ЦБИ Центр безопасности информации

Практические аспекты применения стандартов по управлению компьютерными инцидентами

Конференция РусКрипто'2023
22 марта 2023 года

Сидак Алексей Александрович
Генеральный директор
sidak@cbi-info.ru

ООО «Центр безопасности информации» (ООО «ЦБИ»)

г. Королёв, Московская область

Актуальность предмета стандартизации

1
- ✓ Новые информационные технологии
- ✓ Масштаб систем
- ✓ Взаимосвязи между элементами

2
- ✓ Тактики, техники
- ✓ Инструментальные средства нарушителей

4 Мотивация

3
- ✓ Ценность информации
- ✓ Важность процессов

СИСТЕМЫ

НАРУШИТЕЛИ

Факторы

5
- ✓ Учет типовых угроз
- ✓ Меры защиты

6
- ✓ Целевые угрозы
- ✓ Скрытые каналы

Инциденты ИБ

7 **Потребность в стандартизации**

ДЕЯТЕЛЬНОСТЬ ПО УПРАВЛЕНИЮ ИНЦИДЕНТАМИ

ГОСТ Р 59709 «Управление инцидентами. Термины и определения»

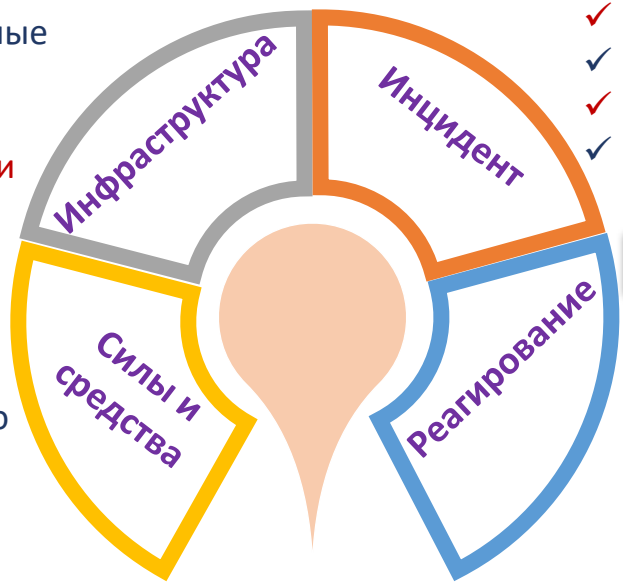
КОМПЬЮТЕРНЫЙ ИНЦИДЕНТ – «факт нарушения» (и прежде всего, в результате компьютерной атаки).
ИНЦИДЕНТ ИБ – это «событие, которое привело или может привести к нарушению или возникновению угроз».

ФГКУ в/ч 43753

ЦБИ Центр безопасности информации

1
- ✓ Информационная инфраструктура
- ✓ Элементы ИИ
- ✓ Информационные ресурсы
- ✓ Зона ответственности

2
- ✓ Подразделения и специалисты по управлению инцидентами.
- ✓ Технические, программные и программно-аппаратные средства

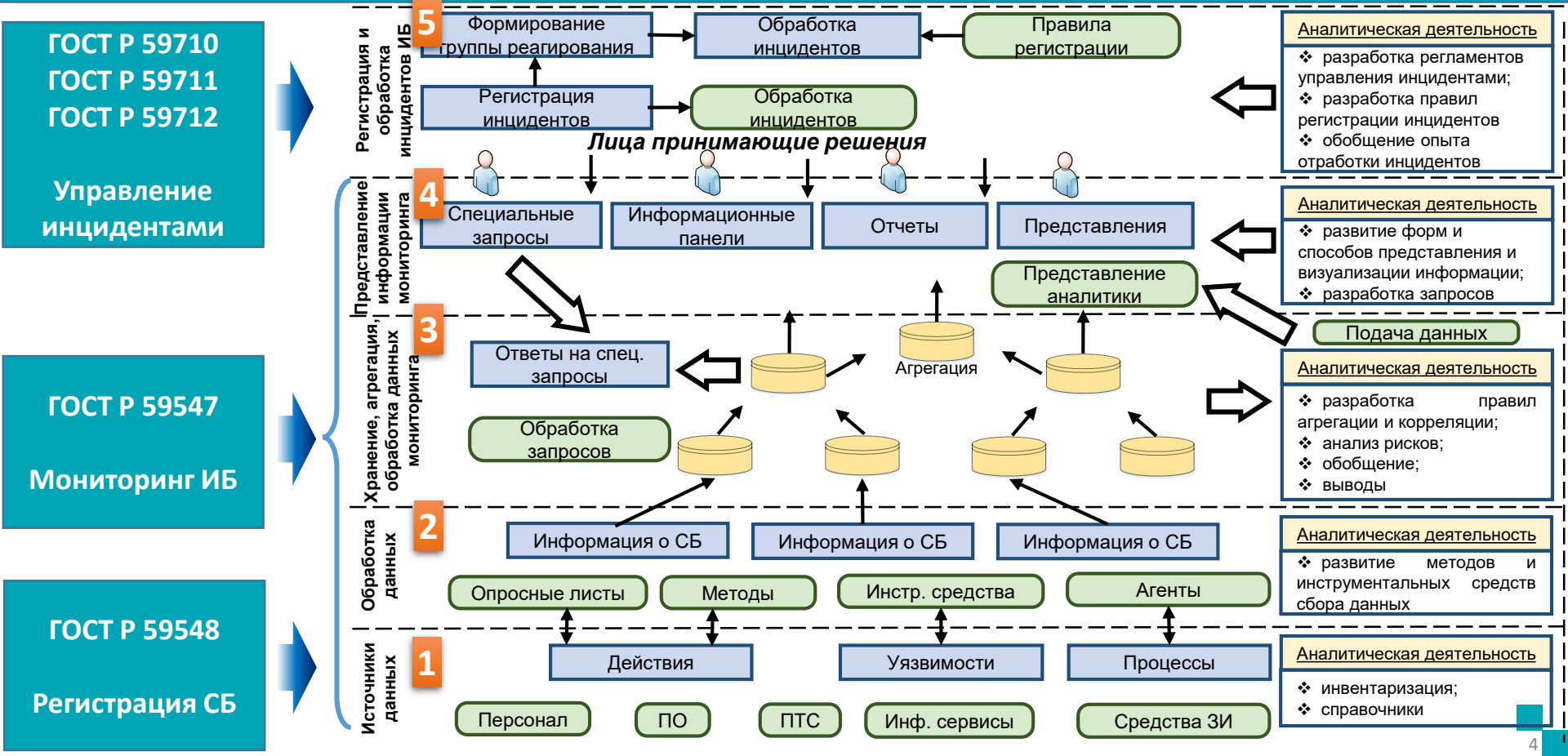


Термины

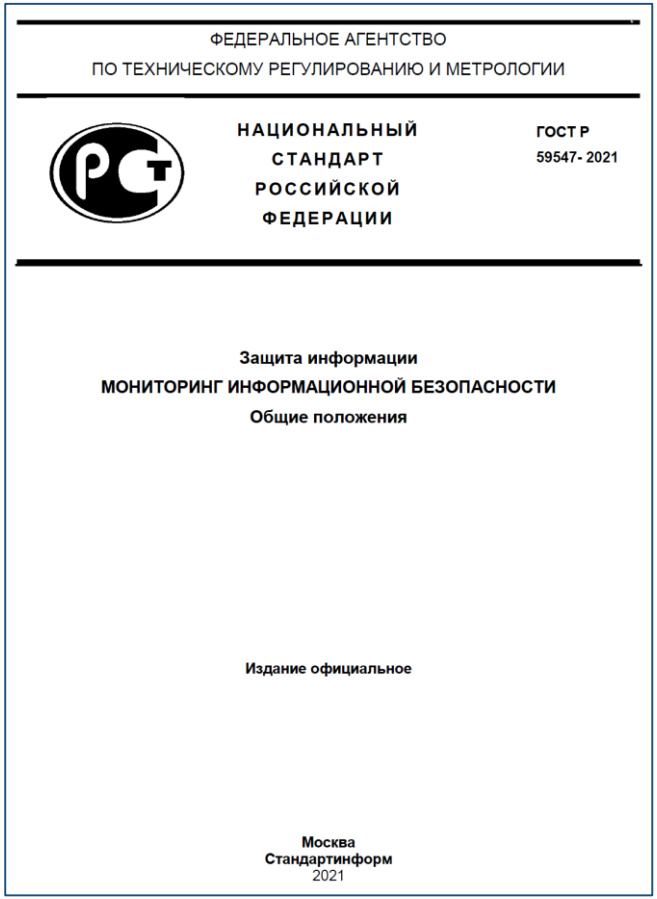
3
- ✓ Определения, относящиеся к инциденту (тип инцидента
- ✓ Источник инцидента
- ✓ техника, тактика
- ✓ Признак инцидента
- ✓ Карточка инцидента

4 Определения, связанные с
- ✓ мониторингом информационной безопасности
- ✓ организацией деятельности, стадиями и этапами выявления, реагирования на инцидент

Общая схема управления инцидентами



ГОСТ Р 59547 Мониторинг информационной безопасности. Общие положения


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59547- 2021

Защита информации
МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Общие положения

Издание официальное

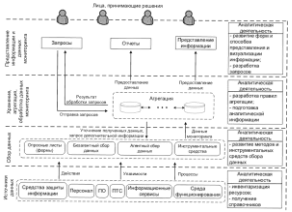
Москва
Стандартинформ
2021

ФСТЭК России

ЦБИ Центр безопасности информации

ТК 362 Защита информации

1 **Уровни мониторинга**



- ✓ **Источники** данных
- ✓ **Сбор** данных
- ✓ Хранение, агрегация, **обработка** данных мониторинга
- ✓ **Представление** информации и данных мониторинга

2 **Требования к уровням мониторинга**

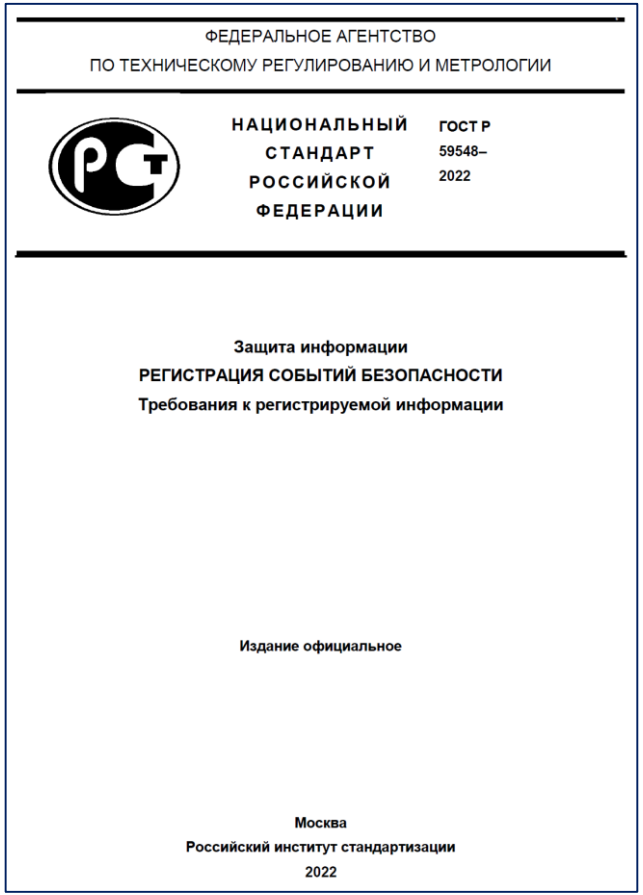
3 **Мероприятия и задачи мониторинга**

4 **Порядок мониторинга**

5 **Защита данных мониторинга**

Признаки нарушений и инцидентов

ГОСТ Р 59548 Регистрация событий безопасности. Требования к регистрируемой информации



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59548–2022

Защита информации
РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ
Требования к регистрируемой информации

Издание официальное

Москва
Российский институт стандартизации
2022

ФСТЭК России

ЦБИ Центр безопасности информации

ТК 362 Защита информации

Состав и содержание информации, подлежащей регистрации

✓ **1** Более **80**-ти **типов событий** безопасности

✓ **2** **Регистрируемая информация** для каждого типа событий безопасности

3 **Используется в нормативных правовых актах – требованиях к средствам ЗИ**

Практика применения стандартов в нормативных правовых актах (на примере НПА для многофункциональных МЭ)

Требования к многофункциональным межсетевым экранам уровня сети

К регистрации событий безопасности в межсетевом экране предъявляются следующие требования:

…

Межсетевой экран должен обеспечивать возможность регистрировать следующие типы событий безопасности с учетом **ГОСТ Р 59548 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации»**:

…

- ✓ **события безопасности, связанные с обнаружением признаков компьютерных атак в сетевом трафике;**

…

- ✓ **события безопасности, связанные с фильтрацией сетевого трафика;**

ГОСТ Р 59548 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации»

6. Требования к составу и содержанию регистрируемой информации

…

6.2.18 Состав и содержание регистрируемой информации для типа события безопасности, связанного **с обнаружением признаков компьютерных атак в сетевом трафике**, представлены в таблице 38.

Состав регистрируемой информации	Содержание регистрируемой информации
Идентификатор сенсора	Формат "Текст". Указывают уникальный (в рамках одного производителя) идентификатор устройства
Класс атаки	Формат "Текст"
Наименование сигнатуры атаки	Формат "Текст"
Сетевой адрес источника	Формат "Сетевой адрес"
Сетевой адрес назначения	Формат "Сетевой адрес"
Протокол	Формат "Текст". Указывают сокращение наименования сетевого протокола. Пример описания: IP/TCP/HTTP
Тип действия	Формат "Текст". Указывают краткое наименование выполняемых действий

…

6.2.22 Состав и содержание регистрируемой информации для типа события безопасности, связанного **с фильтрацией сетевого трафика**, представлены в таблице 46.

Состав регистрируемой информации	Содержание регистрируемой информации
Наименование правила фильтрации	Формат "Текст"
Номер правила фильтрации	Формат "Целое число"
Порт источника	Формат "Целое число". Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Порт назначения	Формат "Целое число". Число от 0 до 65535, указанное в заголовках протоколов транспортного уровня
Сетевой адрес источника	Формат "Сетевой адрес"
Сетевой адрес назначения	Формат "Сетевой адрес"
Сетевой интерфейс	Формат "Текст". Указывают наименование/порядковый номер интерфейса
Протокол	Формат "Текст". Указывают сокращение наименования сетевого протокола. Пример описания: IP/TCP/HTTP
Тип действия	Формат "Текст". Указывают краткое наименование выполняемых действий

Национальные стандарты по управлению компьютерными инцидентами

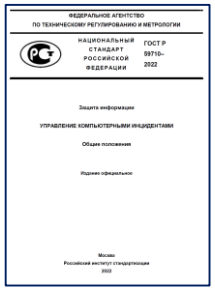
ФГКУ в/ч 43753

ЦБИ Центр безопасности информации

ТК 362 Защита информации

1

ГОСТ Р **59710**-2022
Защита информации. Управление компьютерными инцидентами. **Общие положения**



2

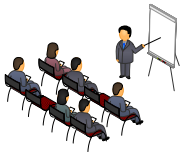
ГОСТ Р **59711**-2022
Защита информации. Управление компьютерными инцидентами. **Организация деятельности по управлению компьютерными инцидентами**

3

ГОСТ Р **59712**-2022
Защита информации. Управление компьютерными инцидентами. **Руководство по реагированию на компьютерные инциденты**

Стадии управления инцидентами

ГОСТ 59710-22



1 **Организация деятельности**

ГОСТ 59711-22

2 **Обнаружение и регистрация инцидентов**

ГОСТ 59712-22

3 **Реагирование на инциденты**

4 **Анализ результатов деятельности**

Организация деятельности. Этапы ГОСТ Р 59711-22

- ✓ Разработка **Политики** управления инцидентами → ***Определить инциденты***
- ✓ Разработка **Плана реагирования** на инциденты → ***- Пошаговые инструкции - Правила определения признаков инцидентов***
- ✓ Определение **подразделения**, ответственного за управление инцидентами → ***Особенности зоны ответственности***
- ✓ Организация **взаимодействия** → ***Подразделения, НКЦКИ, внешние организации***
- ✓ Материально-техническое **оснащение** → ***- задачи, требующие инструмент. поддержки - типы средств***
- ✓ Организация **обучения** и информирования → ***планы обучения***
- ✓ Проведение **тренировок** по отработке мероприятий Плана реагирования → ***Моделирование сценариев на тестовых системах (двойниках)***

Обнаружение и регистрация инцидентов. Этапы

ГОСТ 59712-22

- ✓ **Регистрация признаков** возможного возникновения инцидентов

Карточка признака инцидента 

- ✓ **Подтверждение** инцидентов
  - оценка влияния на ИР
  - Решение о регистрации инцидента
  - Формирование карточки инцидентов

Карточка инцидента 

Реагирование на инциденты

ГОСТ Р 59712-22

- ✓ Определение **вовлеченных** в инцидент **элементов** информационной инфраструктуры → Карточка инцидента

- ✓ **Локализация** компьютерного инцидента →

Предотвращение вовлечения новых элементов

- ✓ Выявление **последствий** инцидента → ***Признаки негативного воздействия: нештатная сетевая активность, аномальное использование ресурсов, изменение объектов, параметров настройки, состава ПО, ...***

- ✓ **Ликвидация** последствий инцидента → ***Действия для восстановления штатного функционирования системы***

- ✓ **Закрытие** инцидента → ***проверка качества и достаточности выполненных действий***

Анализ результатов деятельности. Этапы

Карточка инцидента

ГОСТ 59712-22

- ✓ **Накопление опыта**

  - в целях повторного применения способов реагирования, которые показали свою эффективность

- ✓ **Разработка рекомендаций по устранению причин и условий возникновения инцидентов**

  - для принятия дополнительных мер с целью предотвращения повторного возникновения закрытых инцидентов

- ✓ **Оценка результатов и эффективности реагирования на инциденты**

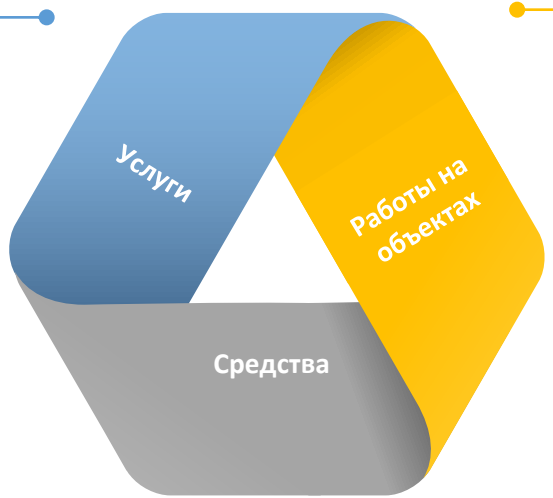
  - с целью совершенствования процессов и процедур

Практическое использование стандартов

1 Оказание услуг

Организация мониторинга и управления инцидентами в зоне ответственности:

- ☑ собственные системы;
- ☑ информационные ресурсы других организаций и субъектов ГосСОПКА, которым оказывается услуга в качестве Центра мониторинга



2 Выполнение работ на объектах

Учет положений новых стандартов при выполнении работ на объектах информатизации

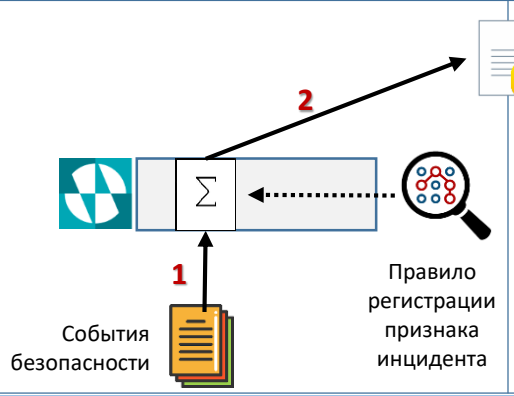
3 Разработка и адаптация средств

Выпускаемые средства для мониторинга и управления инцидентами максимально адаптированы, чтобы способствовать реализации новых стандартов

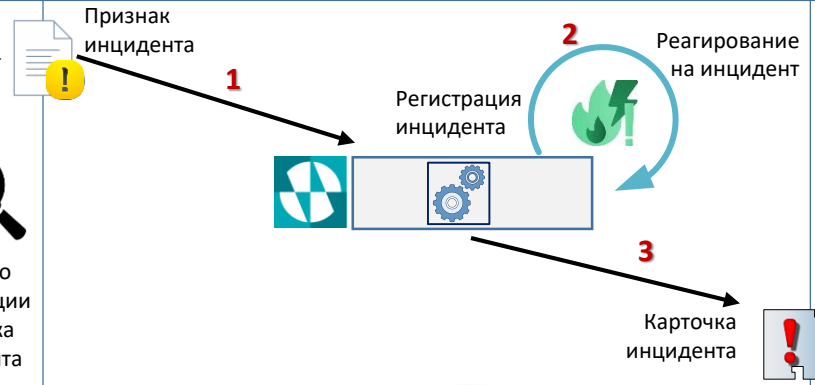
NEURODAT SIEM
NEURODAT SIEM IM
NEURODAT IS
NEURODAT SPLITTER

Инструментальные средства поддержки стандартов

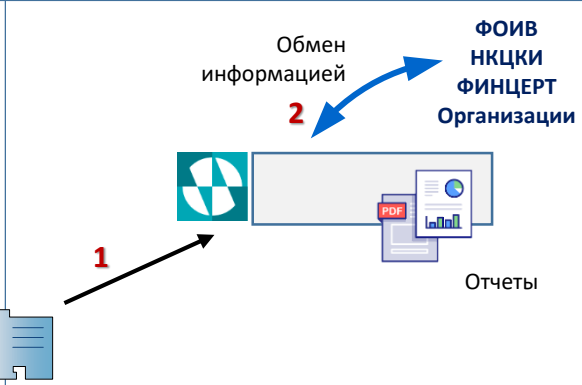
1 Средства управления событиями безопасности



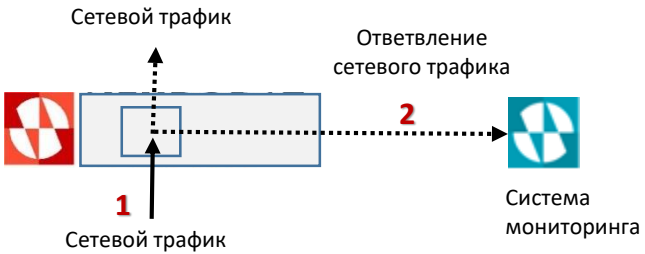
2 Средства управления инцидентами



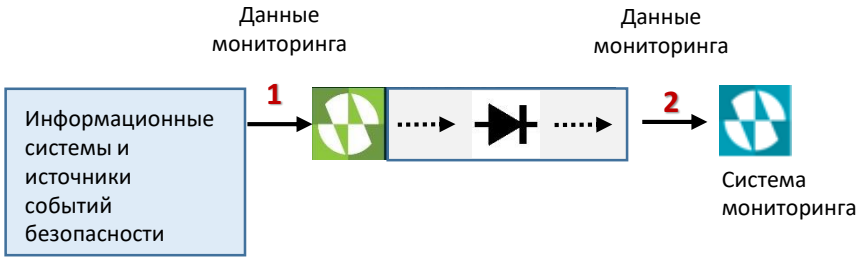
3 Средства обмена информацией об инцидентах



4 Средства ответвления сетевого трафика



5 Средства однонаправленной передачи информации



Национальные стандарты по управлению инцидентами

ГОСТ Р 59709-2022 Защита информации. Управление компьютерными инцидентами. Термины и определения

ГОСТ Р 59710-2022 Защита информации. Управление компьютерными инцидентами. Общие положения

ГОСТ Р 59711-2022 Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами

ГОСТ Р 59712-2022 Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты

ГОСТ Р 59547-2021 Защита информации. Мониторинг информационной безопасности. Общие положения

ГОСТ Р 59548-2022 Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации

ФГКУ в/ч 43753

ФСТЭК России

ЦБИ Центр безопасности информации

ТК 362 Защита информации

ЦБИ Центр безопасности информации

Практические аспекты применения стандартов по управлению компьютерными инцидентами

Конференция РусКрипто’2023. 22 марта 2023 года

ООО «Центр безопасности информации» (ООО «ЦБИ»)

г. Королев, Московской области
Ул. Ленинская, д. 11

: 8 (495) 580-52-18

: info@cbi-info.ru