Скоробогатова А.Е. Средства автоматизации процесса аттестации объектов информатизации // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 11(49) с. 61–67

Международный журнал информационных технологий и энергоэффективности

Сайт журнала: http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.8

СРЕДСТВА АВТОМАТИЗАЦИИ ПРОЦЕССА АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Скоробогатова А.Е.
ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ "МОСКОВСКИЙ ИНСТИТУТ ЭЛЕКТРОННОЙ ТЕХНИКИ", Москва, Россия, (124498, город Москва, город Зеленоград, пл. Шокина, д. 1), e-mail: sk-anastasi@yandex.ru

Для оценки соответствия объекта информатизации требованием по безопасности информации введена система аттестации. Аттестация объекта требует больших трудозатрат. Целью статьи является анализ возможности автоматизации процесса аттестации. Проведенный анализ показал, что существующие комплексы для проведения аттестационных испытаний позволяют автоматизировать проведение измерений и обработку их результатов, но не являются достаточными для подготовки отчетной документации. Дальнейшим направлением исследований является разработка средств автоматизации для оформления отчетной документации.

Ключевые слова. Автоматизация, аттестации, объект информатизации, безопасность информации, аттестационные испытания, автоматизированная система, защищаемое помещение.

AUTOMATION TOOLS FOR THE CERTIFICATION PROCESS OF INFORMATIZATION OBJECTS

Skorobogatova A.E.
"NATIONAL RESEARCH UNIVERSITY "MOSCOW INSTITUTE OF ELECTRONIC TECHNOLOGY", Moscow, Russia, (124498, Moscow, Zelenograd, Shokina Square, 1), e-mail: sk-anastasi@yandex.ru

To assess the compliance of the informatization object with the information security requirement, a certification system has been introduced. Certification of an object requires a lot of labor. The purpose of the article is to analyze the possibility of automating the certification process. The analysis showed that the existing complexes for conducting certification tests allow automating measurements and processing their results, but are not sufficient for the preparation of accounting documentation. A further area of research is the development of automation tools for registration of accounting documentation.

Keywords: Automation, certifications, the object of informatization, information security, certification tests, automated system, protected premises

В данной статье пойдет речь о средствах автоматизации процесса аттестации объектов информатизации. В настоящее время на территории Российской Федерации для оценки соответствия объекта информатизации (далее − ОИ) требованиям по безопасности информации введена система аттестации. Для ОИ (автоматизированные системы, защищаемые помещения), в которых циркулирует конфиденциальная информации или информация, составляющая государственную тайну, аттестация является обязательной. В ходе аттестационных испытаний проверяется соответствие объекта требованиям регулятора (ФСТЭК России). В случае выполнения всех требований, на объект выдается «Аттестат соответствия», без которого владелец ОИ не имеет права обрабатывать информацию

ограниченного доступа. Так как эта система существует не одно десятилетие, на данный момент появилось достаточно способов упростить и автоматизировать процесс аттестации ОИ. Совершенствуются как комплексы оборудования, так и программное обеспечение (далее – ПО), способные облегчить и ускорить работу по аттестации практически на всех этапах. Далее рассмотрим порядок аттестационных испытаний и приведем краткий обзор программно-аппаратных комплексов для проведения аттестационных испытаний, а также специального ПО.

По результатам статьи автор пришел к выводу, что существующие комплексы для проведения измерений, а также расчетное ПО позволяют значительно сократить время, затрачиваемое на проведение аттестационных испытаний. Направлением дальнейшего развития является создание более доступных и полных комплексов, позволяющих провести измерения и сразу получить результаты их обработки.

Порядок аттестационных испытаний ОИ

В аттестации ОИ в соответствии с нормативными документами участвуют заявитель (владелец объекта), орган по аттестации, а также ФСТЭК России. Каждая из сторон выполняет свои обязанности. Так, например, ФСТЭК России, являясь контролирующим органом, разрабатывает требования по безопасности и методики проведения измерений, проводит лицензирование органов по аттестации. Основной обязанностью заказчика (владельца объекта) является подготовка к аттестации, в частности разработка организационно-распорядительной документации. Орган по аттестации проводит аттестационные испытания и подготавливает отчетную документацию. Рассмотрим процесс аттестации со стороны непосредственно органа по аттестации (Рисунок 1).

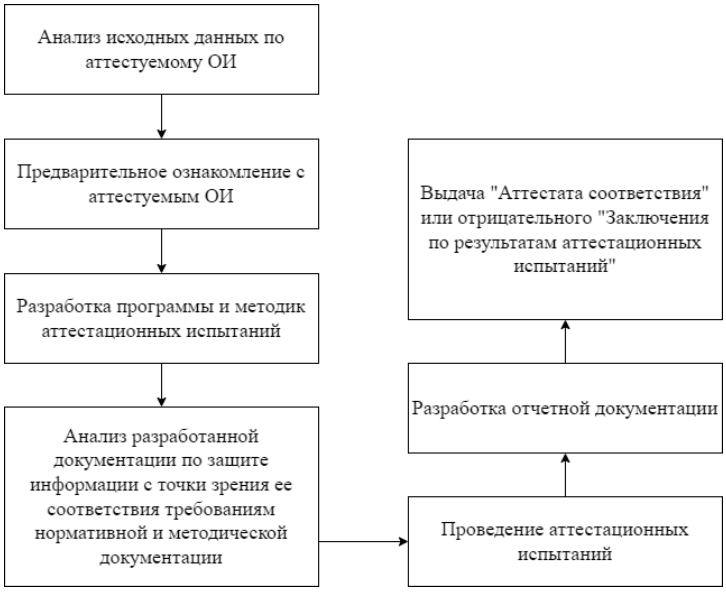

Рисунок 1 - Обобщенный алгоритм аттестации ОИ

Орган по аттестации разрабатывает «Программу и методики аттестационных испытаний», содержание этого документа описано в [1]. После согласования и подписания «Программы и методик» обеими сторонами (органом по аттестации и заявителем) проводится экспертный анализ объекта.

Анализ разработанной документации представляет собой проверку наличия всех требуемых документов [1] и соответствия их содержания требованиям регулятора. В частности, проверяется соответствие реального технологического процесса обработки информации тому, который описан в организационно-распорядительной документации, уточняются категория объекта и класс автоматизированной системы (далее – АС), уточняется состав объекта, проверяется заполнение журналов и др.

Аттестационные испытания АС представляют собой контроль выполнения требований по защите информации от несанкционированного доступа, побочных излучений и наводок, утечки информации за счет специальных устройств, встроенных в ОИ. Для защищаемого помещения аттестационные испытания включают контроль защищенности акустической (речевой) информации от утечки по техническим каналам [2].

Отчетная документация включает в себя протоколы аттестационных испытаний (далее – протоколы), заключение по результатам аттестационных испытаний (далее – заключение) и, в случае выдачи положительного заключения, аттестат соответствия.

Принято разделять оценку защищенности ОИ от утечки за счет несанкционированного доступа и от утечки по техническим каналам. В отношении выполнения требований от утечки информации по техническим каналам результаты оценки защищенности ОИ (до применения средств защиты информации) и эффективности защиты (после применения средств защиты информации) могут быть оформлены разными протоколами или объединены в один. Стоит отметить, что разработка протоколов включает в себя расчет значений, принятых за критерий оценки эффективности защиты. Как правило, для проведения этих расчетов используется специальное ПО.

Заключение содержит выводы о соответствии ОИ требованиям нормативной и методической документации и решение о возможности выдачи Аттестата соответствия.

Программно-аппаратные комплексы для проведения специальных исследований технических средств по ПЭМИН (побочные электромагнитные излучения и наводки)

Для оценки защищенности технических средств (далее – ТС) от утечки по техническим каналам проводятся лабораторные и объектовые специальные исследования. Лабораторные специальные исследования проводятся до аттестации ОИ, их результаты используются при выборе контрольных точек для проведения объектовых измерений и обработки результатов измерения реального затухания. Измерения затухания информационного сигнала проводятся в реальных условиях эксплуатации ТС.

В настоящее время существует несколько различных комплексов для проведения лабораторных специальных исследований ТС, которые в том числе возможно использовать и для оценки реального затухания, например, Навигатор-П5М (Рисунок 2а) на базе различных анализаторов спектра. Несмотря на то, что производители предусмотрели возможность использования комплекса и для проведения объектовых исследований, оборудование, входящее в состав [3] таких комплексов, не является достаточным. Как правило, комплекс собран на базе анализатора спектра с принимающими антеннами и не включает генератор сигналов и излучающие антенны.

Программно-аппаратный комплекс Зонд-М (Рисунок 2б), напротив, создан на базе генератора сигналов ГСУ-009-12000 и не имеет в своем составе [4] приемника (анализатор спектра с набором принимающих антенн).

а) б)

Рисунок 2 - Внешний вид комплексов а) Навигатор-П5М б) Зонд-М

Оба комплекса оснащены специальным ПО с возможностью дистанционного управления измерительным оборудованием. Также есть возможность подключения к ЭВМ, на котором установлено ПО устройств, не являющихся частью комплекса, и дистанционного управления этими устройствами.

Навигатор-П5М позволяет также обрабатывать результаты измерений, в специальное ПО входят расчетные модули для вычисления зон R2, r1, а также показателей эффективности защиты от утечки за счет ПЭМИН [2].

Зонд-М предназначен только для измерений. Для обработки результатов следует использовать расчетное ПО. Например, СПО "Легенда-18Р" [5], в которое входит три расчетных модуля: для вычисления зон R2, r1, показателей оценки защищенности и эффективности защиты информации от утечки за счет ПЭМИН.

Оба комплекса по своему составу не являются достаточными для измерения реального затухания. Навигатор-П5М является более универсальным, так как с его помощью возможно также проведение лабораторных специальных исследований и обработка результатов с помощью ПО. Однако для проведения аттестационных испытаний более подходящим является комплекс Зонд-М, так как после подготовки к проведению измерений практически не требует дальнейшего участия оператора. Все измерения проводятся в автоматическом режиме с помощью специального ПО. Этот комплекс позволяет упростить измерения и существенно сократить время, затрачиваемое на проведение исследований ТС.

Программно-аппаратные комплексы для проведения специальных исследований технических средств по акустическому и акустовибрационному каналам утечки информации

Для защищаемых помещений проводятся исследования по акустическому и акустовибрационному каналам утечки информации [2]. Для проведения измерений существует достаточно широкий выбор комплексов и приборов, например, Экофизика-110А, СКМ-8, комплекс «Смарт» (Рисунок 3).

а) б) с)

Рисунок 3 - а) Экофизика-110А б) СКМ-8 с) «Смарт»

С точки зрения автоматизации измерений и обработки результатов, наименее удобным вариантом является Экофизика-110А. Это прибор, объединяющий в себе функции шумомера, виброметра и анализатора спектра. При использовании данного прибора нет необходимости вручную записывать результаты измерений каждой контрольной точки, файлы результатов измерений переносятся на ПЭВМ и с помощью специального ПО Signal+ [6] преобразовываются в формат текстового документа. Также различные версии этого ПО позволяют обрабатывать результаты измерений, например, строить статистические диаграммы или спектрограмму сигнала. Однако для расчета показателя эффективности защиты (словесной разборчивости речи W) [2] потребуется другое ПО.

СКМ-8 позволяет не только записать результаты измерений, но и сразу после измерений в контрольной точки рассчитать W и сделать выводы об эффективности защиты информации. Соответственно, в специальном ПО СКМ-8, которое устанавливается на ЭВМ, есть возможность не только получить результаты измерений в формате текстового документа, но и протокол специальных исследований с расчетом показателя W и промежуточными вычислениями. Однако данный протокол не является полным и не может быть использован в качестве отчетной документации.

Комплекс «Смарт» учитывает все недостатки СКМ-8. Измерительные приборы сразу подключаются к ПЭВМ (как правило, используется ноутбук), параметры измеряемого сигнала, результаты измерений выводятся на монитор ПЭВМ. Протоколы измерений с расчетной частью можно получить сразу после измерений. По составу они не отличаются от протоколов, полученных с помощью СКМ-8, и также являются недостаточно полными.

На примере рассмотренных устройств можно увидеть эволюцию приборов и специального ПО для проведения аттестационных исследований защищаемого помещения. Измерительные приборы усложняют, оснащают встроенным расчетным ПО, в специальное ПО также добавляются новые функции, как расчетные, так и предназначенные для дистанционного управления измерительным оборудованием.

Заключение

Аттестацию объектов информатизации можно разделить на несколько этапов. Практически для каждого из них в настоящее время существуют средства автоматизации. Для аттестации АС существуют программно-аппаратные комплексы для измерения реального затухания и специальное расчетное ПО. Однако их выбор достаточно ограничен.

Комплексы для проведения аттестационных испытаний защищаемых помещений также позволяют автоматизировать измерения, насколько это возможно, с учетом установленного

порядка измерений. Также неоспоримым преимуществом является то, что часть таких комплексов позволяет получить протоколы с результатами измерений и рассчитанным показателем эффективности защиты.

Как отмечалось ранее, эти протоколы не являются достаточными. То же можно сказать и о протоколах, которые способно формировать ПО, предназначенное для обработки результатов измерений по ПЭМИН. Если вернуться к схеме на рисунке 1, можно увидеть, что процесс аттестации сопровождается большим количеством документов: организационно-распорядительная документация на ОИ, «Программа и методики аттестационных испытаний», протоколы, заключение и аттестат соответствия. Подготовка необходимых документов может занимать в среднем от одного до четырех рабочих дней в зависимости от индивидуальных особенностей ОИ. Можно выделить автоматизацию процесса подготовки отчетной документации как одно из дальнейших направлений исследований.

Существующие комплексы для проведения измерений, а также расчетное ПО позволяют значительно сократить время, затрачиваемое на проведение аттестационных испытаний. Направлением дальнейшего развития является создание более доступных и полных комплексов, позволяющих провести измерения и сразу получить результаты их обработки.

Список литературы

1. Приказ ФСТЭК России №77 от 29 апреля 2021г. «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»
2. Хорев, А.А. Техническая защита информации: учеб. пособие: В 3-х т. Т. 1: Технические каналы утечки информации / А. А. Хорев. - М. : НПЦ "Аналитика", 2008. – 436 с.
3. Навигатор-П5М URL: https://nelk.ru/catalog/sistemy_otsenki_zashchishchennosti_informatsii/programmno_apparatnye_kompleksy/navigator_p5m/ (дата обращения: 13.10.2024)
4. Зонд-М URL: https://nelk.ru/catalog/sistemy_otsenki_zashchishchennosti_informatsii/programmno_apparatnye_kompleksy/zond_m/ (дата обращения: 13.10.2024)
5. СПО «Легенда-18Р» URL: https://nppgamma.ru/catalog/programmnoe-obespechenie/legenda_18r/ (дата обращения: 13.10.2024)
6. Экофизика-110А. Комплекты URL: https://www.octava.info/ecophysica-110A/sets (дата обращения: 13.10.2024)

References

1. Order No. 77 of the FSTEC of Russia dated April 29, 2021 "On the disposal of the procedure for organizing and conducting work on certification of informatization facilities for compliance with the requirements for the protection of restricted access information that does not constitute a State Secret"
2. Khorev, A.A. Technical protection of information: textbook. manual: in 3 volumes. Vol. 1: Technical channels of information leakage / A. Khorev. - M.: NPC "Analytics", 2008. – 436 p.

3. Navigator-5 M URL: https://nelk.ru/catalog/sistemy_otsenki_zashchishchennosti_informatsii/programmno_apparatnye_kompleksy/navigator_p5m / (accessed: 10/13/2024)
4. Um-m URL: https://nelk.ru/catalog/sistemy_otsenki_zashchishchennosti_informatsii/programmno_apparatnye_kompleksy/zond_m / (accessed: 10/13/2024)
5. PDF "Legend-18P" URL: https://nppgamma.ru/catalog/programmnoe-obespechenie/legenda_18r / (accessed: 10/13/2024)
6. Ecophysics-110A. Included URL: https://www.octava.info/ecophysica-110A/sets (date of application: 13.10.2024)