УТВЕРЖДАЮ

Глава муниципального управления поселком

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / Иванов И.И. / «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2025 г.

АУДИТОРСКИЙ ОТЧЕТ О СООТВЕТСТВИИ ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Санкт-Петербург, 2025 г.**

**Содержание**

[I. Введение 2](#_Toc197453399)

[II. Нарушения нормативных требований 2](#_Toc197453400)

[III. Нарушения бизнес-требований 5](#_Toc197453401)

[IV. Рекомендации 6](#_Toc197453402)

[V. Заключение 6](#_Toc197453403)

# I. Введение

Настоящий отчет составлен по результатам аудита информационной безопасности (ИБ) муниципального учреждения. Цель аудита — проверить соблюдение требований нормативно-правовых актов (НПА), внутренних политик и бизнес-процессов.

# II. Нарушения нормативных требований

**a. Соблюдение требований в области КИИ**

| **Нарушаемое требование** | **Источник требования** | **Обоснование нарушения** | **Ответственность** |
| --- | --- | --- | --- |
| Создание систем безопасности значимых объектов | Приказ ФСТЭК №235 | Внедрение SIEM-системы не выполнено (состояние: "Не выполняется") | Руководитель службы ИБ |
| Информирование о компьютерных инцидентах | Приказ ФСБ №282 | Отсутствует регламент и интеграция с системами ФСБ (состояние: "Не выполняется") | Руководитель службы ИБ |
| Подготовка резервных каналов связи | Постановление Правительства РФ №743 | Тестирование отказоустойчивости не проведено (состояние: "Частично выполняется") | Технический директор |
| Регулярное тестирование систем | Приказ ФСТЭК №21 | Нагрузочное и пентест-тестирование не проводятся | Руководитель службы ИБ |
| Защита от вредоносного программного обеспечения. | Приказ ФСТЭК №239 | Не выполняется защита от ВПО | Руководитель службы ИБ |
| Физическая защита объектов КИИ. | Приказ ФСТЭК №239 | Физическая защита объектов КИИ (состояние: выполняется частично) | Технический директор |

**b. Соблюдение требований в области ПДн**

| **Нарушаемое требование** | **Источник требования** | **Обоснование нарушения** | **Ответственность** |
| --- | --- | --- | --- |
| Реализация криптографической защиты | Постановление Правительства РФ №1478 | Сертифицированные СКЗИ не установлены (состояние: "Не выполняется") | Руководитель IT-отдела |
| Резервное копирование данных | ФЗ-152, Приказ ФСТЭК №17 | Автоматическое резервное копирование не настроено (состояние: "Не выполняется") | Системный администратор |
| Ограничение доступа | ФЗ-152, Приказ ФСТЭК №17 | Ограничение доступа к ПДн(состояние: "Выполняется частично") | Ответственный за обработку ПДн |
| Классификация ИСПДн | Приказ ФСТЭК №17 | Проведение классификации ИСПДн (состояние: "Не выполняется") | Руководитель службы ИБ |

**c. Соблюдение требований в области подключения к ГИС**

| **Нарушаемое требование** | **Источник требования** | **Обоснование нарушения** | **Ответственность** |
| --- | --- | --- | --- |
| Использование сертифицированных СЗИ | Приказ ФСТЭК №17 | Применяются несертифицированные межсетевые экраны (состояние: "Не выполняется") | Руководитель отдела ИБ |
| Внедрение СУИБ | ГОСТ Р 56939-2016 | Система управления информационной безопасностью отсутствует (состояние: "Не выполняется") | Руководитель службы ИБ |
| Регулярное обновление ПО | Приказ ФСТЭК №21 | Обновления проводятся с задержками (состояние: "Выполняется частично") | Системный администратор |

# III. Нарушения бизнес-требований

| **Нарушаемое требование** | **Источник требования (политика)** | **Обоснование нарушения** | **Недопустимые события / Финансовые потери** |
| --- | --- | --- | --- |
| Обеспечение доступности АСУГТ | Политика ИБ | Отказ системы управления транспортом может привести к остановке движения | Убытки из-за простоев транспорта: ~500 тыс. руб./час |
| Отсутствие анализа причин инцидентов | Политика ИБ | Повторные инциденты приводят к увеличению времени простоя систем. | Убытки из-за повторных сбоев: ~200 тыс. руб./инцидент. |
| Недостаточное обучение сотрудников | Внутренний регламент ИБ | Риск ошибок при обработке ПДн и реагировании на угрозы. | Штрафы за нарушения ФЗ-152: до 300 тыс. руб |
| Превышение времени восстановления ЭПГ | Политика ИБ | Время восстановления ЭПГ превышает 1 час | Простой электронной приемной: снижение доверия граждан |
| Неустраненные уязвимости | Политика ИБ | Устранено менее 90% уязвимостей | Риск атак: утечка данных (~500 тыс. руб. штрафов) |
| Отсутствие резервного копирования | Политика ИБ | Резервное копирование не настроено | Потеря данных о маршрутах транспорта: простой (~700 тыс. руб./час) |
| Недостаточная защита от DDoS | Политика ИБ | Отсутствие NGFW и пентестинга | Остановка ЭПГ: невозможность подачи обращений (~300 тыс. руб./сутки) |

# IV. Рекомендации

**Для нормативных требований:**

1. **Внедрение SIEM-системы** (Solar JSOC) для выполнения требований Приказа ФСТЭК №235. Срок: 6 месяцев.
2. **Разработка регламента информирования ФСБ** о киберинцидентах и интеграция с их системами. Срок: 3 месяца.
3. **Установка сертифицированных СКЗИ** (например, «КриптоПро») для шифрования ПДн. Срок: 5 месяцев.
4. **Настройка автоматического резервного копирования** с шифрованием данных. Срок: 2 месяца.
5. **Проведение пентестинга** интерфейса ЭПГ и внедрение NGFW для защиты от DDoS. Проведение пентестов и нагрузочного тестирования АСУГТ и ЭПГ каждые 6 месяцев. Срок: 3 месяца).
6. **Внедрение анализа инцидентов.** Создание рабочей группы (ИБ-специалисты + юристы) для детального разбора каждого инцидента и разработки корректирующих мер. Срок: 2 месяца).

**Для бизнес-требований:**

1. **Разработка плана аварийного восстановления** для АСУГТ с тестированием отказоустойчивости. Срок: 3 месяца.
2. **Обучение сотрудников** по противодействию фишингу и DDoS-атакам. Срок: ежеквартально. Включение обязательных тренингов по противодействию фишингу и DDoS-атакам для всех сотрудников, работающих с КИИ и ПДн
3. **Проведение независимого аудита ПДн** для минимизации риска штрафов. Срок: 1 месяц.
4. Оптимизировать процедуры восстановления ЭПГ (срок: 3 месяца).
5. Устранить 100% критических уязвимостей в АСУГТ (срок: 6 месяцев).

# V. Заключение

Аудит выявил системные нарушения в области КИИ, ПДн и бизнес-процессов. Основные причины:

* Недостаточное финансирование ИБ-мероприятий.
* Отсутствие регулярного контроля выполнения требований.

**Рекомендации:**

1. Утвердить бюджет на внедрение SIEM-системы и сертифицированных СЗИ.
2. Назначить ответственных за выполнение рекомендаций и ежеквартальную отчетность.

**Разработчик отчета:**

[ФИО аудитора]

**Согласовано:**

[ФИО руководителя ОИБ]