ни до, ни после принятия на работу. Надежность инспектора, контролирующего пломбы и маркировки, является решающей для эффективного обнаружения попытки вмешательства, и может представлять собой источник серьезной уязвимости. Помимо выполнения контролирующей функции, инспектор должен пройти тщательную проверку на доступ к ядерным установкам и материалам, и игнорировать это требование просто неразумно. Многие инспекторы, специалисты по безопасности и высокопоставленные руководители МАГАТЭ, вероятно, проходят более тщательную проверку при получении кредитной карточки, чем при получении доступа к пломбам, данным по безопасности, контрольному оборудованию, ядерным материалам и установкам. МАГАТЭ, по всей видимости, также не готово противостоять психологической атаке и другим нападкам на инспекторов и руководство Агентства, участвующих в программах безопасности.

Надежность гарантий и обнаружения вмешательства со стороны МАГАТЭ также снижается ввиду недостаточности мер элементарной безопасности в этой организации. Никаких существенных изменений не произошло с 1994 года, когда Дэвид Кей обвинил МАГАТЭ в том, что оно "…представляет собой международную бюрократическую организацию, которая даже не проверяет анкетные данные своих сотрудников до и после приема на работу, не осуществляет реальной охраны коммуникаций, не обеспечивает защиту документации в соответствии с государственными нормативами, а также не имеет соответствующей практики

осуществления контрразведывательных мероприятий либо неспособно их осуществлять".

НОВЫЕ ВИДЫ УСТРОЙСТВ ИНДИКАЦИИ ВМЕШАТЕЛЬСТВА

Существует значительный интерес к использованию электронных средств контроля, например, таких, как видеонаблюдение и системы дистанционного контроля в рамках программ проверки выполнения международных соглашений. Традиционно видеонаблюдение применяется для защиты объектов от внешнего вмешательства либо как дополнительное средство контроля над деятельностью персонала самого объекта. Однако, в случае проверки выполнения условий международных соглашений потенциальные нарушители не являются ни персоналом, обслуживающим установку, ни вторгшимися извне злоумышленниками. Потенциальным нарушителем выступает само государство, владеющее всем объектом, в том числе и теми самыми стенами, на которые монтируются камеры наблюдения. Метод видеонаблюдения в таком контексте проанализирован слабо. Между тем, этот контекст подразумевает нечто большее, чем простое применение уже существующих подходов к видеонаблюдению.

Ограниченная оценка уязвимости видеосигналов и видеокодирования обычно предполагает, что устройство-передатчик и устройство-приемник физически недоступны для злоумышленника. Это предположение не безопасно, с учетом тех скромных мер, которые предприняты к настоящему моменту для защиты систем видеонаблюдения от физического вмешательства на уровне передатчика и приемника, а также защиты от подмены электронного или оптического сигнала. Сигналы датчиков удаленного контроля других типов также уязвимы для вмешательства.

Даже если само оборудование и "защищено" каким-то образом, то функция видео-кодирования (или проверка подлинности входного сигнала) может быть уязвима. Это должно вызывать особенное беспокойство в связи с тем, что наиболее современные методы кодирования могут быть недоступны для международных программ безопасности, а контролируемая страна может направить существенные ресурсы на взлом алгоритмов кодирования.

Непрерывный, крупноплановый телевизионный контроль маркировок и пломб представляет собой нетрадиционный вид видеонаблюдения, который может оказаться полезным для программ контроля выполнения международных соглашений по ядерному разоружению и нераспространению ядерных материалов. Использование видеокамер в сочетании с пломбами в целях контроля достаточно распространено. При этом камеры, как правило, направлены на помещение, проход или людей, а не на саму пломбу крупным планом. Пока что мало известно о слабых сторонах и оптимальных пользовательских протоколах для непрерывного крупнопланового видеонаблюдения за самими пломбами.

Еще одной потенциально важной сферой применения пломб в целях контроля выполнения международных соглашений является контроль подлинности объектов контроля, например, таких, как образцы окружающей среды. Международные споры вокруг подлинности образцов среды могут со временем стать такими же напряженными, как нынешние споры вокруг справедливости результатов спортивного допинг-контроля.

ЧТО НЕОБХОДИМО СДЕЛАТЬ?

С учетом разнообразия изложенных выше проблем, возникает вопрос о том, что необходимо сделать для совершенствования методов обнаружения вмешательства – как в настоящее время, так и в будущем – в рамках внутренних и международных программ безопасности, инспекций и контроля выполнения соглашений. Вот некоторые рекомендации:

1. Имеющиеся пломбы необходимо использовать более эффективно. В том числе должны более активно применяться протоколы и проводиться соответствующее обучение, более полно представляющее слабые стороны и возможные способы вмешательства в

применяемые типы пломб. Инспекторы должны обучаться навыкам обнаружения скрытых признаков вмешательства в конструкцию пломб и учитывать их слабые стороны.

2. Существующие пломбы и программы обнаружения вмешательства должны подвергаться более тщательной оценке их слабых сторон. Рекомендации, полученные в результате таких оценок (при условии их пользы, практичности и экономичности), должны неукоснительно выполняться.
3. Необходимо осуществлять хотя бы минимальные базовые проверки инспекторов пломб и персонала, занятого в программах обнаружения вмешательства, а также другого инспектирующего персонала, имеющего доступ к ядерным установкам.
4. Выбор пломб должен выполняться более осторожно, после тщательного анализа.
5. Необходимо создавать новые/усовершенствованные пломбы и маркировки, особенно для инспекционной деятельности в рамках международных соглашений. Их слабые стороны должны быть хорошо известны. Также необходимы усовершенствованные контейнеры.
6. Необходимо выполнить исследования в области защиты от вмешательства оборудования видеонаблюдения и других средств дистанционного контроля.
7. Необходимо выполнить исследования возможностей применения и недостатков непрерывного крупнопланового видеонаблюдения за маркировками и пломбами.
8. Маркировки, пломбы и обнаружение вмешательства в целом требует более тщательного теоретического исследования и практического анализа. Он должен включать более подробную проработку действий, предпринимаемых в случае обнаружения признаков вмешательства. В нынешних программах контроля вмешательства это недостаточно проработано.
9. Нормы и стандарты безопасности в части контроля вмешательства нуждаются в более глубокой проработке и более широком применении.
10. Необходимы реалистичные ожидания и понимание того, что в конечном итоге контроль выполнения соглашений представляет собой вероятностный тип деятельности, предполагающий как сбор, так и оценку и толкование информации. Какой бы сложной в количественном отношении ни была технология контроля и как бы уверены (справедливо или ошибочно) в ней мы ни были, в конечном итоге контроль будет всегда сводиться к субъективному мнению.

В том, что касается маркировок и пломб, не следует впадать в отчаяние по поводу невозможности эффективного контроля, а также отказываться вообще от использования пломб, маркировок и видеокамер просто потому, что они уязвимы, как и все средства безопасности. Вместо этого, необходимо использовать разумный, реалистичный, комплексный (не "двоякий") подход к контролю и обнаружению вмешательства, четко представлять себе слабые стороны используемых и разрабатываемых устройств и программ, быть готовым к внедрению разумных мер безопасности в оборудование и программы, а также проводить исследования, направленные на совершенствование обнаружения вмешательства, более полное понимание его роли и ограничений применения.

В конечном итоге, перед любой программой обнаружения вмешательства должны ставиться следующие реальные цели:

1. Обнаружение непрофессионально осуществленного или открытого вмешательства с высокой вероятностью;
2. Обнаружение вмешательства, осуществленного профессиональным противником, с вероятностью значительно выше нуля (но она никогда не составит 100%), выполненное на

максимально достижимом уровне в результате анализа затрат и результатов;
3. Низкое количество ложных тревог;
4. Обеспечение высокого уровня психологического сдерживания, заставляющего потенциальных нарушителей тратить значительные средства на разработку и реализацию вмешательства, и также заставляющего их беспокоиться о своем возможном обнаружении.

Наконец, стоит заметить, что контроль выполнения условий международных соглашений мог бы быть значительно проще, дешевле, легче и надежнее, если определенное ограниченное количество секретной информации могло бы стать открытым для всех сторон соглашения. Частичное раскрытие секретной или чувствительной информации, как правило, все равно происходит с течением времени в ходе реализации программ разоружения и нераспространения ядерных материалов, особенно если в их рамках проводятся инспекции объектов. Для России и Соединенных Штатов было бы полезно более реалистично проанализировать, какую информацию действительно нужно скрывать друг от друга. Вполне возможно, что существует категория информации, которая вполне может быть открыта для обеих сторон, но не должна разглашаться общественности или какой-либо третьей стороне. Проблема заключается в том, что анализ такой информации должен быть тщательным, комплексным и сбалансированным. Руководители ведомств безопасности, разработчики вооружений и консервативные политики будут, вероятно, видеть угрозу национальной безопасности в раскрытии некоторой части секретной информации и игнорировать или недооценивать пользу, которую принесет стране получение аналогичной информации другой стороны. Специалисты по анализу разведывательных данных и сторонники разоружения, в свою очередь, могут преувеличивать пользу информации, полученной от другой стороны, меньше беспокоясь о раскрытии секретов своей собственной страны.