Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ **ИНФОРМАТИКА И СИСТЕМЫ УПРАВЛЕНИЯ**

КАФЕДРА **КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ (ИУ6)**

НАПРАВЛЕНИЕ ПОДГОТОВКИ **09.04.01 Информатика и вычислительная техника**

МАГИСТЕРСКАЯ ПРОГРАММА **09.04.01/12 Интеллектуальный анализ больших данных в системах поддержки принятия решений.**

О Т Ч Е Т

по лабораторной работе № 5

Вариант № 9

Название: организационно-правовое обеспечение защиты информации

Дисциплина: Информационная безопасность автоматизированных систем

Студент ИУ6-31М (Группа) _____ (Подпись, дата) И.С. Марчук (И.О. Фамилия)

Преподаватель _____ (Подпись, дата) Д.А. Миков (И.О. Фамилия)

Москва, 2024

Цель: закрепление теоретических знаний в области правового обеспечения информационной безопасности.

Задание:

1. Изучить литературу и учебные материалы по теме (Конституция РФ, Доктрина информационной безопасности РФ и федеральные законы в области информационной безопасности, правовые режимы защиты информации).
2. Ответить на контрольные вопросы.
3. Оформить отчет, содержащий краткую информацию по контрольным вопросам.
4. Защитить практическую работу преподавателю (защита в виде опроса).

Ход работы

Я изучил учебные материалы по теме «законодательство РФ в области информационной безопасности».

Контрольные вопросы

1. Какая документация представляется органу по аттестации?

Для проведения аттестации объект информатизации должен быть подготовлен соответствующим образом. Органу по аттестации предоставляется:

- Технический паспорт объекта информатизации, включающий сведения о составе объекта, характеристиках технических и программных средств.
- Описание информационных процессов, включая технологические схемы обработки информации.
- Модель угроз безопасности информации, на основе которой строится система защиты.
- План мероприятий по защите информации.

- Документы, подтверждающие соответствие применяемых средств защиты информации (СЗИ) требованиям безопасности.
- Результаты предварительных обследований и проверок.

2. Что такое технический паспорт объекта информатизации и какие сведения о объекте он включает в себя?

Технический паспорт объекта информатизации — это документ, который содержит систематизированные сведения об объекте, необходимые для его идентификации и аттестации.

Он включает:

- Название и назначение объекта информатизации.
- Перечень аппаратных и программных средств, включая их характеристики.
- Топологию сетей и способы подключения к внешним системам.
- Уровни и объемы обрабатываемой информации, включая категории конфиденциальности.
- Перечень используемых средств защиты информации.

3. В чем состоит содержание специального исследования аттестуемого объекта информатизации?

Специальное исследование направлено на:

- Анализ уязвимостей объекта и оценки их влияния на безопасность информации.
- Оценку уровня угроз, моделируемых для конкретного объекта информатизации.
- Определение эффективности используемых СЗИ в реальных условиях.
- Подтверждение, что объект соответствует нормативным требованиям по защите информации.

4. Цель и содержание специальных обследований и проверок.

Цель - определить соответствие объекта требованиям нормативных документов в области защиты информации.

Содержание:

- Оценка организационных мер по защите информации.
- Проверка правильности установки, настройки и функционирования средств защиты информации.
- Анализ процессов обработки, передачи и хранения информации.
- Оценка соблюдения требований безопасности персоналом.

5. Проведение измерения и оценка уровней защищенности.

Включает:

- Проведение инструментальных измерений параметров защищенности.
- Тестирование СЗИ на устойчивость к известным и предполагаемым угрозам.
- Оценку возможности утечек информации по техническим каналам (например, электромагнитным).
- Анализ защищенности на уровне сетевой инфраструктуры.

6. Какие измерения дополнительно проводятся при использовании на объекте информатизации систем активной защиты?

При использовании систем активной защиты дополнительно измеряются:

- Эффективность активных методов обнаружения и предотвращения угроз (например, антивирусов, систем обнаружения вторжений).
- Влияние активных систем на производительность и корректность обработки информации.
- Устойчивость систем активной защиты к внешним атакам.

7. Содержание заключения аттестационной проверки объекта информатизации.

Заключение включает:

- Перечень проверенных параметров безопасности.
- Результаты всех проведенных исследований и испытаний.
- Выявленные недостатки и рекомендации по их устранению.

- Оценку соответствия объекта установленным требованиям.
- Резюме о возможности выдачи аттестата соответствия.

8. Содержание протокола аттестационных испытаний объекта информатизации.

Протокол содержит:

- Описание процедуры испытаний, включая методики и инструменты.
- Сведения о протестированных системах и подсистемах.
- Результаты тестирования, включая выявленные отклонения.
- Заключение о соответствии или несоответствии нормативным требованиям.

9. Содержание аттестата соответствия на объект информатизации.

Аттестат включает:

- Наименование объекта информатизации.
- Перечень категорий обрабатываемой информации.
- Перечень использованных СЗИ.
- Срок действия аттестата.
- Условия эксплуатации объекта.
- Реквизиты органа, выдавшего аттестат.

10. Ответственность за выполнение установленных условий функционирования аттестованного объекта информатизации.

Ответственность несет руководитель организации, эксплуатирующей объект, а также уполномоченные лица, назначенные приказом. Их задачи:

- Соблюдение требований аттестата.
- Организация мероприятий по поддержанию уровня защищенности.
- Обеспечение контроля за работоспособностью СЗИ.
- Принятие мер по устранению выявленных нарушений.

Вывод

Я изучил литературу и учебные материалы по теме (Конституция РФ, Доктрина информационной безопасности РФ и федеральные законы в области информационной безопасности, правовые режимы защиты информации). А также закрепил теоретические знания в области правового обеспечения информационной безопасности.