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

Факультет прикладной информатики (ФПИН)

Лабораторная работа №1

по дисциплине: Основы кибербезопасности

Автор: доцент практики, кандидат технических наук

Кравчук Алексей Владимирович

Санкт-Петербург
2025

Тема занятия: Моделирование угроз безопасности информации в государственной информационной системе.

Цель работы.

- ознакомиться с нормативным документом ФСТЭК России «*Методический документ. **Методика** оценки угроз безопасности информации*» (утв. ФСТЭК России 05.02.2021)» (Далее – **Методика оценки УБИ**);
- освоить основополагающие принципы моделирования угроз безопасности информации;
- разработать Модель угроз безопасности информации для государственной информационной системы (ГИС) по выбору слушателя.

Краткие теоретические сведения.

Моделирование угроз — это этап проектирования системы защиты информации (СЗИ) для информационной системы (ИС), на котором определяются *актуальные угрозы* информационной безопасности (ИБ) для *обоснованного выбора мер защиты* информации (на следующем этапе) для защищаемых ИС.

Результатом моделирования угроз является *перечень актуальных угроз* для защищаемой информационной системы (ИС). Как правило, этот перечень составляется в табличном виде (и, в целом, всё, что связано с моделированием угроз представляется в табличном виде).

Для моделирования угроз ФСТЭК России разработана методика: «*Методический документ. Методика оценки угроз безопасности информации*» (утв. ФСТЭК России 05.02.2021)» (Далее – **Методика оценки УБИ**). Ключевое отличие от всех предыдущих методических документов регулятора – это **сценарный подход при определении актуальных угроз** (до этого использовался простой вероятностный математический аппарат).

ГОСТы и методические документы регуляторов носят рекомендательный характер, но только до тех пор, пока их обязательное использование не определено в нормативно-правовых документах более высокого уровня.

Так, 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**) определяет, что при проектировании системы защиты информации (далее - СЗИ) для ГИС, **должна быть** реализована «Модель угроз безопасности информации» (Далее - **Модель угроз**).

Модель угроз, разработанная вами в рамках Лабораторной работы № 1 будет использована в Лабораторной работе № 2 на этапе формирования уточненного адаптированного базового набора мер защиты информации (порядок

формирования наборов мер прописан в разделе II «*Методический документ. Меры защиты информации в государственных информационных системах*», утв. ФСТЭК России 11.02.2014 г. (далее – **Методический документ**). На рисунке ниже можно увидеть, что разработанная Модель угроз потребуется в лабораторной работе №2 при формировании уточненного адаптированного базового набора мер защиты информации.

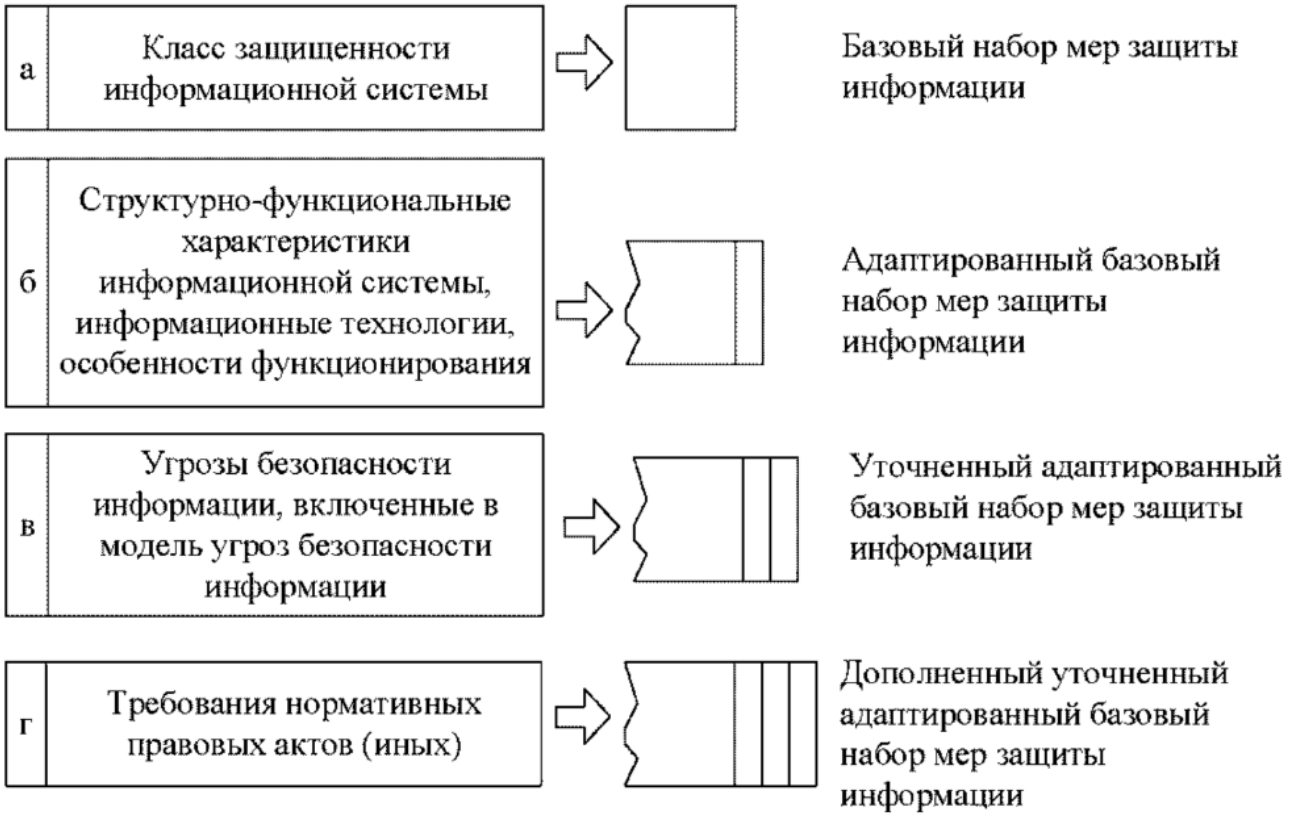

Рисунок - Общий порядок действий по выбору мер защиты информации для их реализации в информационной системе

СПРАВОЧНО: нужно понимать, что Модель угроз — это не нечто статичное. В «Методике оценки УБИ» в п. 2.14 указано, что «Модель УБИ должна поддерживаться в актуальном состоянии в процессе функционирования систем и сетей.»

Существуют онлайн-сервисы, которые позволяют автоматизировать процесс построения Модели угроз. Декларируется, что происходит АВТОМАТИЧЕСКОЕ обновление перечня угроз, когда появляются новые угрозы.

Примеры таких сервисов:

1) Цифровая модель угроз: https://digital-threat-model.ru/?utm_source=habr&utm_medium=article&utm_content=04-12-24

2) DocShell 4.0: https://docshell.ru/

Задание на практическую работу:

Теоретическая часть:

Ознакомиться со следующим нормативным документом ФСТЭК России: «Методический документ. Методика оценки угроз безопасности информации», утв. ФСТЭК России 05.02.2021 г.

На этом этапе от вас требуется (не более 20 минут на ознакомление):

- ознакомиться со структурой документа в целом;
- ознакомиться с Приложением 3 (Рекомендуемая структура модели угроз);
- ознакомиться с информацией, представляемой в табличном виде, начиная с Приложения 4.

Практическая часть:

ПРИМЕЧАНИЕ 1: Структуру ГИС вы придумываете в соответствии с уровнем ваших компетенций.

ПРИМЕЧАНИЕ 2: В случае откровенно безответственного отношения к описанию ГИС будут проблемы и с Лабораторной работой №2.

ПРИМЕЧАНИЕ 3 (Примеры действующих ГИС в России:**):**

- ГИС «Госуслуги» (ЕПГУ / ЕПГУ-ЕСИА), единый портал государственных и муниципальных услуг, предоставляет населению доступ к электронным госуслугам, ключевой элемент цифрового государства.
- ГИС «ЕГР ЗАГС», единый государственный реестр записей актов гражданского состояния, ведётся Минюстом РФ, хранит сведения о рождении, браке, разводе, смерти.
- ГИС «ЕГРН», единый государственный реестр недвижимости, ведётся Росреестром, содержит сведения о земельных участках и объектах недвижимости.
- ГИС «ГАС «Правосудие», государственная автоматизированная система «Правосудие», обеспечивает работу судов общей юрисдикции, ведение судебных дел в электронном виде.
- ГИС «ГАС «Выборы», система для обеспечения избирательного процесса, используется ЦИК России.

1. Придумать (в качестве прообраза можно взять существующую) и описать государственную информационную систему (ГИС) с учётом ограничений, накладываемых на класс защищенности ГИС *(класс защищенности задается преподавателем*). Классы защищенности рассмотрены в **Приказе №17** (п. 14.2 и Приложение №1).

1.1. Взять за основу структуру абстрактной информационной системы с клиент-серверной архитектурой (пока ещё не ГИС), представленную на рисунке 2.

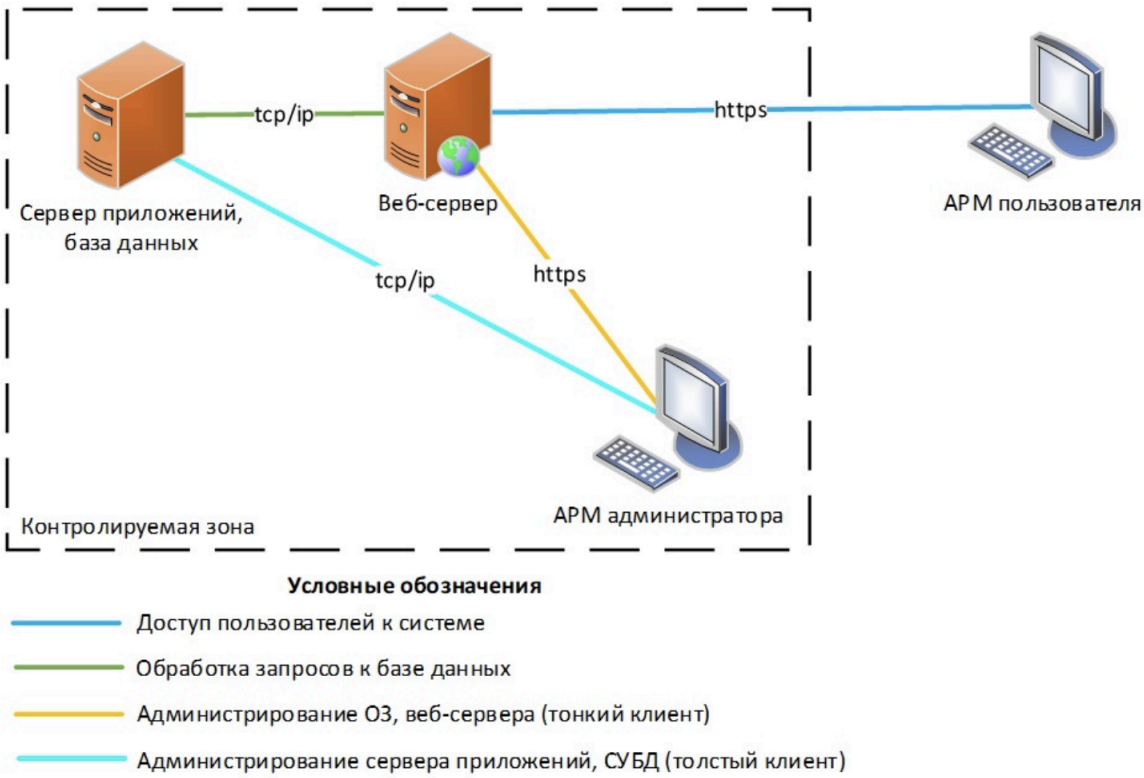

Рисунок 2. Типовая структура информационной системы

1.2. Провести простой поисковый анализ относительно типовой структуры ГИС. Как правило, ГИС:

- функционирует на базе уже существующей инфраструктуры центра обработки данных (ЦОД);
- функционирует с использованием средств виртуализации (физический сервер, гипервизор, гостевая ОС), – сразу думаем о том, что в дальнейшем обязательно должны быть рассмотрены угрозы, связанные с виртуализацией, гипервизорами и аутентификацией к интерфейсам удаленного доступа на всех уровнях архитектуры (включая «железо» - такие, как IPMI);
- содержит (*как минимум*) веб-сервер, который осуществляет доступ пользователей к веб-сайту и систему управления базами данных (СУБД), можно указать DMZ (демилитаризованную зону);
- подключена к другим ГИС.

1.3. Учесть следующие особенности (на примере портала «Госуслуги»):

- «Госуслуги» — это бренд, общее название для портала ЕПГУ и интегрированной с ним ЕСИА.

ЕСИА - Единая система идентификации и аутентификации;
ЕПГУ - Единый портал государственных и муниципальных услуг
ГИС ЕСИА используется не только для портала «Госуслуги», но и для доступа к десяткам других государственных сервисов. Соответственно, рекомендовано рассмотреть интеграцию проектируемой ГИС с ЕСИА и/или СМЭВ (Системой межведомственного электронного взаимодействия).

- ГИС содержит 2 контура.
  I) Внешний контур (гражданин ↔ портал):
  В целом, для базового сценария взаимодействия пользователя с ГИС не нужно использовать специализированные криптоалгоритмы и плагины к браузеру (клиентские СКЗИ). Но для некоторых сценариев нужно выполнять требования ФСБ и использовать HTTPS/TLS на основе российских криптоалгоритмов. Речь идет о сценариях, в которых требуется электронная (криптографическая) подпись.
  II) Внутренний контур, межведомственный обмен (портал ↔ ведомственные системы через СМЭВ). Здесь присутствуют обязательные шифрование канала связи и электронная подпись (ЭП) (реализуются средствами криптографической защиты (СКЗИ) с ГОСТ-алгоритмами шифрования, сертифицированными ФСБ, например, КриптоПро CSP, VipNet, SignalCom и др.).

2. Скачать файл «Заготовка Модель угроз.docx». В этом файле представлена реальная Модель угроз для информационной системы персональных данных (ИСПДН). Ваша задача адаптировать эту модель угроз с учетом особенностей вашей ГИС.

В файле «Заготовка Модель угроз.docx» некоторые места выделены желтым цветом – это примечания, вместо них нужно вставить релевантную информацию по вашей ГИС (либо удалить их после ознакомления, например: [!!!ТАБЛИЦА для ПДн, не для ГИСов!!!]).

Ваша задача – ознакомиться с документом и внести изменения в *Таблицу 12. Перечень рассматриваемых угроз безопасности информации и оценка их актуальности*. В таблице должны остаться только те строки, которые отвечают вашей ГИС. Для удобства работы вам нужно открыть банк данных угроз ФСТЭК России (БДУ ФСТЭК): https://bdu.fstec.ru/threat?size=100 , проанализировать угрозы и выбрать **НЕ МЕНЕЕ 20** САМЫХ АКТУАЛЬНЫХ (по вашему мнению) угроз, характерных для защищаемой ГИС (обязательно должны присутствовать угрозы, связанные с аутентификацией и виртуализацией).

В п. «9.3. Заключение о необходимости использования СКЗИ» рассмотрены вопросы, касающиеся применимости средств криптографической защиты информации (СКЗИ). Этот важный момент для себя отмечаем (потребуется во 2-ой лабораторной).

Результатом вашей работы будет являться *Таблица 16. Перечень актуальных угроз безопасности информации объекта информатизации.*

ПРИМЕЧАНИЕ: Перечень тактик и соответствующих им техник приведен в приложении 1 к модели угроз из «Заготовка Модель угроз.docx».