Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет прикладной информатики (ФПИН)

Лабораторная работа №2

по дисциплине: Основы кибербезопасности

Автор: доцент практики, кандидат технических наук

Кравчук Алексей Владимирович

Санкт-Петербург
2025

Тема занятия: Обоснованный выбор мер защиты информации для реализации в государственной информационной системе.

Цель работы.

Целью лабораторной работы № 2 является приобретение следующих навыков:

- работа с нормативными документами регуляторов и применением их для проектирования систем защиты информации в государственных информационных системах (ГИС) в части выбора мер защиты информации для их реализации в ГИС;
- обоснование выбора средств защиты информации, реализующих указанные меры защиты информации;

Краткие теоретические сведения.

Основные теоретические сведения представлены в следующих приказах и иных нормативных документах регулятора:

1. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.08.2024) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее — **Приказ № 17**).
2. «Методический документ. Меры защиты информации в государственных информационных системах», утв. ФСТЭК России 11.02.2014 г. (далее — **Методический документ**).

Приказ № 17 устанавливает требования к мерам защиты информации, содержащейся в государственных информационных системах (ГИС). В разделе III в п. 20 приведены 14 категорий мер (13 + DDoS в последней редакции). Порядок выбора мер защиты информации определен в п. 21 Приказа № 17.

Методический документ *детализирует* порядок выбора мер из Приказа № 17.

Вся лабораторная работа посвящена выбору мер защиты для выбранной слушателем ГИС.

Задание на практическую работу:

Теоретическая часть:

Изучить Приказ №17 ФСТЭК России, в частности:

- п. 13 пп.2 «Разработка системы защиты информации информационной системы»;

- раздел III «Требования к мерам защиты информации, содержащейся в информационной системе»;

- Приложение №2 «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы».

Изучить Методический документ, в частности:

- п. 2.2. Определение угроз безопасности информации в информационной системе.

- раздел 3. Содержание мер защиты информации в информационной системе (бегло).

Практическая часть:

1. Выбрать меры защиты для своей ГИС (рассмотренной в лабораторной работе № 1), руководствуясь рисунком «Общий порядок действий по выбору мер защиты информации для их реализации в информационной системе»:

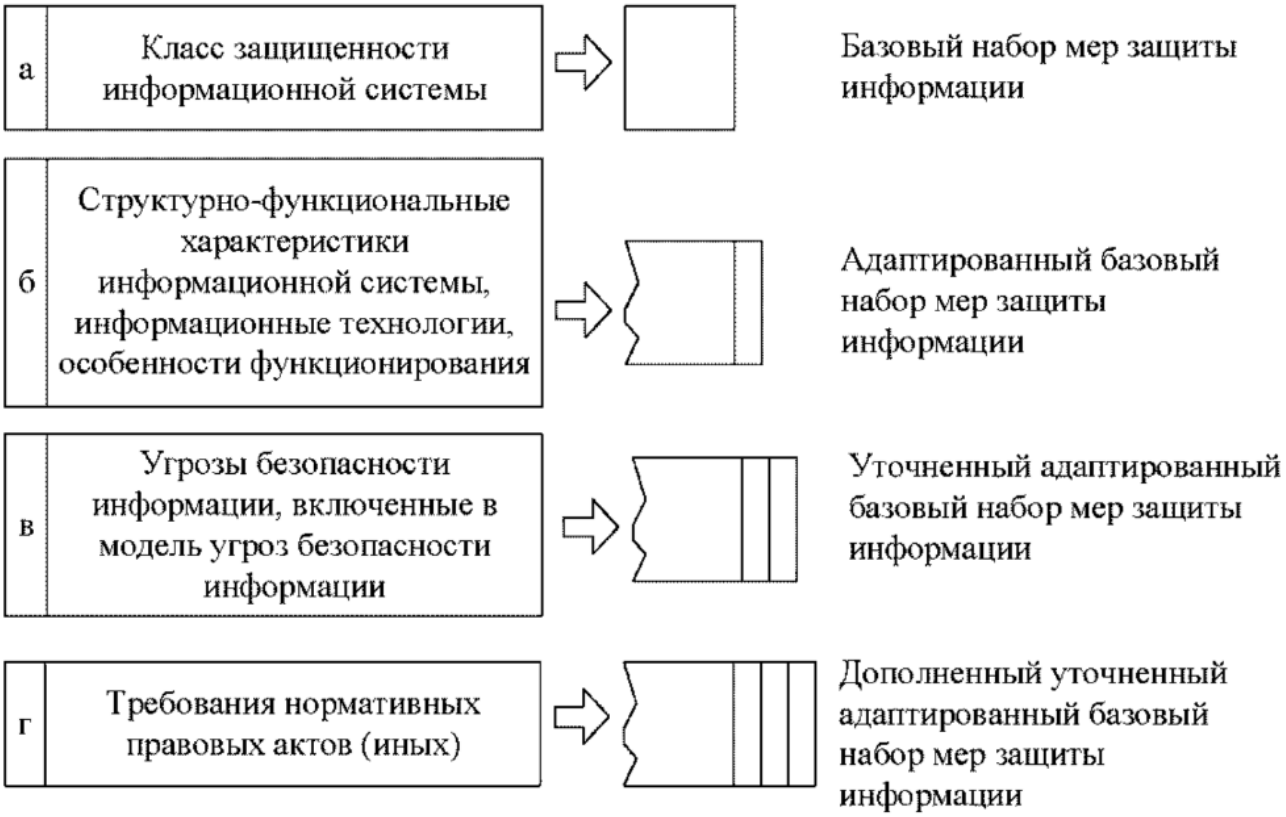

Рисунок - Общий порядок действий по выбору мер защиты информации для их реализации в информационной системе

1.1. Для формирования базового набора мер защиты информации используем Приложение №2 из Приказа №17. Если мера входит в базовый набор,

то это отмечено знаком «+». Выбираем *минимум 2 меры* из каждой категории. В результате выполнения этого пункта должна появиться таблица: «Базовый набор мер защиты информации» (Таблица № 1).

1.2. Для формирования адаптированного базового набора мер защиты информации необходимо из базового набора удалить меры, которые связаны с информационными технологиями, не используемыми в вашей ГИС (накладываем архитектуру вашей ГИС на базовый набор). В результате выполнения этого пункта должна появиться таблица: «Адаптированный базовый набор мер защиты информации» (Таблица № 2).

1.3. Уточненный адаптированный базовый набора мер защиты информации составляется на основе адаптированного базового набора мер таким образом, чтобы он нейтрализовывал все угрозы безопасности информации, включенные в Модель угроз для вашей ГИС, которую вы разработали в лабораторной работе № 1.

В результате выполнения этого пункта должна появиться таблица: «Уточненный адаптированный базовый набора мер защиты информации» (Таблица № 3).

1.4. Дополненный уточненный адаптированный базовый набора мер защиты информации строится чтобы удовлетворить требования о защите информации, установленных иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

Что это означает на практике? Поскольку в ГИС, как правило, хранятся персональные данные (ПД) пользователей, то должна быть учтена нормативная база для ИСПДн. Поскольку доступ к ГИС предоставляется пользователям удаленно посредством незащищенных каналов связи, то должна быть учтена нормативная база ФСБ в части КСЗИ. *Этот набор мер мы не формируем*.

2. Результатом выполнения лабораторной работы должна стать таблица, отражающая меры защиты информации, нейтрализующие УБИ, актуальные для вашей ГИС: Таблица 4. «Сопоставление мер защиты информации с актуальными УБИ». Пример этой таблицы приведен в файле «Таблица сопоставление МЕР.docx». В ней должны быть приведены не менее 20 УБИ (из первой лабораторной), каждая из которых закрыта определенными мерами из уточненного адаптированного базового набора мер.

3. Выбрать 3-5 (не менее) сертифицированных средств защиты информации (СрЗИ), в которых реализованы меры для защиты вашей ГИС (обычно одно СрЗИ «закрывает» несколько мер). Будет хорошо, если сможете подобрать что-то из потоковых антивирусных средств. Вспоминаем, что МЕРА должна быть реализована на всех уровнях модели OSI и на всех уровнях архитектурных решений защищаемой системы. То есть, если предусматриваем СрЗИ для гипервизора, то также нужно предусмотреть лёгкий агент, который ставится на гостевую (guest) операционную систему. Искать, какие конкретно меры

«закрываются» тем или иным СрЗИ можно в том числе по презентациям разработчика (обычно они прямо указывают, какие меры реализованы в их СрЗИ).

4. Ход работы, включая построение 4 таблиц и обоснованного выбора 3-5 сертифицированных СрЗИ, оформить в виде отчета о лабораторной работе.