УЦСБ SOC

МОНИТОРИНГ ИБ ПО-НОВОМУ?

Приказ №117 и ГОСТ Р 59547-2021: разбор требований и практика применения



WHOAREWE

Модератор



КОНСТАНТИН МУШОВЕЦ

Директор
УЦСБ SOC

Спикер



МАРИНА ЖУКОВА

Сервисный менеджер
УЦСБ SOC

Спикер



ВАДИМ ШТЫРЕВ

Старший аналитик
УЦСБ SOC

Эксперт



ЕЛЕНА ЗАВОДОВА

Руководитель направления аудитов и соответствия требованиям ИБ, УЦСБ

О ЧЕМ ПОГОВОРИМ

01 Ключевые требования Приказа ФСТЭК России №117 от 11.04.2025

02 ГОСТ Р 59547-2021 как инструмент соответствия

03 Практическая реализация требований по мониторингу ИБ в SOC

04 Спецпредложения для участников вебинара

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ

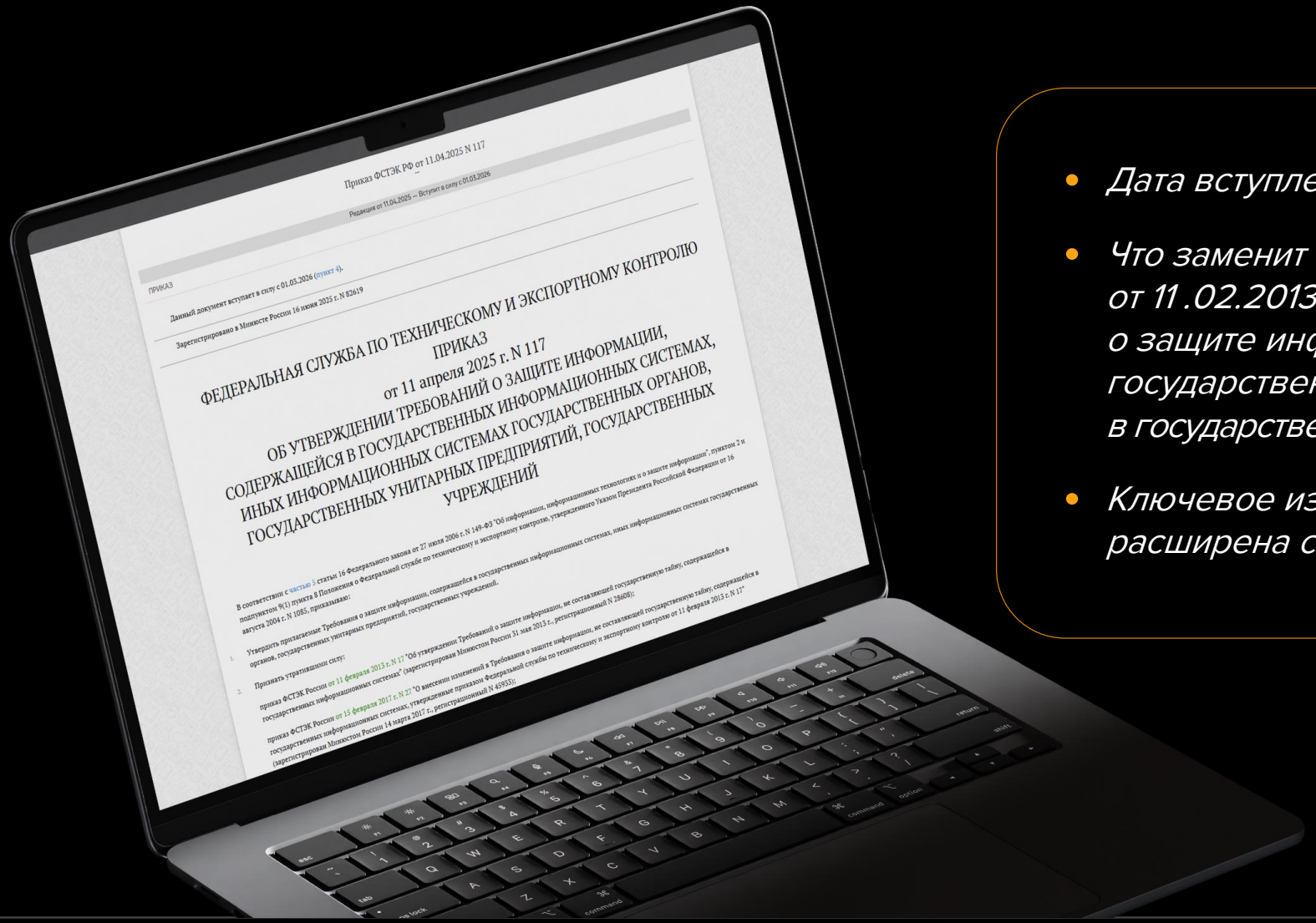
УЦСБ SOC

ПРИКАЗ ФСТЭК РОССИИ

№117 ОТ 11.04.2025

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ | УЦСБ SOC

ПРИКАЗ ФСТЭК РОССИИ №117 ОТ 11.04.2025



- *Дата вступления в силу — 1 марта 2026*
- *Что заменит — Приказ ФСТЭК России N° 17 от 11.02.2013 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»*
- *Ключевое изменение — существенно расширена сфера регулирования*

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ | УЦСБ SOC

АНАЛИЗ ПАРАМЕТРОВ МОНИТОРИНГА ИЗ ПРИКАЗА №117

Формирование отчетности в адрес ФСТЭК России

- Проведение регулярных оценок:
  защищенности КЗИ — раз в полгода,
  уровня зрелости ПЗИ — раз в два года
- Оперативно информировать ФСТЭК России о выявленных уязвимостях — в течение 5 рабочих дней после обнаружения
- Отчет о результатах мониторинга — один раз в год

Требования к кадрам

- Назначено ответственное лицо, выполняющее обязанности специалиста по ИБ

или

- Создан отдел ИБ, в котором не менее 30% сотрудников с базовым образованием или профессиональной переподготовкой

Требования по применению ИИ

При использовании в информационных системах искусственного интеллекта или сервисов на основе искусственного интеллекта должны применяться доверенные технологии искусственного интеллекта или их компоненты

Обязательная аттестация для государственных информационных систем

- Действующие аттестаты соответствия сохраняются
- Если была модернизация системы, аттестовываться нужно будет уже по новым требованиям

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ | УЦСБ SOC

ДЛЯ КОГО ВАЖЕН ДАННЫЙ ПРИКАЗ?

01

ИС государственных органов: федеральных и региональных

02

ИС государственных унитарных предприятий (ГУП) и учреждений

03

Муниципальные информационные системы

ВЫВОД

Все организации, связанные с государственным управлением, должны будут привести свои ИС в соответствие с новыми требованиями

ОБЯЗАТЕЛЬНЫЙ ПЕРЕЧЕНЬ МЕР

- Идентификация и аутентификация
- Управление доступом
- Регистрация событий безопасности
- Защита виртуализации и облачных вычислений
- Защита технологий контейнерных сред и их оркестрации
- Защита сервисов электронной почты
- Защита веб-технологий
- Защита программных интерфейсов взаимодействия приложений
- Защита конечных устройств

- Защита мобильных устройств
- Защита технологий интернета вещей
- Защита точек беспроводного доступа
- Антивирусная защита
- Обнаружение и предотвращение вторжений на сетевом уровне — *мониторинг*
- Сегментация и межсетевое экранирование
- Защита от компьютерных атак, направленных на отказ в обслуживании — *мониторинг*
- Защита каналов передачи данных и сетевого взаимодействия

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ

УЦСБ SOC

ГОСТ Р 59547-2021
КАК ИНСТРУМЕНТ СООТВЕТСТВИЯ И ПРАКТИКА УЦСБ SOC

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ | УЦСБ SOC

КТО ВХОДИТ В SOC ПРИ ОБЕСПЕЧЕНИИ МОНИТОРИНГА ИБ 24/7

П. 5.5.4 ГОСТ Р 59547-2021



КОМПЕТЕНЦИИ ИСПОЛНИТЕЛЕЙ ЭТИХ РОЛЕЙ ПОЛНОСТЬЮ СООТВЕТСТВУЮТ ТРЕБОВАНИЯМ РАЗДЕЛА II П.20 ПРИКАЗА №117

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ | УЦСБ SOC

АНАЛИЗ ПАРАМЕТРОВ МОНИТОРИНГА ИЗ ПРИКАЗА №117

Формирование отчетности в адрес ФСТЭК России

- Проведение регулярных оценок:
  защищенности КЗИ — **раз в полгода**,
  уровня зрелости ПЗИ — **раз в два года**
- Оперативно информировать ФСТЭК России
  о выявленных уязвимостях — в течение **5 рабочих дней** после обнаружения
- Отчет о результатах мониторинга — **один раз в год**

Требования к кадрам

- Назначено ответственное лицо, выполняющее обязанности специалиста по ИБ

или

- Создан отдел ИБ, в котором не менее 30% сотрудников с базовым образованием или профессиональной переподготовкой

Требования по применению ИИ

При использовании в информационных системах искусственного интеллекта или сервисов на основе искусственного интеллекта должны применяться доверенные технологии искусственного интеллекта или их компоненты

Обязательная аттестация для государственных информационных систем

- Действующие аттестаты соответствия сохраняются
- Если была модернизация системы, аттестовываться нужно будет уже по новым требованиям

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ | УЦСБ SOC

РЕАЛИЗАЦИЯ МЕРОПРИЯТИЙ ПО МОНИТОРИНГУ ИБ

П.4.2 ГОСТ Р 59547-2021

Мероприятий анализа и оценки функционирования систем ЗИ информационных (автоматизированных) систем

- Средства мониторинга состояния, например, Zabbix

Мероприятия контроля (анализа) защищенности информации

- VM

Мероприятия анализа событий безопасности и иных данных мониторинга

- SIEM
- NTA
- EDR
- NGFW
- WAF
- узконаправленные средства мониторинга

Мероприятия периодического анализа изменения угроз безопасности информации в информационных (автоматизированных) системах, возникающих в ходе эксплуатации

- Threat Intelligence
- Threat Hunting

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ | УЦСБ SOC

АНАЛИЗ ПАРАМЕТРОВ МОНИТОРИНГА ИЗ ПРИКАЗА №117

Формирование отчетности в адрес ФСТЭК России

- Проведение регулярных оценок:
  защищенности КЗИ — **раз в полгода**,
  уровня зрелости ПЗИ — **раз в два года**
- Оперативно информировать ФСТЭК России о выявленных уязвимостях — в течение **5 рабочих дней** после обнаружения
- Отчет о результатах мониторинга — **один раз в год**

Требования к кадрам

- Назначено ответственное лицо, выполняющее обязанности специалиста по ИБ

или

- Создан отдел ИБ, в котором не менее 30% сотрудников с базовым образованием или профессиональной переподготовкой

Требования по применению ИИ

При использовании в информационных системах искусственного интеллекта или сервисов на основе искусственного интеллекта должны применяться доверенные технологии искусственного интеллекта или их компоненты

Обязательная аттестация для государственных информационных систем

- Действующие аттестаты соответствия сохраняются
- Если была модернизация системы, аттестовываться нужно будет уже по новым требованиям

ОБЪЕКТЫ МОНИТОРИНГА

П.4.3 ГОСТ Р 59547-2021

- АРМ
- СКЗИ
- Серверы
- Базы данных с ПДн
- Приложения для обработки ПДн
- Внутренние сети (LAN)
- СЗИ
- САВЗ
- Сетевое оборудование
- Сервисы аутентификации
- Сервера резервного копирования
- Иное

УРОВНИ МОНИТОРИНГА

П.4.4 ГОСТ Р 59547-2021

01

Источник данных

+ П.5.1 ГОСТ о требованиях к источникам

02

Сбор данных

+ П.5.2 ГОСТ о требованиях к сбору

03

Хранение и обработка

+ П.5.3 ГОСТ о требованиях к хранению, обработке и агрегированию

04

Представление

+ п.5.4 ГОСТ о требованиях к представлению

О ЧЕМ ЕЩЕ СТОИТ ЗАДУМАТЬСЯ ЗАРАНЕЕ ДЛЯ ОБЕСПЕЧЕНИЯ МОНИТОРИНГА ИБ?

П.4.6 ГОСТ Р 59547-2021

Представление результатов анализа данных мониторинга в режиме времени, близком к реальному

Возможность формирования различных отчетов по результатам мониторинга ИБ

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ | УЦСБ SOC

АНАЛИЗ ПАРАМЕТРОВ МОНИТОРИНГА ИЗ ПРИКАЗА №117

Формирование отчетности в адрес ФСТЭК России

- Проведение регулярных оценок: защищенности КЗИ — раз в полгода, уровня зрелости ПЗИ — раз в два года
- Оперативно информировать ФСТЭК России о выявленных уязвимостях — в течение 5 рабочих дней после обнаружения
- Отчет о результатах мониторинга — один раз в год

Требования к кадрам

- Назначено ответственное лицо, выполняющее обязанности специалиста по ИБ

или

- Создан отдел ИБ, в котором не менее 30% сотрудников с базовым образованием или профессиональной переподготовкой

Требования по применению ИИ

При использовании в информационных системах искусственного интеллекта или сервисов на основе искусственного интеллекта должны применяться доверенные технологии искусственного интеллекта или их компоненты

Обязательная аттестация для государственных информационных систем

- Действующие аттестаты соответствия сохраняются
- Если была модернизация системы, аттестовываться нужно будет уже по новым требованиям

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ

УЦСБ SOC

СПЕЦПРЕДЛОЖЕНИЕ
ДЛЯ УЧАСТНИКОВ ВЕБИНАРА

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ | УЦСБ SOC

ТАРИФ SOC ДЛЯ ГОССТРУКТУР

ВЫГОДНЫЙ МОНИТОРИНГ ИБ НА 12 МЕСЯЦЕВ

Стоимость предложения*

2,4 млн рублей

Параметры услуги

До 200 EPS или 100 активов

Хранение событий

90 дней

Модель подключения

Облачная модель (SOCaaS)

Ограничения

Только для новых заказчиков УЦСБ SOC

Продление

+20% к стоимости тарифа

Вам нужно обсудить другие параметры?

Оставьте заявку и получите персональное предложение

*Указаны цены без учета НДС

СОСТАВ УСЛУГ

Сервис предназначен для оперативной постановки на мониторинг ИБ ваших критичных активов, а также закрытия факта мониторинга перед регулирующими органами

УСЛУГИ МОНИТОРИНГА ИБ	SOC ДЛЯ ГОССТРУКТУР	СТАНДАРТ
Мониторинг, выявление и анализ инцидентов ИБ	Да	Да
Выдача рекомендаций, сопровождение до момента устранения инцидента	Да	Да
Выделенный сервис-менеджер и группа аналитиков	Да	Да
Доступ к Личному кабинету	Да	Да
Запуск типовых сценариев	Да	Да
Разработка нетиповых сценариев	Нет	Да
Обогащение Threat Intelligence	Да	Да
Подключение типовых источников	Да	Да
Подключение нетиповых источников	Нет	Да
Расследование инцидентов ИБ	Нет	Да
Подключение к ГосСОПКА и взаимодействие с НКЦКИ и ФинЦЕРТ	Да	Да
Подготовка ежемесячных отчетов по работе SOC	Да	Да, в т.ч. нетиповых отчетов

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ | УЦСБ SOC

КАК ПОДКЛЮЧИТЬ ТАРИФ?

ЗАБРОНИРОВАТЬ СКИДКУ МОЖНО **ДВУМЯ СПОСОБАМИ**

01

Нажмите на экране

«ХОЧУ КОНСУЛЬТАЦИЮ»

02

Напишите нам на почту

soc@ussc.ru

ОСТАЛИСЬ ВОПРОСЫ?

Пишите нам на почту soc@ussc.ru и мы проконсультируем вас по предложению или другим услугам УЦСБ SOC

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ | УЦСБ SOC

О КОМПАНИИ УЦСБ

с 2007
экспертиза в ИТ и ИБ

> 900
профессионалов в штате

> 4000
завершенных проектов

Входим в список 100 крупнейших компаний России в сфере защиты информации и ИТ по версии CNews Analytics и TAdviser

КОМПЕТЕНЦИИ

- Информационная безопасность
- Информационные технологии
- Анализ защищенности
- Центры обработки данных
- Инженерно-технические средства охраны
- Интеллектуальные инженерные системы
- Сервисный центр

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ | УЦСБ SOC

СВОЮ БЕЗОПАСНОСТЬ НАМ ДОВЕРЯЮТ

ОПЫТ

Успешно оказываем услугу компаниям из разных отраслей

ЭКСПЕРТИЗА

Команда УЦСБ SOC — сертифицированные эксперты по компьютерной криминалистике

НАСМОТРЕННОСТЬ

Видим симптомы в различных источников благодаря современным инструментам и базе Заказчиков

- Металлургические предприятия
- Авиационная промышленность
- Пищевая промышленность
- Разработчики ПО
- Государственный сектор
- Химическая промышленность
- Топливно-энергетический комплекс
- Финансовая сфера

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ

УЦСБ SOC

ВОПРОСЫ?

УЦСБ SOC

Security Operations Center

НЕПРЕРЫВНЫЙ МОНИТОРИНГ ИБ

soc@ussc.ru

soc.ussc.ru