РАЗДЕЛ XI. ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Вантеева А.Е.

Разработка метода проведения аттестации объектов информатизации

Волгоградский государственный университет

(Россия, Волгоград)

doi: 10.18411/trnio-01-2022-43

Аннотация

Данная статья посвящена вопросам защиты информации посредством аттестационных мероприятий по требованиям безопасности информации. Изучаются методы аттестации объектов информатизации, которые содержат в себе информацию ограниченного распространения.

Ключевые слова: информация, информационная безопасность, объект информатизации, информационная система, средство защиты информации, аттестация, организационно-распорядительная документация.

Abstract

This article is devoted to the issue of information protection through certification measures for information security requirements. Methods of certification of informatization objects they contain information of limited distribution.

Keywords: information, information security, objects of informatization, information system, means of information protection, certification, organizational and administrative documentation.

В процессе проведения аттестации объектов информатизации, являющиеся автоматизированными системами различных масштабов, можно условно выделить следующие категории получаемой и обрабатываемой информации:

- 1) Классификационные сведения об объекте информатизации (далее — ОИ):
 - тип конфиденциальной информации;
 - свойства защищаемой информации.
- 2) Перечень требований по защите информации при её обработке на ОИ;
- 3) Перечень актуальных угроз безопасности информации при её обработке на ОИ;
- 4) Сведения об ОИ, технических характеристиках, реализованных мерах по защите информации:
 - перечни ОТСС и ВТСС и их характеристики;
 - перечень помещений, схемы контролируемой зоны, расположения ОТСС и ВТСС;
 - перечень используемого прикладного и системного ПО;
 - меры по ограничению доступа, в том числе матрица доступа и другие организационные меры.
- 5) перечень организационно-распорядительной документации:
 - внутренняя документация по защите информации;
 - описание технологического процесса обработки информации;
 - технический паспорт ОИ;
 - модель угроз и нарушителя;
 - данные об используемых средствах защиты информации: наименование, версия, действующие сертификаты, формуляры, места установки.
- 6) данные о персонале:

- перечень лиц, участвующих в обработке конфиденциальной информации, их уровень допуска;
- сведения о лицах, ответственных за обеспечение безопасности информации. Оценка трудоемкости различных этапов аттестации приведена в табл. 1 из расчета, что трудоемкость всего процесса равна 100 %. Исходя из полученных данных видно, что существенного сокращения затрачиваемых на аттестацию ресурсов можно достичь за счет автоматизации этапов 2, 3, 4, 5, 6, 8. При этом программное обеспечение должно решать следующие проблемы:
- одновременно ведение нескольких проектов по аттестации;
- взаимодействие и импорт данных из ОИ различного масштаба, например через Active Directory;
- составление корректной модели угроз и нарушителя, учитывающей одновременно требования и ФСТЭК России, и ФСБ России [3]; 173
- актуализация сведений в соответствии с банком данных угроз ФСТЭК России;
- определение полного перечня требований по защите информации в зависимости классификации автоматизированной системы;
- формирование и доступ к единой базе нормативно-правовых актов по защите информации, в том числе по аттестации ОИ;
- ведение перечня используемых средств защиты информации и проверка их применимости в данном ОИ;
- получение актуальных сведений из реестра ФСТЭК России о сертифицированных средствах защиты информации;
- проверка соответствия ОИ требованиям по защите информации;
- проверка целостности используемых средств защиты информации;
- выпуск пакета аттестационной документации, в том числе программы и методики аттестационных испытаний.

Этапы аттестации объекта информатизации:

1. предаттестационное обследование;
2. оценка правильности категорирования;
3. определение требований по защите информации;
4. разработка программы и методик аттестационных испытаний;
5. проведение аттестационных испытаний;
6. анализ организационно-распорядительной документации;
7. оценка уровня защищенности;
8. подготовка аттестационной документации.

К сожалению, исследование имеющегося похожего российского и зарубежного программного обеспечения показал, что полноценных аналогов нет вследствие их ограниченности по функционалу либо поддержке стандартов и требований недостаточных для проведения аттестации [4]. Все это объясняет потребность разработки похожего программного обеспечения.

1. ФСТЭК России. Приказ № 17 от 11 февраля 2013 г. «Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
2. Барабанов А.В., Марков А.С., Цирлов В.Л. Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации // Спецтехника и связь. 2011. № 3. С. 48–52.
3. Зулькарнеев И.Р., Тякунов М.С., Кибардина Ю.А. Объединение методик создания модели нарушителя по требованиям ФСТЭК и ФСБ // Безопасность информационного пространства. Курган : РИЦ Курган. гос. ун-та, 2016. С. 22-25.
4. Бурькова Е.В. Задача оценки защищенности информационных систем персональных данных // Вестн. Чуваш. ун-та. 2016. № 1. С. 112–118.