УДК 004.056:004.41

**Шегай Алексей Сергеевич,** магистрант,
Амурский государственный университет
Shegai Aleksey Sergeevich**,** Master's student,
Amur State University

**Никифорова Лариса Владимировна,**
канд. техн. наук, доцент,
Амурский государственный университет
Nikiforova Larisa Vladimirovna,
Candidate of Technical Sciences, Associate Professor,
Amur State University

# АНАЛИЗ ПРОЦЕДУРЫ КАТЕГОРИРОВАНИЯ И ОПРЕДЕЛЕНИЯ УРОВНЕЙ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПО ТРЕБОВАНИЯМ ФСТЭК РОССИИ
# ANALYSIS OF THE PROCEDURE FOR CATEGORIZING AND DETERMINING SECURITY LEVELS OF INFORMATION SYSTEMS ACCORDING TO FSTEC OF RUSSIA REQUIREMENTS

**Аннотация.** В статье рассмотрены методические аспекты классификации государственных информационных систем (ГИС) и определения уровней защищенности информационных систем персональных данных (ИСПДн). Систематизированы критерии категорирования и типы актуальных угроз безопасности на основе требований ФСТЭК России для корректного подбора средств защиты информации.

**Abstract.** The article discusses methodological aspects of classifying state information systems (SIS) and determining security levels of personal data information systems (PDIS). Categorization criteria and types of relevant security threats are systematized based on the requirements of FSTEC of Russia for the correct selection of information security tools.

**Ключевые слова:** Информационная безопасность, ФСТЭК России, уровни защищенности, персональные данные, ГИС, ИСПДн.

**Keywords:** Information security, FSTEC of Russia, security levels, personal data, SIS, PDIS.

Современная цифровая трансформация корпоративной среды выводит вопросы защиты конфиденциальных массивов на первый план. Формирование устойчивого периметра безопасности внутри организации неразрывно связано с государственным надзором и обязательной оценкой соответствия. Ключевым этапом здесь выступает комплексная аттестация объектов информатизации согласно ведомственным регламентам регулятора. Грамотное проектирование защитной архитектуры и рациональное распределение бюджета на приобретение сертифицированных программно-аппаратных инструментов требуют предварительной точной классификации контура. Ошибки при определении ранга объекта чреваты либо необоснованными финансовыми расходами, либо отказом в выдаче разрешительного документа.

Информационная система персональных данных (ИСПДн) представляет собой упорядоченную совокупность сведений о субъектах, обрабатываемых с применением вычислительной техники [1]. Действующие нормативы градируют подобные платформы на четыре базовых уровня защищенности, при этом высший ранг накладывает наиболее строгие требования по техническому контролю [2]. Процедура выявления оптимального режима безопасности опирается на поэтапный разбор трех независимых критериев.

На первом шаге анализируется специфика обрабатываемых массивов: выделяют специальные сведения (информация о здоровье, расовой принадлежности, убеждениях), биометрические маркеры, общедоступные базы и иные персональные записи. На втором этапе оценивается принадлежность субъектов (штатный персонал компании-оператора либо внешние контрагенты и клиенты) вкупе с масштабом выборки, где пороговым значением выступает отметка в сто тысяч записей. На третьем шаге классифицируются актуальные векторы угроз: первейший тип ассоциирован со скрытыми дефектами системного софта, второй обусловлен уязвимостями прикладных программ, а третий охватывает риски, не связанные с недокументированными функциями ПО. Сводная матрица параметров оценки приведена в таблице 1.

Таблица 1

Критерии определения уровня защищенности ИСПДн

| **Оцениваемый параметр** | **Допустимые значения / категории** |
|---|---|
| **Вид персональных данных** | Специальные (ИСПДн-С), биометрические (ИСПДн-Б), общедоступные (ИСПДн-О), иные (ИСПДн-И) |
| **Тип субъектов ПДн** | 1 тип – сотрудники оператора; 2 тип – лица, не являющиеся сотрудниками |
| **Объем данных (количество субъектов)** | Менее 100 000 субъектов; более 100 000 субъектов |
| **Тип актуальных угроз** | 1 тип (НДВ в системном ПО), 2 тип (НДВ в прикладном ПО), 3 тип (отсутствие НДВ) |

Государственные информационные платформы (ГИС) создаются для обеспечения управленческих функций органов власти и организации защищенного межведомственного документооборота [3]. Аудит подобных ресурсов предусматривает их распределение по трем эксплуатационным классам – от максимального (1К) до базового (3К). При ранжировании учитываются два фундаментальных показателя: географический охват инфраструктуры (федеральный, региональный или локальный уровень) и тяжесть последствий при компрометации информации (критический ущерб УЗ1 с остановкой работы ведомства, средний ущерб УЗ2 со сбоями процессов или незначительный ущерб УЗ3). Итоговая схема определения защищенности представлена в таблице 2.

Таблица 2

Матрица определения класса защищенности ГИС

| **Уровень значимости информации (степень ущерба)** | **Федеральный масштаб ИС** | **Региональный масштаб ИС** | **Объектовый масштаб ИС** |
|---|---|---|---|
| **Высокий ущерб (УЗ1)** | Класс 1К | Класс 1К | Класс 2К |
| **Средний ущерб (УЗ2)** | Класс 1К | Класс 2К | Класс 3К |
| **Низкий ущерб (УЗ3)** | Класс 2К | Класс 3К | Класс 3К |

Резюмируя вышесказанное, классификация информационных контуров выступает многомерной аналитической задачей, жестко регламентированной стандартами ФСТЭК России. Точное определение рангов защищенности закладывает необходимый методологический фундамент для последующей автоматизации подбора защитных решений, нивелируя риски человеческого фактора и ускоряя прохождение аттестационных проверок [4].

*Список литературы:*

1. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.

2. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК России от 18.02.2013 № 21 (зарегистрирован в Минюсте России 14.05.2013 № 28375). – Текст: электронный // Официальный сайт ФСТЭК России. – URL: https://fstec.ru (дата обращения: 24.10.2026).

3. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ ФСТЭК России от 11.02.2013 № 17 (зарегистрирован в Минюсте России 31.05.2013 № 28608). – Текст: электронный // Официальный сайт ФСТЭК России. – URL: https://fstec.ru (дата обращения: 29.10.2026).

4. Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну: Приказ ФСТЭК России от 29.04.2021 № 77 (зарегистрирован в Минюсте России 18.08.2021 № 64683). – Текст: электронный // Официальный сайт ФСТЭК России. – URL: https://fstec.ru (дата обращения: 05.11.2026).