Вопросы стандартизации процессов управления инцидентами информационной безопасности

ТБ ФОРУМ 2023. 15 февраля 2023 года
Актуальные вопросы защиты информации. XIII Конференция

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

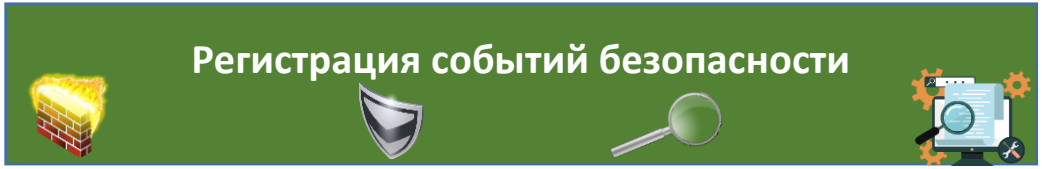
Инциденты ИБ

7 **Потребность в стандартизации**

ДЕЯТЕЛЬНОСТИ ПО УПРАВЛЕНИЮ ИНЦИДЕНТАМИ

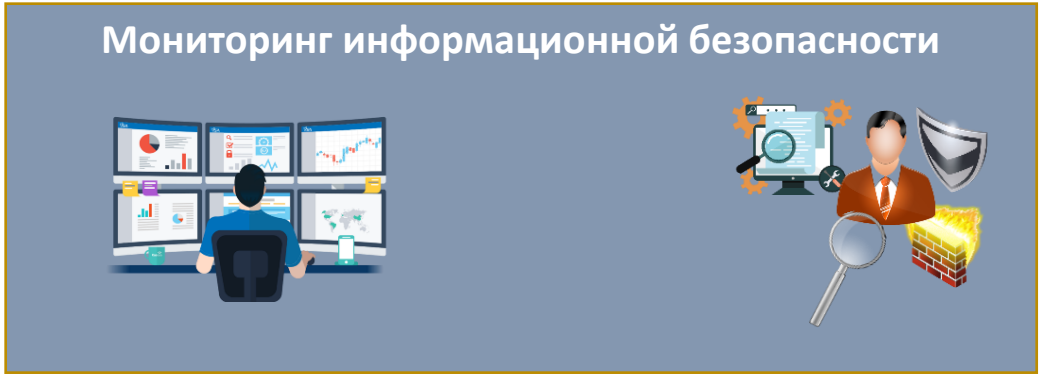
Регистрация, мониторинг, управление инцидентами

1



Данные регистрации

2



Результаты мониторинга

3

Управление инцидентами

Постановка задач стандартизации

Заседание ТК 362

ТК 362 Защита информации

Рабочая группа № 2

Экз. № 1

Решение
председателя технического комитета
по стандартизации «Защита информации» (ТК 362)

«12» июля 2018 г. г. Москва № 74

О назначении руководителей рабочих групп

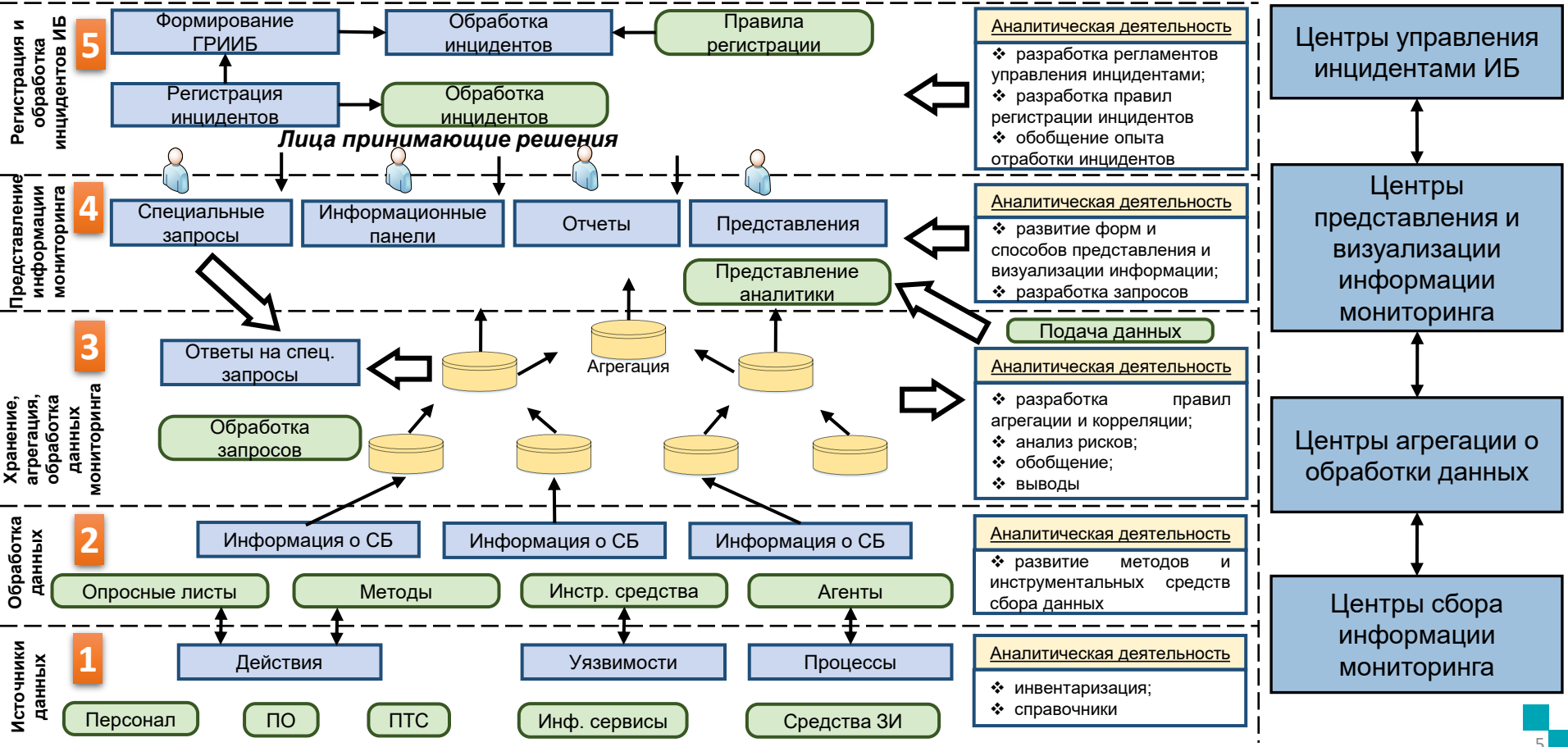
В соответствии с п. 4.3 Положения о ТК 362 и во исполнение пункта 1 раздела I, пункта 1 раздела III и пункта 2 раздела IV решения заседания подкомитетов ТК 362 17 мая 2018 г.

Основные направления стандартизации:

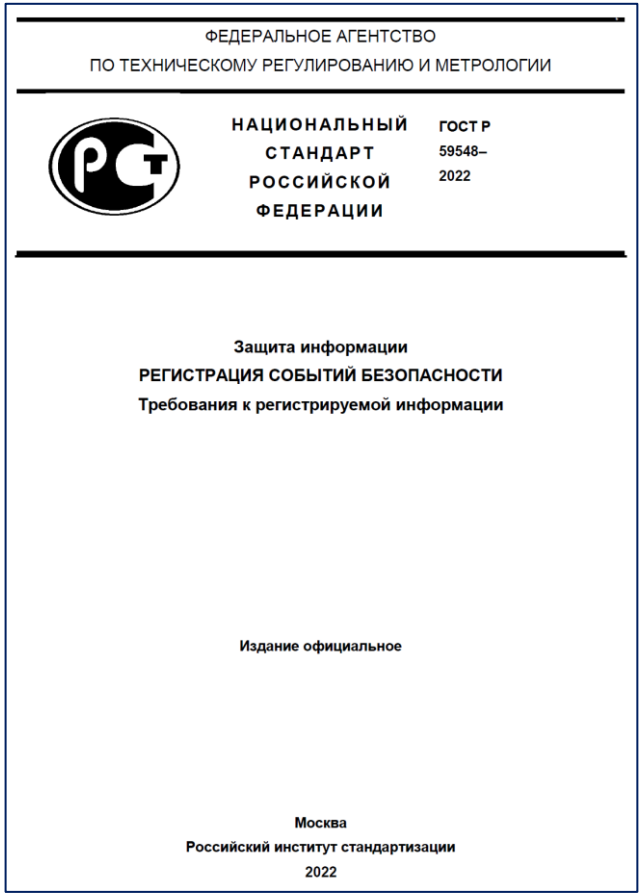
- ✓ Регистрация событий безопасности
- ✓ Мониторинг ИБ
- ✓ Управление инцидентами

ЦБИ Центр безопасности информации

Общая схема стандартизируемой деятельности



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

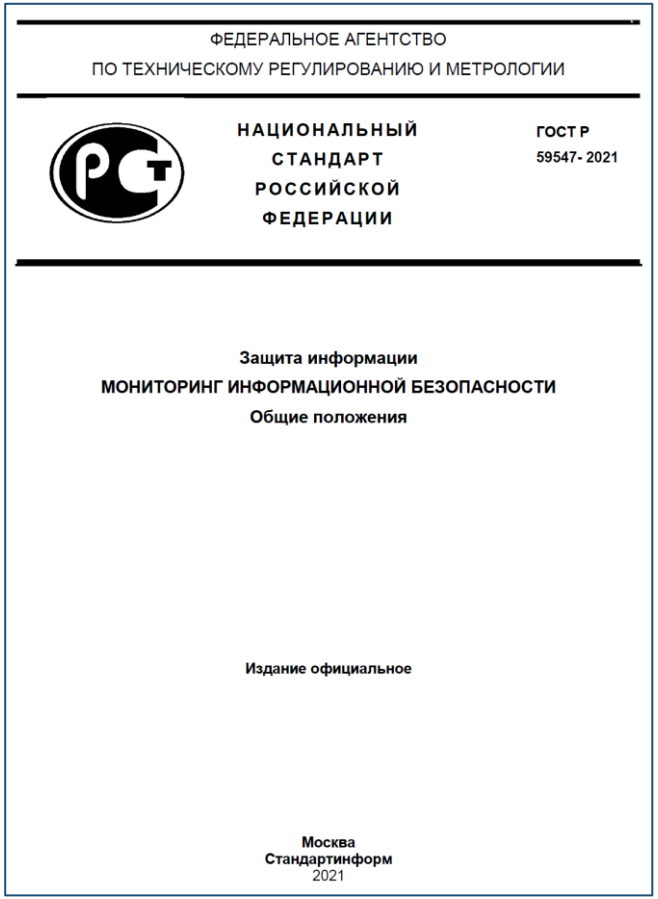
Состав и содержание информации, подлежащей регистрации

✓ 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**

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

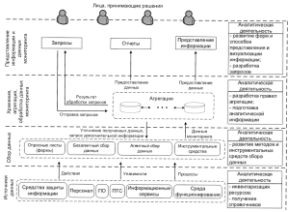
Москва
Стандартинформ
2021

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

Национальные стандарты управление инцидентами

ГОСТ Р 59709

Защита информации. Управление компьютерными инцидентами. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Приказ Росстандарта 1375-ст от 29.11.2022 г.

ГОСТ Р 59710

Защита информации. Управление компьютерными инцидентами. ОБЩИЕ ПОЛОЖЕНИЯ

Приказ Росстандарта 1376-ст от 29.11.2022 г.

ГОСТ Р 59711

Защита информации. Управление компьютерными инцидентами. ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПО УПРАВЛЕНИЮ КОМПЬЮТЕРНЫМИ ИНЦИДЕНТАМИ

Приказ Росстандарта 1377-ст от 29.11.2022 г.

ГОСТ Р 59712

Защита информации. Управление компьютерными инцидентами. РУКОВОДСТВО ПО РЕАГИРОВАНИЮ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

Приказ Росстандарта 1378-ст от 29.11.2022 г.

ФГКУ в/ч 43753

ЦБИ Центр безопасности информации

ТК 362 Защита информации

*** - Стандарты введены в действие с 1.02.2023 г.**

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».

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

Национальные стандарты по управлению инцидентами

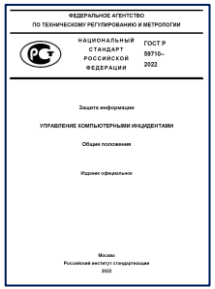
ФГКУ в/ч 43753

ЦБИ Центр безопасности информации

ТК 362 Защита информации

1

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



2

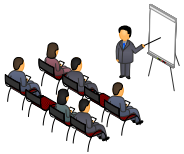
ГОСТ Р **59711**-2022
Защита информации. Управление компьютерными инцидентами. **Организация деятельности по управлению компьютерными инцидентами**

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

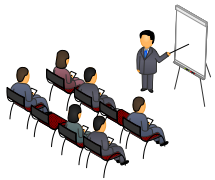
ГОСТ 59712-22

3 Реагирование на инциденты

4 Анализ результатов деятельности

Организация деятельности

ГОСТ 59711-22



- ✓ Разработка **Политики** управления инцидентами
- ✓ Разработка **Плана реагирования** на инциденты
- ✓ Определение **подразделения**, ответственного за управление инцидентами
- ✓ Организация **взаимодействия**
- ✓ Материально-техническое **оснащение**
- ✓ Организация **обучения** и информирования
- ✓ Проведение **тренировок** по отработке мероприятий Плана реагирования

Обнаружение и регистрация инцидентов

ГОСТ 59712-22

- ✓ **Регистрация признаков** возможного возникновения инцидентов

Карточка признака инцидента 

- ✓ **Подтверждение** инцидентов

(Оценка влияния на ИР)

Карточка инцидента 

Реагирование на инциденты

ГОСТ 59712-22

- ✓ Определение **вовлеченных** в инцидент **элементов** информационной инфраструктуры

Карточка инцидента

- ✓ **Локализация** компьютерного инцидента

- ✓ Выявление **последствий** инцидента
- ✓ **Ликвидация** последствий инцидента
- ✓ **Закрытие** инцидента

Отдельные этапы реагирования на инциденты

ГОСТ 59712-22

- ✓ **Фиксация материалов**, связанных с возникновением инцидента
- ✓ Установление **причин и условий** возникновения инцидента

Очередность реагирования на инциденты

Очередь реагирования	1-я	2-я	3-я	4-я	5-я	6-я	7-я	8-я	9-я
Уровень влияния компьютерного инцидента	Критический	Высокий	Высокий	Средний	Средний	Средний	Низкий	Низкий	Низкий
Приоритет компьютерного инцидента	Высокий	Высокий	Средний	Высокий	Средний	Низкий	Высокий	Средний	Низкий

Определение уровней влияния инцидента

Критерии	Уровни влияния			
	Критический	**Высокий**	**Средний**	**Низкий**
Ущерб в социальной сфере	Ущерб здоровью 500 человек или более	Ущерб здоровью от 50 до 500 человек	Ущерб здоровью от 1 до 50 человек	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности
Ущерб в политической сфере	Прекращение или нарушение функционирования Администрации Президента РФ, Правительства РФ и т.п.	Прекращение или нарушение функционирования федерального органа государственной власти	Прекращение или нарушение функционирования органа государственной власти субъекта РФ или города федерального значения	
Экономический ущерб	Ущерб, выраженный в снижении уровня дохода по всем видам деятельности более чем на 20 % от годового объема доходов, усредненного за прошедший 5-летний период	Ущерб, выраженный в снижении уровня дохода по всем видам деятельности от 10 до 20 % от годового объема доходов, усредненного за прошедший 5-летний период	Ущерб, выраженный в снижении уровня дохода по всем видам деятельности от 1 до 10 % от годового объема доходов, усредненного за прошедший 5-летний период	Снижение уровня дохода, которое не попадает под критерии других уровней
Ущерб в экологической сфере	Вредные воздействия на 5 000 человек и более	Вредные воздействия на 1 000 - 5 000 человек	Вредные воздействия на 2 - 1 000 человек	Вредные воздействия на людей, не попадающие под критерии других уровней
Ущерб для обеспечения обороны страны, безопасности государства и правопорядка	Прекращение или нарушение функционирования пункта управления государством или ситуационного центра Администрации Президента РФ, Правительства РФ и т.п.	Прекращение или нарушение функционирования пункта управления или ситуационного центра федерального органа государственной власти	Прекращение или нарушение функционирования пункта управления или ситуационного центра органа государственной власти субъекта РФ или города федерального значения	

Определение приоритета: значимость вовлеченных СВТ

Приоритет	Значимость вовлеченных СВТ
Высокий	**СВТ, реализующие сервисы, связанные с критическими процессами**
Средний	**СВТ, с которых инцидент наиболее быстро может распространиться на СВТ, связанные с критическими процессами**
Низкий	**Иные СВТ**

Определение приоритета: масштаб инцидента (количество вовлеченных СВТ)

Приоритет	Количество СВТ, на которых обнаружены признаки зарегистрированного инцидента
Высокий	**30% и более**
Средний	**10%-30%**
Низкий	**10%**

Анализ результатов деятельности

ГОСТ 59712-22

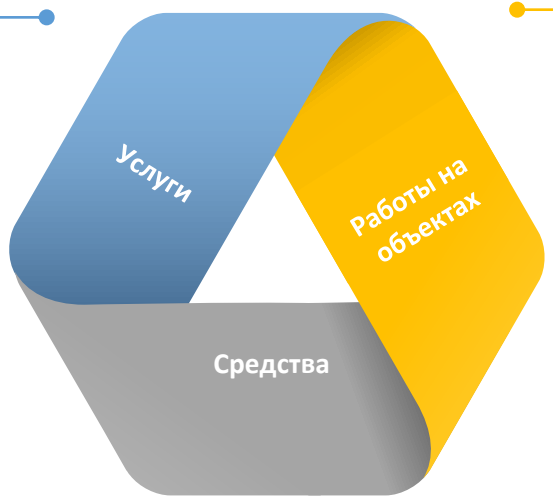
- ✓ **Накопление опыта**
- ✓ **Разработка рекомендаций по устранению причин и условий возникновения инцидентов**
- ✓ **Оценка результатов и эффективности реагирования на инциденты**

Практическое использование новых 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

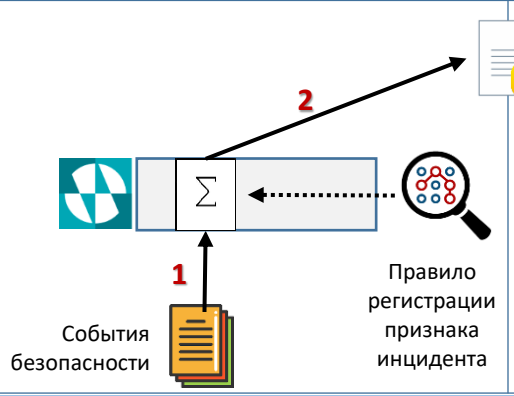
3 Разработка и адаптация средств

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

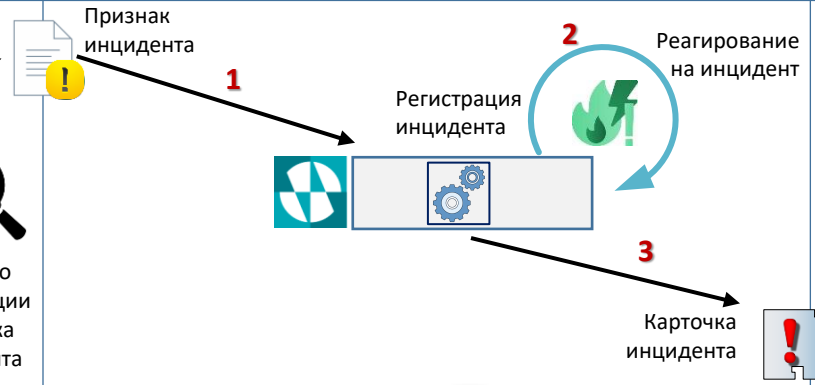
NEURODAT SIEM
NEURODAT SIEM IM
NEURODAT IS
NEURODAT SPLITTER

Средства, реализуемые по стандартам

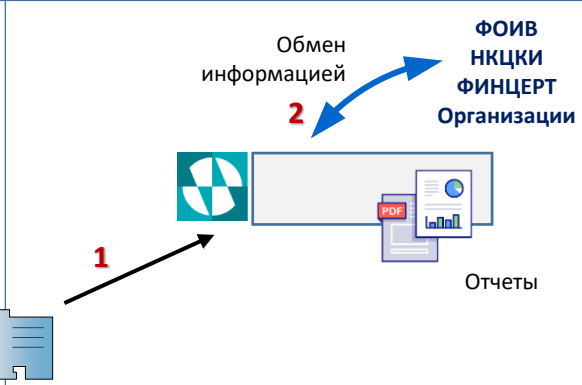
1 Средства управления событиями безопасности



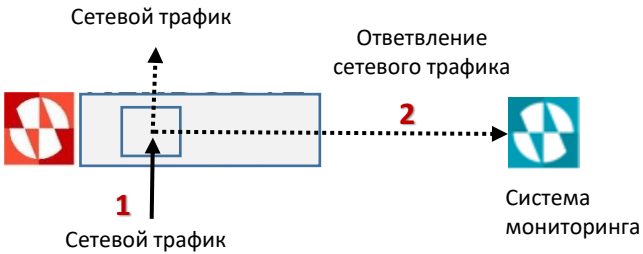
2 Средства управления инцидентами



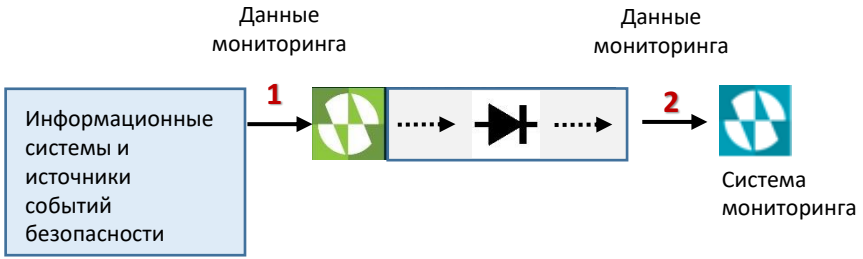
3 Средства обмена информацией об инцидентах



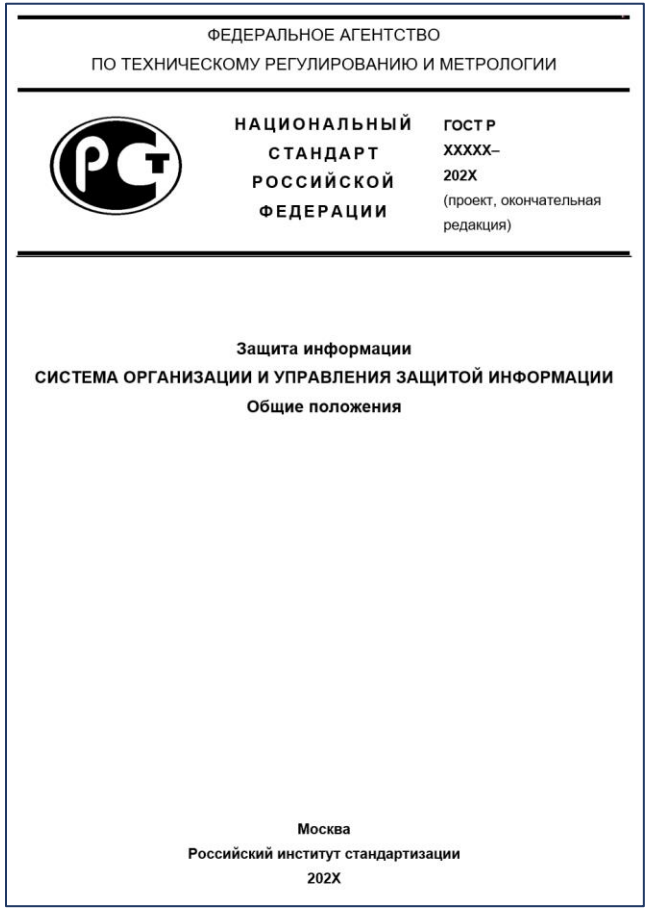
4 Средства ответвления сетевого трафика



5 Средства однонаправленной передачи информации



ГОСТ Р Защита информации. Система организации и управления защитой информации. Общие положения (проект)



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р XXXXX–202X
(проект, окончательная редакция)

Защита информации
СИСТЕМА ОРГАНИЗАЦИИ И УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ
Общие положения

Москва
Российский институт стандартизации
202X

ФСТЭК России

ЦБИ Центр безопасности информации

ТК 362 Защита информации

- ☑ **Процессы организации и управления защитой информации**
- ☑ **Планирование деятельности**
- ☑ **Обеспечение функционирования системы организации и управления защитой информации**
- ☑ **Оценка функционирования системы организации и управления защитой информации**
- ☑ **Совершенствование системы организации и управления защитой информации**

ЦБИ Центр безопасности информации

Вопросы стандартизации процессов управления инцидентами информационной безопасности

ТБ-ФОРУМ. 15 февраля 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