Бажано ввести таке поняття та термін, як **піднаглядність об'єкта вимогам ТЗІ**, як це існує наприклад у такій сфері стандартизації, як охорона праці; у метрології – державний метрологічний контроль, державний метрологічний нагляд.

При проектуванні приладів з ТЗІ слід відрізняти такі поняття, як технічна характеристика, метрологічна характеристика, точнісна характеристика.

Необхідно розрізняти поняття: *одиниця фізичної величини*, *одиниця вимірювання*, *метрологічна характеристика;* а також: *коефіцієнт*, *параметр*, *фактор*.

Висновок. Для розвитку сфери використання технічних засобів ТЗІ необхідно розширити кількість еталонів та повірочних схем, підвищити чутливість приладів.

УДК 638.235.231

ЛИЦЕНЗИРОВАНИЕ, СЕРТИФИКАЦИЯ, ИСПЫТАНИЯ В ОБЛАСТИ ТЗИ В УКРАИНЕ

Александр Лаврентьев
НИЦ "ТЕЗИС" НТУУ "КПИ"

Аннотация: **В настоящей статье изложена точка зрения специалиста по ПД ТСР на формирование системы лицензирования и сертификации в области ТЗИ в Украине.**
Summary: **In this article of the specialists of counteraction of TMSS presents his point of view on the formation of the licence and sertification system in the field of TDI in Ukraine.**
Ключевые слова: **Лицензирование, сертификация, испытания.**

Одним из первых реальных шагов в формировании национальной системы ТЗИ в Украине явилось создание системы государственного лицензирования деятельности в области защиты информации. Были внесены соответствующие изменения в Закон о предпринимательской деятельности и введена в действие соответствующая инструкция. Несколько лет функционирования этой системы позволяют подвести некоторые итоги. Прежде всего необходимо установить, какие цели преследует лицензирование в области ТЗИ и достигнуты ли они? Одной из основных задач института лицензирования вообще является защита страны и ее населения от товаров, которые могут нанести ущерб жизни и здоровью граждан, экологии, нормальной работе важных систем и т.д. Целью лицензирования может служить также пополнение бюджета государства (как форма "скрытого налога" на высокодоходные виды деятельности). Обе эти цели маловероятны, так как деятельность в области ТЗИ не проносит сверхприбылей, цена лицензии не высока, а угрозы для здоровья и экологии отсутствует.

Можно сделать вывод, что лицензирование предпринимательской деятельности в области защиты информации с ограниченным доступом от утечки по техническим каналам может иметь смысл как государственная гарантия качества предоставляемых услуг. Это существенно при проведении мероприятий по защите гостайны. Но для тех, кто работает с гостайной, давно существует налаженный механизм допуска и при отсутствии такого, надлежащим образом оформленного, никакая лицензия не даст права на проведение работ по защите секретной информации. Несколько иная ситуация возникает при организации защиты информации субъектами негосударственного сектора. При этом наблюдаются два подхода к решению проблемы.

В первом случае руководство субъекта предпринимательской деятельности (далее фирма) понимает необходимость защиты информации и реально заинтересовано в качественном выполнении работ. При этом фирма будет искать специалистов, имеющих наибольший авторитет в данной области, не зависимо от того, работают ли специалисты в организации, имеющей лицензию. Таким образом, стимулируется проведение этих работ за счет теневого сектора экономики. Не исключено, что коммерческие структуры не всегда охотно пойдут на сотрудничество с лицензиатами, находящимися под прямым контролем СБУ.

Во втором случае руководство фирмы не считает актуальным необходимость проведения мероприятий по защите информации, но желает выполнить все положенные требования. В этой ситуации для заказчика не имеет значения качество выполнения работ, важно только, чтобы договор и результаты работ были оформлены в соответствии с требованиями руководящих документов (кстати, аналогичное отношение в ряде случаев просматривается и в госучреждениях). Такой подход дискредитирует систему ТЗИ вообще и лицензирования деятельности в этой области в частности. Кроме того, в этой ситуации снижаются требования к линцезиатам, что понижает общий уровень проведения работ в области ТЗИ в целом по стране.

Рассмотрим лицензирование с точки зрения направлений деятельности лицензиатов в области ТЗИ. Поскольку речь идет об оказании платных услуг потребителю, нормативная база должна, прежде всего, учитывать интересы заказчика. Сегодня защита информации на фирмах и в организациях сводится, в основном, к следующим направлениям:

- защита речевой информации с ограниченным доступом, циркулирующей на объекте, от утечки по техническим каналам;
- защита информации с ограниченным доступом, циркулирующей в средствах вычислительной техники, от утечки по техническим каналам;
- защита информации с ограниченным доступом от утечки через закладные устройства;
- защита информации с ограниченным доступом, циркулирующей в АС, от несанкционированного доступа (компьютерная безопасность - КБ);
- защита информации с ограниченным доступом, передаваемой по коммуникациям различного назначения.

Очевидно, что система лицензирования должна быть адекватной названным задачам. Кроме интересов потребителя, указанные направления деятельности объединяет единство технической и нормативно-методической базы. Каждое направление может разделяться на уровни - защита государственной и негосударственной тайны. Можно также выделить монтаж средств защиты и их специсследования, при условии, что аттестация объекта защиты уже проведена силами самой организации или другим лицензиатом.

Рассмотрим с этой точки зрения, какие требования к видам деятельности предъявляет к лицензиатам «Інструкція про умови і правила провадження підприємницької діяльності (ліцензійні умови), пов’язаної з розробленням, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів технічного захисту інформації, а також з наданням послуг із технічного захисту інформації, та контроль за їх дотриманням». В ней определены такие виды работ, подлежащих лицензированию:

«1.3.1. Дослідження об’єктів інформаційної діяльності та інформаційних систем щодо безпеки інформації, надання консультативних послуг з технічного захисту інформації.

1.3.2. Розроблення, впровадження, атестація, обслуговування систем технічного захисту інформації від технічних розвідок та спеціальних впливів на об’єктах інформаційної діяльності.

1.3.3. Розроблення, впровадження, супроводження систем технічного захисту інформації в інформаційних системах.

1.3.4. Виявлення та блокування витоку мовної та видової інформації через закладні пристрої на об’єктах інформаційної діяльності.

1.3.5. Розроблення, виготовлення, використання та реалізація засобів забезпечення технічного захисту інформації.

1.3.6. Ввезення, вивезення засобів технічного захисту інформації»

Как видно из приведенного перечня, он не учитывает реального подхода к технической защите информации и потребностей заказчика. Реализация пп. 1.3.2. 1.3.3. невозможна без п. 1.3.1., так как нельзя разработать и реализовать систему защиты информации без исследования объектов; а разработанные на основе исследования рекомендации по созданию системы ТЗИ фактически являются "консультативными услугами". Пп. 1.3.1. - 1.3.3. не определяют конкретный вид деятельности. Как уже говорилось, оценка защищенности АС от утечки информации за счет ПЭМИН и защита речевой информации существенно отличаются методологией и используемой аппаратурой. Инструкция не предусматривает конкретного вида деятельности. Таким образом, лицензиат должен либо показать готовность к проведению любого вида работ (что не всегда необходимо и оправдано), либо заявить одно направление деятельности по защите, что не мешает впоследствии произвольно расширять сферу деятельности. Наиболее четкий, обоснованный и конкретный вид деятельности определен п. 1.3.4. Это, видимо, связано с тем, что процесс поиска закладных устройств носит не столько технический, сколько оперативно-технический характер.

Кроме того, первые три вида деятельности обеспечены только закрытой нормативно-методической документацией, для защиты конфиденциальной информации открытая нормативная база отсутствует. Лицензиатам по этим пунктам необходимо иметь 1-й отдел или доступ к документации, независимо от категории лицензии.

Рассмотрим последовательно составляющие п.1.3.5. *Разработка* средств обеспечения ТЗИ. Неясно, какую роль в этом виде деятельности играет лицензирование. Простой пример - помехоподавляющие сетевые фильтры. Они имеют двойное назначение - защита ПК от помех в сети и защита информации от утечки по цепям питания. Если предприятие давно изготавливает такие фильтры, то теперь оно должно получить на это лицензию (?). С другой стороны, для получения лицензии достаточно предъявить простое по конструкции изделие (например, диодно-емкостной фильтр типа "Гранит- VIII"), а потом можно изготавливать любое по сложности и назначению изделие. Если разработка ведется по госзаказу, то никакой лицензии не требуется. Тогда зачем она организации, которая нашла решение в инициативном порядке? Можно разрабатывать тот же сетевой помехоподавляющий

фильтр без лицензий, а потом найти ему применение в целях ТЗИ. *Изготовление* средств обеспечения ТЗИ. В лицензии не указано, на какое именно средство она выдана.

Основным (и единственным) регулятором применения средств обеспечения ТЗИ является система сертификации. Рассмотрим простую ситуацию: предприятие имеет лицензию на производство средства обеспечения ТЗИ, но оно не прошло сертификационных испытаний. Такое изделие не может быть рекомендовано для применения. С другой стороны, изготовленное в инициативном порядке и прошедшее сертификационные испытания изделие может быть рекомендовано для обеспечения ТЗИ. Возникает закономерный вопрос, какую цель преследует лицензирование в єтой области.

Те же аргументы относятся к "ввозу, вывозу средств ТЗИ". Еще можно понять регламентацию ввоза и вывоза средств съема информации, но средства защиты могут вводиться без ограничений при условии их сертификации.

Еще одним существенным аспектом является нормирование труда в этой области. В других областях деятельности такое нормирование существует. Безусловно, в рыночных условиях нереально навязывать стоимость договорных работ, вместе с тем ориентировочные средние трудозатраты должны быть определены нормативным документом. Отсутствие норм трудозатрат приводит к тому, что некоторые лицезиаты неоправданно и значительно завышают стоимость работ. Это не принципиально, если договор заключают между собой коммерческие структуры. Но если договор на выполнение работ по защите информации заключается на бюджетные средства, то это приводит к неоправданному расходу государственных денег. С другой стороны, имеет место демпинг со стороны лицензиатов с целью получения заказа любой ценой. За предлагаемые сроки и стоимость работа просто физически не может быть выполнена с необходимым качеством. Таким образом, гарантия, которую должна обеспечивать государственная лицензия, фактически не обеспечивается качеством работы. В предлагаемом документе, нормирующем трудозатраты, не должно быть точных расценок. Достаточно, как это было указано в методиках ГТК, привести нормы затрат труда для основных видов работ. Причем это может быть рассчитано как для случая использования стандартной КИА, так и для автоматизированных измерительных комплексов, которые разрешены к применению. Таким образом, может быть сформирован регулируемый цивилизованный рынок в области защиты информации, в противовес существующему. В результате не пострадает здоровая конкуренция, так как будет сохранена разница цен за счет разной стоимости рабочей силы, различных накладных и прочих расходов, разной прибыли.

Итак, проведенный анализ показывает, что принятая в Украине система лицензирования в области ТЗИ не полностью отвечает поставленным задачам и современным требованиям. Из сложившейся ситуации имеется два выхода - отказ от системы лицензирования в области ТЗИ вообще, либо ее радикальное изменение с учетом интересов Украины и здравого смысла.

Выводы:

1. Необходимо четко и однозначно определить цели и задачи лицензирования в области ТЗИ, изучив мировую практику в этом вопросе.
2. Определить конкретные направления деятельности, установить перечень аппаратуры и нормативно-методической документации, необходимые для качественного выполнения поставленной задачи.
3. Исходя из установленных целей и задач лицензирования в области ТЗИ, разработать подробные требования к лицензиатам по каждому направлению деятельности.
4. Разработать пакет нормативно-методических документов, регулирующих деятельность по защите конфиденциальной информации.
5. Провести расчет средних трудозатрат на выполнение основных операций при проведении работ в области ТЗИ и разработать соответствующий нормативный документ.

Очевидно, что система лицензирования предпринимательской деятельности в области ТЗИ в Украине представляет сложный комплекс проблем, которые необходимо решать в ближайшее время. Вместе с тем, существуют предложения по еще более усугублению ситуации, предполагающие введение так называемой системы "выдачи разрешений на проведение работ по ТЗИ для собственных потребностей". Во-первых "разрешение" и "лицензия" - одно и тоже слово на разных языках (licentia (лат) - разрешение, право). Во-вторых, не наладив в совершенстве систему лицензирования в области предпринимательской деятельности, вводить новые разрешения, которых потребуются тысячи, по меньшей мере, нецелесообразно. В третьих, из действующих документов неясно, к каким организациям планируется применение этой системы - отнесения ее и к негосударственным структурам, безусловно станет нарушением прав и свобод. И, в-четвертых, нужны ли такие разрешения при условии реализации ответственности руководителей за состояние системы ТЗИ в организации (Положение о ТЗИ) и грамотно организованном контроле?

Значительно медленнее идет формирование системы сертификации в области ТЗИ. Только на восьмом году после создания ГСТЗИ моздан первый сертификационный центр и испытательные лаборатории. Отсутствуют стандарты, нормативные документы, не определены критерии, которые позволяли бы квалифицированно оценивать технические условия на предъявляемые изделия. Методики контроля ГТК устарели морально и по своей структуре не отвечают современным требованиям. В данной ситуации, чтобы избежать ненужных ошибок,

целесообразно обратиться к опыту России, в которой такая система действует, и перенять ту его часть, которая может оказаться полезной Украине.

Главный вопрос в этой сфере, тот же, что и в области лицензирования - какие цели перед собой ставит сертификация и каким образом эти цели будут достигаться? В принципе, система сертификации должна нести полезную для ТЗИ в Украине функцию – защита потребителя, пользующегося средствами защиты информации, от недобросовестных поставщиков (производителей). Но поскольку применение средств ТЗИ не несет угрозы жизни и здоровью граждан Украины, состоянию окружающей среды, то она не должна быть обязательной. Вместе с тем, интересы государственной безопасности требуют надежной защиты гостайны. В этом случае должны применяться только проверенные (сертифицированные) средства защиты информации. Таким образом, будут решены две задачи: можно избежать государственного давления на предпринимателя без особой необходимости, с одной стороны, и обеспечить надежную защиту государственных интересов – с другой. Предприниматель сам сможет выбирать любое средство обеспечения ТЗИ, но заинтересованный в защите своей информации остановится на сертифицированном устройстве.

При отсутствии государственных стандартов возникает проблема с техническим основанием для проведения сертификации. Стандартная схема на сегодняшний день:

- разработка технических условий (ТУ) с включением в него требований по ТЗИ осуществляется разработчиком изделия;
- согласование ТУ в части требований по ТЗИ в государственном органе;
- утверждение ТУ в части отсутствия противоречий и выполнения требований стандартов по оформлению документа в Госстандарте.

Как видно, в этой схеме не участвуют научно-исследовательские организации, которые должны давать техническую оценку предложенного решения. Ранее эти функции выполняли головные научно-исследовательские организации по направлениям защиты информации, которые в Украине в настоящее время не созданы.

Не решенным на сегодняшний день является вопрос сертификации в части ТЗИ импортируемых изделий или признания иностранных сертификатов. В этом случае затраты на сертификацию какого-либо образца понесет одна организация, а ее результатами будут пользоваться все поставщики.

В связи с отсутствием системы сертификации в области ТЗИ в Украине, были разработаны перечни средств ТЗИ, разрешенных к применению. Эта мера была как вынужденной, так и необходимой - она позволила в какой-то степени управлять применением средств ТЗИ при отсутствии системы сертификации. Но теперь, когда сделаны первые шаги в формировании этой системы, перечни стали тормозом в ее развитии. Зачем тратить средства на сертификацию, если изделие есть в упомянутом перечне, или его не сложно включить в этот перечень? Одним из выходов из создавшейся ситуации, позволивших перейти от системы разрешений к системе сертификации, могла бы стать централизованная организация испытаний с последующей компенсацией затрат путем отчислений от реализации сертифицированных изделий. По мере выдачи сертификатов из перечня должны исключаться изделия, аналогичные сертифицированным по назначению и основным параметрам.

Так же,как и в области лицензирования, в области сертификации существует проблема нормирования труда при проведении типовых испытаний.

Выводы:

1. Необходимо четко и однозначно определить цели и задачи сертификации в области ТЗИ, изучив мировую практику в этом вопросе.
2. Определить конкретные направления деятельности, установить перечень и порядок разработки нормативно-методической документации, необходимых для проведения сертификационных испытаний.
3. Разработать действенный механизм постепенного перехода от системы разрешений к системе сертификации изделий, предназначенных для ТЗИ.
4. Провести расчет средних трудозатрат на выполнение основных операций при проведении сертификационных испытаний.

Почти все технические работы в области защиты информации связаны с проведением измерений и испытаний. Это относится к аттестации объектов, специальным исследованиям изделий, инструментальной проверке эффективности защиты, сертификационным испытаниям и измерениям и т. д. В ряде операций по ТЗИ технические средства применяются в качестве индикаторов, например средства поиска закладных устройств, что не является предметом расмотрения в настоящей статье.

Любой измерительный процесс связан с измерением физических величин. Для проведения таких измерений необходимо выполнять определенные требования – к аппаратуре, к климатическим и другим условиям, методологии, приемам работы, квалификации операторов и т. д. Всестороннюю готовность к проведению измерительных работ проверяют соответствующие подразделения Госстандарта Украины. По результатам этой проверки органам Госстандарта выдаются соответствующие аттестаты аккредитации, подтверждающие готовность к квалифицированному проведению измерительных работ. В области ТЗИ целый ряд измерений

проводится безотносительно к области применения. Характерными примерами являются измерения коэффициента экранирования экранного сооружения или коэффициента затухания сетевого фильтра. В этих случаях значения параметров затухания измеряются независимо от того, какое дальнейшее назначение изделия: для защиты устройств от внешних непреднамеренных помех или для защиты информации от утечки по техническим каналам. Вместе с тем в настоящее время в Украине существует два вида разрешения на проведение деятельности такого рода – лицензия на право проведения проверок средств ТЗИ и аккредитация Госстандарта Украины. Для чисто физических измерений, пример которых приведен выше, такой двойственный подход не допустим. С другой стороны, целый ряд специальных проверок и исследований включает особые требования, которые не могут быть предусмотрены Госстандартом. К этим особенностям относятся специальные начальные условия, отличные от лабораторных, режимы работы и тесты исследуемой аппаратуры, специальный порядок обработки результатов измерений, нормированные значения эффективности защиты и многое другое. Поэтому было бы неправильно противоставлять аккредитацию испытательных лабораторий и лицензирование в области ТЗИ.

Эти два направления должны разумно сочетаться. Для измерений общефизического характера, необходимо и достаточно иметь аккредитацию органов Госстандарта, не зависимо от назначения и функций предмета испытаний. Другое дело проведение специфических для защиты информации исследований и аттестаций. Они требуют специальных знаний и навыков, наличия нормативно-методической документации и т.д. Однако, и в этом случае, если эти работы сопровождаются измерениями, - они должны проводиться только аккредитованными в органах Госстандарта лабораториями.

Проблема нормирования труда при проведении типовых измерений и испытаний является актуальной так же, как при проведениии лицензионных и сертификационных работ.

Выводы:

1. Необходимо определить задачи и место измерений при проведении работ в области ТЗИ.
2. Определить перечень работ, содержащих измерения и испытания.
3. Провести расчет средних трудозатрат на выполнение основных операций при проведении измерений и испытаний в ходе выполнения работ различного назначения в области ТЗИ.

УДК 681.528.54

ПРОБЛЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЕКСПЕРТНИХ СИСТЕМ

Володимир Тарасенко, Антон Михайлюк, Дмитро Воробей
Національний Технічний Університет України «КПІ»

Анотація: **У доповіді надані рекомендації щодо особливостей забезпечення інформаційної безпеки експертних систем (ЕС). Розглянуто фактори, що визначають ці особливості, та наведено узагальнену класифікацію засобів інформаційної атаки на експертну систему. Запропоновано елементи структури системи безпеки, яка була б спроможна подолати нестандарті атаки на експертну систему.**

Summary: **The report provides recommendations concerning provisions of information security to the expert systems. The causes of such features have been considered and summarized in the classification of attack methods on expert system. The report presents the structural elements of such security system, which would enable the system to resist nonstandard attacks on it.**

Ключові слова: **експертна система, засоби інформаційної атаки, система безпеки,евристичний аналізатор.**

І Необхідність створення нової системи безпеки ЕС

В більшості існуючих ЕС реалізовані методи захисту програмного забезпечення (ПЗ) без урахування огляду на специфіку ЕС. Тобто застосовуються традиційні методи захисту, а саме, верифікація користувачів, створення резервних копій тощо.

Безперечно, така система безпеки (СБ) частково вирішує проблему захисту ЕС, але робить вона це з одним припущенням – атака на ЕС повинна бути ззовні. Це припущення може дорого коштувати ЕС, оскільки, атака може бути здійснена і власними засобами ЕС.

Інтелектуальні властивості ЕС є безперечним досягненням і перевагою над іншими системами, але з точки зору безпеки це одночасно є її ахіллесовою п’ятою. Тому виникає потреба в створенні нової СБ ЕС, яка б забезпечила надійну роботу з врахуванням особливостей ЕС.