# Организация внутренних аудитов объектов КИИ

Константин Саматов

# Аудит ИБ

Аудит ИБ - форма независимой оценки состояния информационной безопасности объекта аудита (информационная система, автоматизированная система, организация как объект защиты в целом и т.п.) на соответствие заданным критериям (например, требованиям действующего законодательства или принятых корпоративных стандартов, отсутствия уязвимостей, содержащиеся в банке данных угроз безопасности информации и т.п.).

ГОСТ Р ИСО/МЭК 27007-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности»

ГОСТ Р ИСО 19011-2012 «Руководящие указания по аудиту систем менеджмента»

# Виды аудита ИБ

1. Первичный (перед созданием СБ ЗОКИИ)
2. Периодический (в процессе функционирования СБ ЗОКИИ)
3. Внутренний (раздел V Состава мер… пр. ФСТЭК № 239, п. 35-36 Требований к СБ ЗОКИИ, пр. ФСТЭК № 235)
4. Внешний (раздел V Состава мер… пр. ФСТЭК № 239, п. 35-36 Требований к СБ ЗОКИИ, пр. ФСТЭК № 235)
5. Комплаенс (соответствие требованиям НПА и стандартов)
6. Технический аудит (в т.ч. с тестированием на проникновение)

# Первичный аудит ИБ (перед созданием СБ ЗОКИИ)

1

**Цель** - определение тех мер по защите информации, которые уже приняты в отношении данного объекта КИИ, и тех, которые необходимо будет реализовать в процессе создания СБ ЗОКИИ

2

Что изучается?

1. Силы обеспечения информационной безопасности, т.е. кто и как обеспечивает информационную безопасность в организации.
2. Средства обеспечения информационной безопасности ЗОКИИ, т.е. какие программные и (или) программно-аппаратные средства используются для обеспечения информационной безопасности ЗОКИИ.
3. Организационно-распорядительная документация, т.е. какая документация в части безопасности информации имеется в организации и какие вопросы она регламентирует.
4. Организация работ по обеспечению информационной безопасности:

• каким образом организован процесс планирования и разработки мероприятий по обеспечению информационной безопасности, чем он регламентирован;
• как осуществляется реализация мероприятий по информационной безопасности;
• каким образом осуществляется контроль за соблюдением требований в области информационной безопасности и контроль текущего уровня безопасности;
• как оценивается уровень зрелости процессов обеспечения информационной безопасности и осуществляется их совершенствование.

# Первичный аудит ИБ (перед созданием СБ ЗОКИИ)

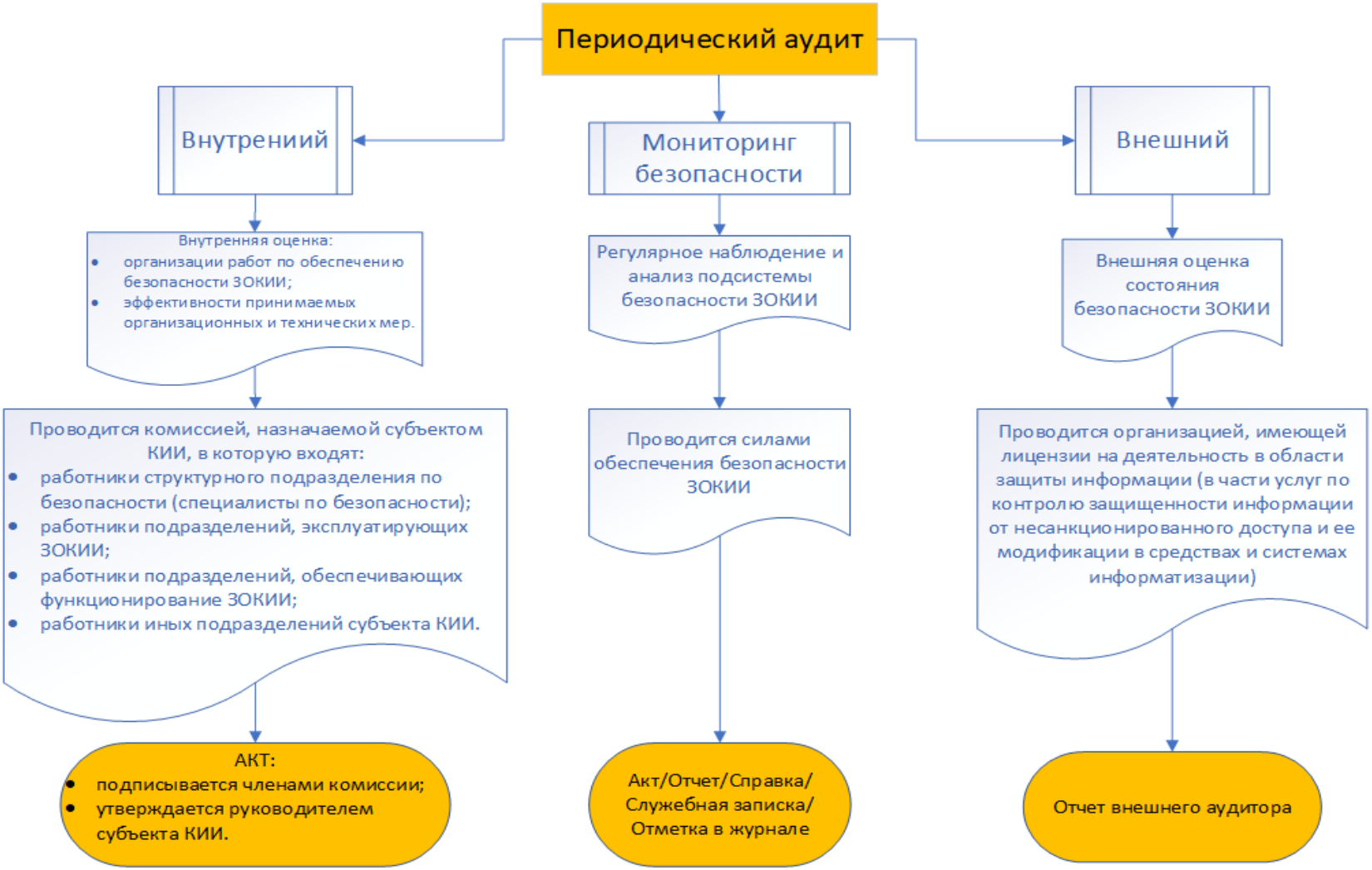
| Обозначение и номер меры | Меры обеспечения безопасности значимого объекта | Объект КИИ № 1 ИС … | | Объект КИИ № 2 АСУТП …. | | Объект КИИ № 3 АСУТП … | |
|---|---|---|---|---|---|---|---|
| | | КЗ* | Как реализуется? | КЗ | Как реализуется? | КЗ | Как реализуется? |
| | | 3 | | 2 | | 1 | |
| УПД.0 | Регламентация правил и процедур управления доступом | + | Утвержден регламент управления доступом (рег. № … от …) | + | Утвержден регламент управления доступом (рег. № … от …) | + | Утвержден регламент управления доступом (рег. № … от …) |
| *** | | | | | | | |
| АВЗ.1 | Реализация антивирусной защиты | + | На рабочих станциях и серверах установлено антивирусное программное средство … (сертификат …) | - | Антивирусное программное обеспечение не используется в виду ограничений производителя АСУТП, систем изолирована не имеет выходов в сети связи общего пользования | + | На рабочих станциях и серверах используется согласованное с производителем антивирусное программное средство … (сертификат…) |
| *** | | | | | | | |
| УПД.9 | Ограничение числа параллельных сеансов доступа | - | Не применимо | - | Не применимо | + | Штатными средствами SCADA системы предусмотрена возможность задавать ограничения на число параллельных (одновременных) сеансов (сессий)… |
| *** | | | | | | | |
| ИПО.3 | Проведение практических занятий с персоналом по правилам безопасной работы | - | Не применимо | + | Проведение занятий с персоналом по правилам безопасной работы не осуществляется. Требуется регламентация и реализация данного процесса | + | Проведение занятий с персоналом по правилам безопасной работы не осуществляется. Требуется регламентация и реализация данного процесса |

*КЗ – категория значимости

3

**Результат:** понимание того, какая часть обязательных мер по обеспечению безопасности ЗОКИИ уже реализована, а какая требует реализации в процессе создания СБ ЗОКИИ, какая часть мер может быть «закрыта» встроенными средствами защита, а для какой потребуется применение наложенных.

# Периодический аудит ИБ



# Почему внутренний аудит?

1. Обязательный (требования приказов ФСТЭК России № 235 и 239)
2. При внешнем аудите ТРЗ Заказчика и Подрядчика ≈ 50/50
3. Отсутствие компетенций у Подрядчиков
4. Возможность привлечения внешних (действительно) экспертов
5. Правильное и полное понимание текущей ситуации на выходе

# Организация внутреннего аудита ИБ

**1 Этап. Инициация аудита**

- создание комиссии;
- определение целей, границ проведения аудита, критериев;
- разработка плана проведения аудита;
- выпуск приказа о проведении внутреннего аудита.

**2 Этап. Проведение аудита**

- распределение задач между членами комиссии;
- проведение установочного совещания;
- проведение интервьюирования специалистов;
- проведение инструментального обследования;
- проведение тестирования на проникновения;
- анализ и верификация собранной в рамках мероприятий информации.

**3 Этап. Завершение аудита**

- подготовка акта по итогам аудита;
- согласование и утверждение акта;
- разработка плана мероприятий по устранению выявленных недостатков.

# Спасибо за внимание!

Константин Саматов