



ФГБУ ФБ МСЭ Минтруда России

Конференция

**«Вопросы совершенствования
системы медико-социальной экспертизы:
современное состояние, тенденции и
перспективы»**

12 декабря 2023 года



ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УПРЯЖДЕНИЕ
«ФЕДЕРАЛЬНОЕ АГЕНТСТВО ТЕХНИЧЕСКОГО РЕГУЛИРОВАНИЯ
И ТЕХНИЧЕСКОГО РЕГУЛИРОВАНИЯ»

Результаты работы по информационной
безопасности и информационным технологиям МСЭ
в 2023 году и перспектива их развития в 2024 году

Сорокин Евгений Евгеньевич
Руководитель центра ИТО и МЭИ
ФГБУ ФБ МСЭ Минтруда России

Подберёзкин Владислав Иванович
заместителя руководителя
ФГБУ ФБ МСЭ Минтруда России

Пилотный проект Центра информационной безопасности

В рамках создания пилотного проекта по обеспечению информационной безопасности инфраструктуры федеральных учреждений МСЭ по субъектам РФ (далее – проект):

- 1) Развернута система управления информацией о безопасности и событиях информационной безопасности;
- 2) Развернута антивирусная система;
- 3) Развернута система контроля конфигураций и состояния рабочей среды сетевого оборудования;
- 4) Развернут программный комплекс автоматического анализа инцидентов на основе анализа событий информационной безопасности;
- 5) Развернут центр управления политиками безопасности VIPNet xFirewall;
- 6) Внедрены массовых экранов VIPNet xFirewall в федеральных учреждениях МСЭ по субъектам РФ.

Подберёзкин Владислав Иванович
заместителя руководителя
ФГБУ ФБ МСЭ Минтруда России



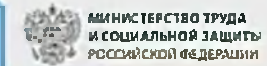
Пилотный проект Центра информационной безопасности

В рамках создания пилотного проекта по обеспечению информационной безопасности инфраструктуры федеральных учреждений МСЭ по субъектам РФ сделано:

- 1) Развернута система управления информацией о безопасности и событиями информационной безопасности;
- 2) Развернута антивирусная система;
- 3) Развернута система контроля конфигураций и состояний рабочей среды сетевого оборудования;
- 4) Развернут программный комплекс автоматического выявления инцидентов на основе анализа событий информационной безопасности;
- 5) Развернут центр управления политиками безопасности ViPNet xFirewall ;
- 6) Внедрение межсетевых экранов ViPNet xFirewall в федеральных учреждениях МСЭ по субъектам РФ.



ФГБУ ФБ МСЭ Минтруда России





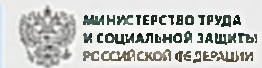
Пилотный проект Центра информационной безопасности

В рамках создания пилотного проекта по обеспечению информационной безопасности инфраструктуры федеральных учреждений МСЭ по субъектам РФ сделано:

- 1) Развернута система управления информацией о безопасности и событиях информационной безопасности;
- 2) Развернута антивирусная система;
- 3) Развернута система контроля конфигураций и состояний рабочей среды сетевого оборудования;
- 4) Развернут программный комплекс автоматического выявления инцидентов на основе анализа событий информационной безопасности;
- 5) Развернут центр управления политиками безопасности ViPNet xFirewall ;
- 6) Внедрение межсетевых экранов ViPNet xFirewall в федеральных учреждениях МСЭ по субъектам РФ.



ФГБУ ФБ МСЭ Минтруда России

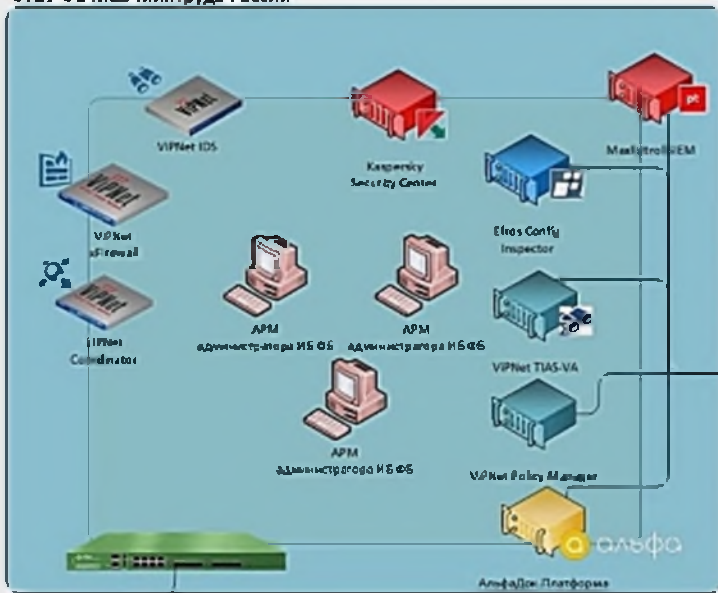


2

Сорокин Евгений Евгеньевич
руководитель Центра ИТО и МЭВ
ФГБУ ФБ МСЭ Минтруда России

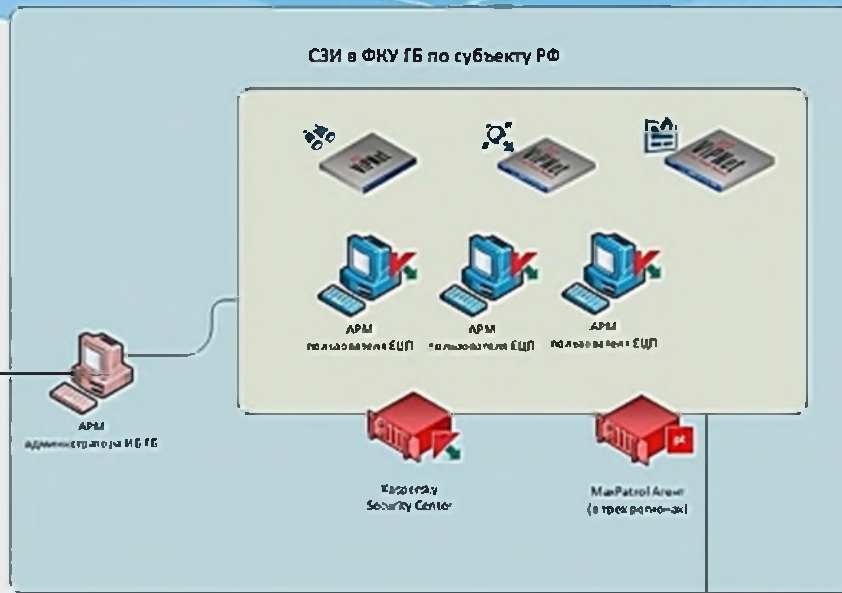
Центр информационной безопасности инфраструктуры федеральным учреждениям МСЭ по субъектам РФ

Центр информационной безопасности
ФГБУ ФБ МСЭ Минтруда России



ФКУ ГБ по субъекту РФ

СЗИ в ФКУ ГБ по субъекту РФ



КАЗ Karapinsky End Point Security

АльфаДок. Платформа

Etnos Config Inspector

MaxPatrol SIEM



ФГБУ ФБ МСЭ Минтруда России



МИНИСТЕРСТВО ТРУДА
И СОЦИАЛЬНОЙ ЗАЩИТЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Центр информационной безопасности
Система управления информацией о безопасности и событиями
информационной безопасности

Решаемые задачи:

- сбор, обработка и анализ событий безопасности, поступающих в систему из множества источников;
- обнаружение в режиме реального времени атак и нарушений критериев и политик безопасности;
- оперативная оценка защищенности информационных, телекоммуникационных и других критически важных ресурсов;
- анализ и управление рисками безопасности;
- проведение расследований инцидентов;
- принятие эффективных решений по защите информации;
- формирование отчетных документов.



Центр информационной безопасности
Система управления информацией о безопасности и событиями
информационной безопасности

Настроен сбор событий информационной безопасности:

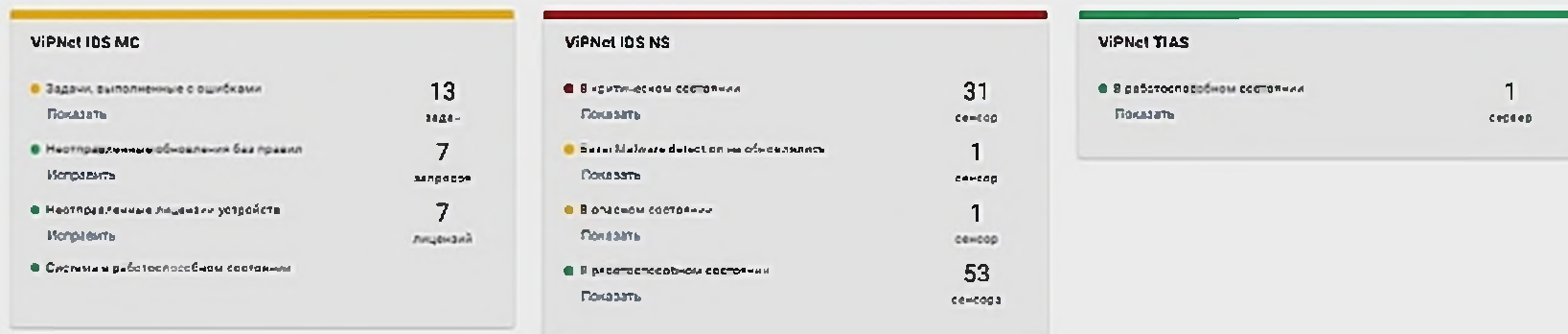
- Инфраструктуры ФГБУ ФБ МСЭ Минтруда России;
- Серверов, сетевого оборудования и АРМ трех пилотных регионов для сбора и обработки событий информационной безопасности;
- Оборудования VipNet Coordinator федеральных учреждений МСЭ по субъектам РФ;
- Комплекса автоматического выявления инцидентов на основе анализа событий информационной безопасности поступающих с VipNet IDS федеральных учреждений МСЭ по субъектам РФ.
- Мониторинга конфигураций сетевого оборудования.



Пилотный проект Центра информационной безопасности VipNet IDS MC

VipNet IDS MC (Management Center) – центр управления и мониторинга компонентами средств обнаружения вторжений VipNet IDS NS и системой интеллектуального анализа угроз безопасности информации VipNet TIAS.

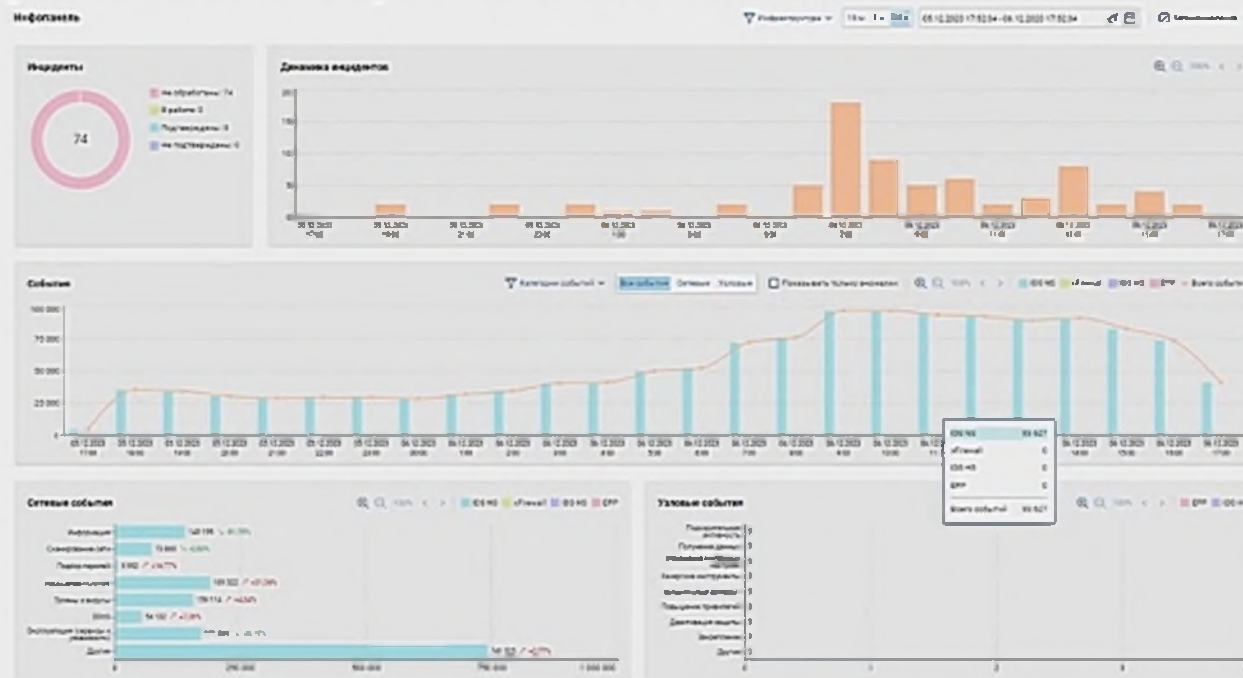
Инфопанель



Пилотный проект Центра информационной безопасности

Централизованнный сбор событий информационной безопасности с ViPNet IDS федеральных учреждений МСЭ по субъектам РФ .

Доступ к событиям информационной безопасности имеется в каждом федеральном учреждении МСЭ по субъектам РФ части касающейся.



Пилотный проект Центра информационной безопасности программный комплекс контроля конфигураций «Efros Config Inspector»

«Efros Config Inspector» реализует следующие функциональные возможности:

- Контроль и разграничение доступа пользователей к функциям комплекса и к устройствам;
- Ведение списка контролируемых устройств;
- Идентификация и аутентификация пользователей и устройств;
- Управление устройствами;
- Контроль работы устройств;
- Проверка наличия уязвимостей контролируемого оборудования;
- Сбор и обработка событий;
- Настройка общих параметров работы комплекса;
- Контроль целостности программного обеспечения комплекса и функционирования оборудования;
- Формирование и просмотр пользовательских отчетов.



Развернутая схема высоконагруженной системы управления информацией о безопасности и событиями информационной безопасности

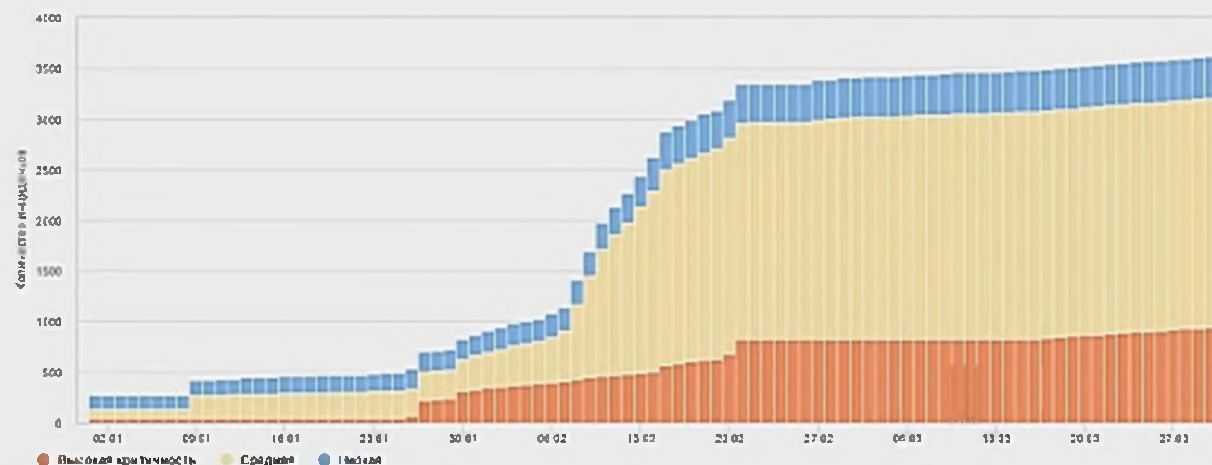
В период с 09.01.2023 по настоящее время было зарегистрировано более **3 500** инцидентов информационной безопасности (ИБ).

Из них **942** инцидента с высокой критичностью. В рамках пилота применяемые меры снижают среднее количество инцидентов за период времени.

Сотрудниками отдела ИБ закрыто более **2000** инцидентов высокой и средней критичности.

Инциденты ИБ сформированы с инфраструктуры трех пилотных регионов и ФГБУ ФБ МСЭ Минтруда России.

На данный момент можно спрогнозировать количество инцидентов ИБ при подключении всех регионов. Ожидаемое количество инцидентов ИБ со всех регионов более **70 000** инцидентов в период три месяца.



ФГБУ ФБ МСЭ Минтруда России



МИНИСТЕРСТВО ТРУДА
И СОЦИАЛЬНОЙ ЗАЩИТЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Центр информационной безопасности

Приказ Минтруда России № 804

от 14 ноября 2023

Согласно приказу Минтруда России № 804 от 14 ноября 2023 на федеральное государственное бюджетное учреждение «Федеральное бюро медико-социальной экспертизы» Министерства труда и социальной защиты Российской Федерации возложена роль по обеспечению информационной безопасности, в том числе по обнаружению, предупреждению, ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, а также управлению информационно-технической инфраструктурой федеральных учреждений медико-социальной экспертизы Министерства труда и социальной защиты Российской Федерации.

Основные задачи поставленные перед созданным в ФГБУ ФБ МСЭ Минтруда России подразделением:

- а) планирование, организация и координация работ по обеспечению информационной безопасности и контроль за ее состоянием в учреждениях МСЭ;
- б) планирование, организация и координация работ по обеспечению работоспособности информационно-технологической инфраструктуры и контроль за ее состоянием в учреждениях МСЭ;
- в) планирование, организация и координация работ по обеспечению работоспособности информационно-телекоммуникационных сетей и контроль за их состоянием в учреждениях МСЭ;
- г) выявление угроз безопасности информации и уязвимостей информационных систем, программного обеспечения и программно-аппаратных средств;
- д) предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;
- е) поддержание стабильной деятельности учреждений МСЭ и их производственных процессов в случае проведения компьютерных атак;
- ж) взаимодействие с Национальным координационным центром по компьютерным инцидентам;
- з) обеспечение нормативного правового регулирования при использовании информационных ресурсов;
- и) мониторинг информационно-технологической и информационно-телекоммуникационной инфраструктуры учреждений МСЭ.

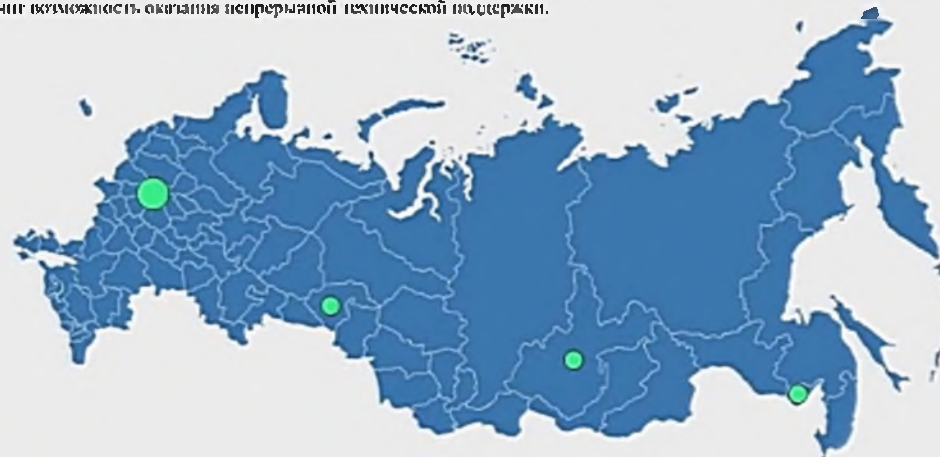




Центр информационной безопасности Приказ Минтруда России №804 от 14 ноября 2023

В рамках исполнения приказа Минтруда России № 804 от 14 ноября 2023 (ФГБУ ФБ МСЭ) помимо создания подразделения для выполнения поставленных задач создан отдел, на «Центр компетенций» и целях повышения устойчивости и безопасности функционирования информационных ресурсов федеральных учреждений медиа-социальной экспертизы Министерства труда и социальной защиты Российской Федерации.

В состав центра компетенций будут входить сотрудники федеральных учреждений МСЭ по субъектам РФ, что обеспечит возможность оказания непрерывной технической поддержки.



ФГБУ ФБ МСЭ Минтруда России

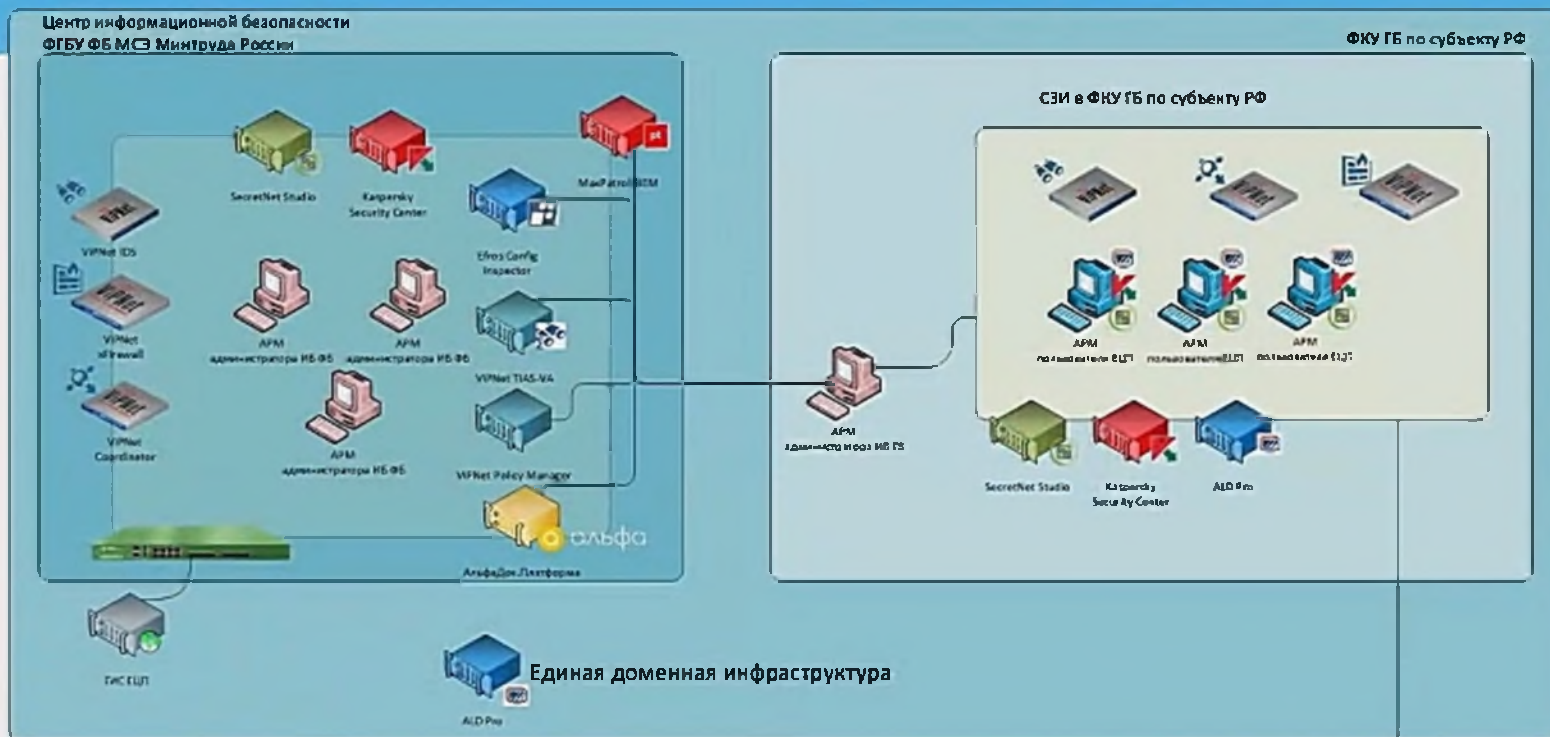








МИНИСТЕРСТВО ТРУДА
И СОЦИАЛЬНОЙ ЗАЩИТЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

11

Сорокин Евгений Евгеньевич
руководитель Центра ИТО и МЭВ
ФГБУ ФБ МСЭ Минтруда России

Центр информационной безопасности инфраструктуры федеральных учреждений МСЭ по субъектам РФ



-  СЗИ от ИСД SecretNet
-  Система для централизованного управления и автоматизации ИДРPro
-  САЭ Kaspersky End Point Security
-  Etnos Config Inspector
-  АльфаДок.Платформа
-  MaxPatrol SIEM



ФГУ ФБ МСЭ Минтруда России



МИНИСТЕРСТВО ТРУДА
И СОЦИАЛЬНОЙ ЗАЩИТЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Центр информационной безопасности распределение ролей между федеральными учреждениями МСЭ по субъектам РФ

Функция	ФКУ ГБ МСЭ Минтруда России	ФГБУ ФБ МСЭ Минтруда России
Управление событиями ИБ	Обеспечение работоспособности технических средств и передачи событий ИБ	Сбор, анализ и долгосрочное хранение событий информационной безопасности, собранных в рамках инфраструктуры ФБ МСЭ и ГБ МСЭ Передача статистики, отчетности и значимых событий информационной безопасности
Управление инцидентами ИБ	Участие в мероприятиях по реагированию на инциденты ИБ Предоставление отчетности	Работа с типовыми инцидентами и инцидентами локального значения в рамках инфраструктуры ФБ МСЭ и ГБ МСЭ Информирование о нештатных / массовых / критических инцидентах. Предоставление статистики и отчетности
Управление уязвимостями	Участие в мероприятиях по устранению уязвимостей Предоставление отчетности	Работа по выявлению и устранению уязвимостей в рамках инфраструктуры ФБ МСЭ и ГБ МСЭ Предоставление статистики и отчетности по уязвимостям
Управление угрозами ИБ	—	Информирование об индикаторах компрометации в рамках инфраструктуры ФБ МСЭ и ГБ МСЭ. Предоставление статистики и отчетности по выявленным угрозам
Контроль защищенности	Участие в мероприятиях по контролю защищенности Предоставление отчетности	Анализа защищенности инфраструктуры ФБ МСЭ и ГБ МСЭ, включая аудиты, тестирования на проникновение и контроль соответствия требованиям ИБ Предоставление статистики и отчетности



ФГБУ ФБ МСЭ Минтруда России



МИНИСТЕРСТВО ТРУДА
И СОЦИАЛЬНОЙ ЗАЩИТЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ



Спасибо за внимание!

Содержимое данного pdf-файла составлено из скриншотов видео, находящегося в свободном, открытом доступе по ссылке:
<https://rutube.ru/video/2a8086a944104059ca2cfbac8a5cb551/>



ФГБУ ФБ МСЭ Минтруда России



МИНИСТЕРСТВО ТРУДА
И СОЦИАЛЬНОЙ ЗАЩИТЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ