ТИПОВЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ ПО ПРИМЕНЕНИЮ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

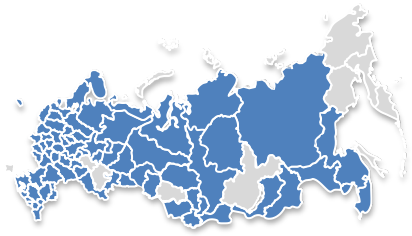
ДМИТРИЙ ХИЖКИН

Заместитель начальника Департамента обеспечения безопасности «Россети», начальник Департамента информационной безопасности «Россети ФСК ЕЭС»

декабрь 2021 года

WWW.ROSSETI.RU

СЕТИ СВЯЗИ ЭЛЕКТРОСЕТЕВОГО КОМПЛЕКСА



28 сетевых компаний
субъекты критической информационной инфраструктуры (КИИ)

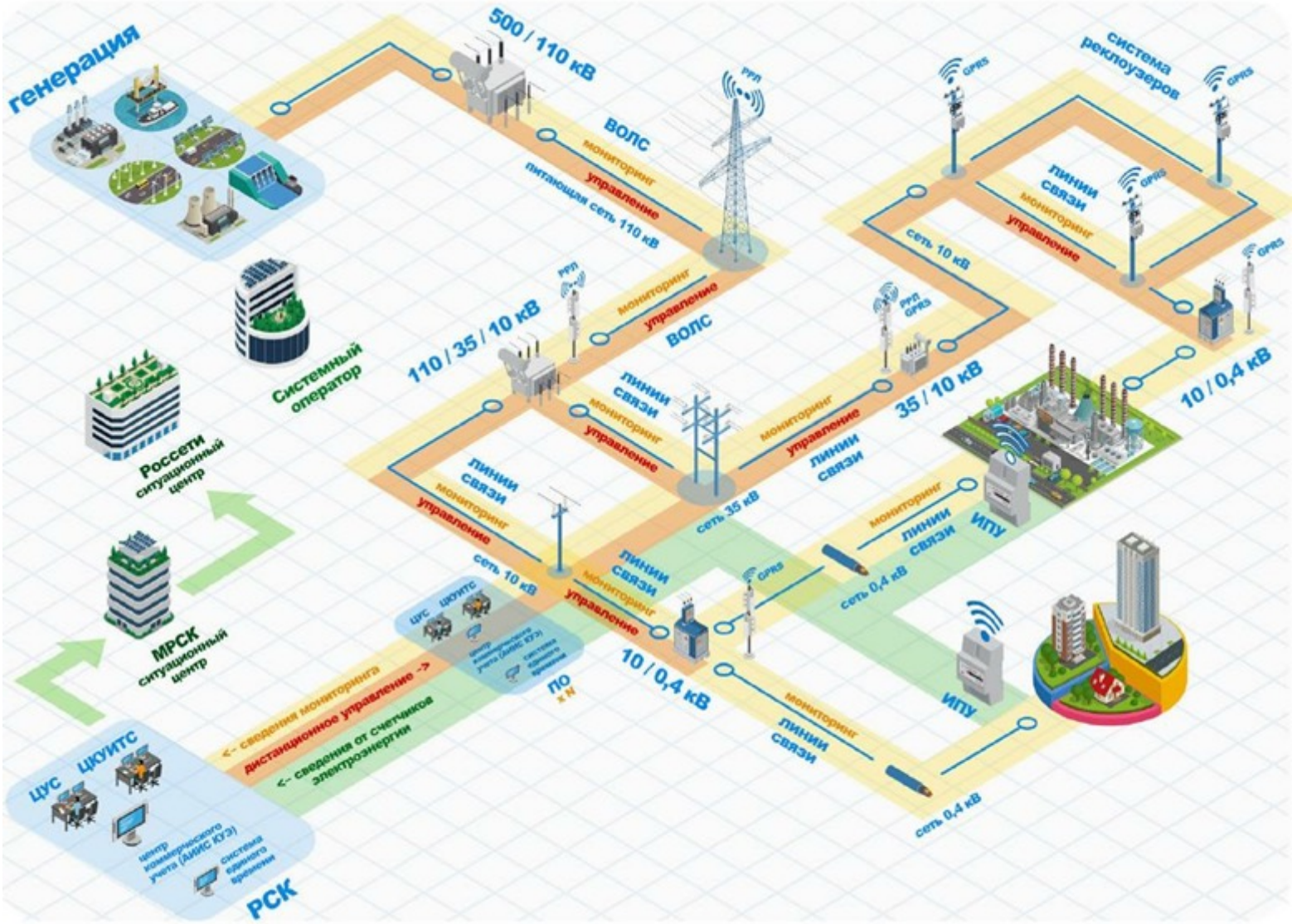
80 субъектов
география присутствия

3,240 тыс. ед.
микропроцессорых устройств, имеющих интерфейсы сетевого взаимодействия

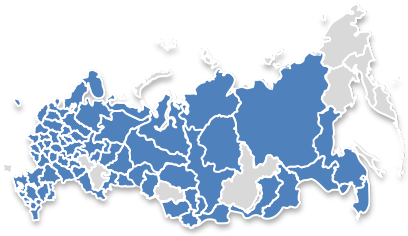
125 тыс. ед.
автоматизированных рабочих мест

517 тыс. ед.
подстанций

217 тыс. чел.
Среднесписочная численность персонала



СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОСЕТЕВОГО КОМПЛЕКСА



28 сетевых компаний
субъекты критической информационной инфраструктуры (КИИ)

80 субъектов
география присутствия

3.240 тыс. ед.
микропроцессорых устройств, имеющих интерфейсы сетевого взаимодействия

125 тыс. ед.
автоматизированных рабочих мест

517 тыс. ед.
подстанций

217 тыс. чел.
Среднесписочная численность персонала

Определены угрозы информационной безопасности для электросетевого комплекса
Доктрина энергетической безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 13 мая 2019 г. № 216

Определены обязанности и ответственность субъектов критической информационной инфраструктуры
Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Значимые объекты критической информационной инфраструктуры включены в реестр значимых ОКИИ
Реестр значимых объектов критической информационной инфраструктуры (Статья 8. 187-ФЗ, уполномоченное лицо - ФСТЭК России) **3 602**

Стратегия развития ПАО «Россети» и его ДЗО на период до 2030 года
(утверждена протоколом Совета директоров ПАО «Россети» от 26.12.2019 № 388)

Создание в ДЗО комплексной системы безопасности в отношении всех объектов критической информационной инфраструктуры, с учетом значимых ОКИИ и ОКИИ, эксплуатируемых в обособленных подразделениях, филиалах, представительствах, дочерних и зависимых Обществах, реализуя правовые, организационные, технические и иные меры защиты, направленные на обеспечение защиты обрабатываемой информации и непрерывность функционирования объектов информационной инфраструктуры

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА ГК РОССЕТИ

КИС	-	корпоративные информационные системы, ИСУЭ	4 706
АСУ	-	автоматизированные системы управления, мониторинга и диагностики	5 761
ИТС	-	**корпоративные и технологические информационно-телекоммуникационные сети и системы управления сетями и сетевым оборудованием**	2 802
ОКИ	-	**архитектура и конфигурация** КИС, АСУ, **ИТС**	

а также сети электросвязи, используемые для организации взаимодействия объектов КИИ

К СИЛАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КИИ ОТНОСЯТСЯ

- подразделения (работники), ответственные за обеспечение безопасности ОКИИ, в том числе значимых ОКИИ;
- подразделения (работники), эксплуатирующие объекты критической информационной инфраструктуры, в том числе значимые;
- **подразделения (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) объектов критической информационной инфраструктуры**, в том числе значимых.

ЗАЩИТА СЕТЕЙ СВЯЗИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К НИМ И ПЕРЕДАВАЕМОЙ ПО НИМ ИНФОРМАЦИИ

Порядок создания подсистемы безопасности ИТС и Систем управления сетями связи

- Для существующих и эксплуатируемых ОКИИ – в рамках Программы «Информационная безопасность» Общества (ДЗО)
- Для создаваемых, модернизируемых ОКИИ – в рамках реализации инвестиционных проектов (Типовое задание на проектирование)

ОКИИ без установленной категории значимости

- Единая техническая политика в ЭСК;
- Концепция построения сети связи ЭСК (распоряжение ПАО «Россети»
- от 02.09.2020 № 252р);
- Базовый набор технических мер защиты (распоряжение ПАО «Россети»
- от 09.03.2021 № 72р).

ЗНАЧИМЫЕ ОКИИ

- 235, 239 Приказ ФСТЭК России;
- Типовые технические решения по проектированию подсистем информационной безопасности ОКИИ (распоряжение ПАО «Россети» от 09.03.2021 № 72р);

- Использование выделенных сетей связи, технологических сетей связи
- Взаимодействие посредством сети связи общего пользования (ССОП) (например, сеть «Интернет») необходимо согласовать со ФСТЭК России.

В этом случае защиту передаваемой информации и безопасность сети связи обеспечивает оператор связи.

ПП РФ от 08.06.2019 №743

УЗЛЫ СВЯЗИ И МЕСТА РАЗМЕЩЕНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ СВЯЗИ

- оснащение мест размещения средств связи запирающими устройствами, тревожной и охранной сигнализацией;
- осмотр антенно-мачтовых сооружений, линейно-кабельных сооружений, в том числе колодцев кабельной канализации, оконечных кабельных устройств на предмет наличия следов НСД, сторонних технических средств.

Ввод в эксплуатацию ОКИИ или составных частей допускается только при наличии протокола (акта) приемочных испытаний с положительным заключением о соответствии и эффективности подсистемы безопасности установленным требованиям по обеспечению безопасности

БАЗОВЫЙ НАБОР ТЕХНИЧЕСКИХ МЕР ВКЛЮЧАЕТ

1. Средства защиты информации от несанкционированного доступа, в том числе средства идентификации и аутентификации, управления доступом, ограничения программной среды, защиты машинных носителей информации, контроля целостности (включая встроенные функции безопасности в общесистемное, прикладное программное обеспечение и (или) программно-аппаратные средства);
2. Межсетевые экраны уровня сети;
3. Средства обнаружения (предотвращения) вторжений (компьютерных атак) уровня сети, уровня сервера, автоматизированного рабочего мест;
4. Средства антивирусной защиты общего назначения, потовых и веб-серверов, файловых хранилищ и защиты от спама;
5. Средства защиты (кодирования) данных при передаче по сетям связи общего пользования, выделенным сетям связи;
6. Средства защищенного удаленного доступа в ЛВС, в том числе средства терминального доступа;
7. Средства резервного копирования, в том числе создания и хранения резервных копий.

ЗАЩИТА СЕТЕЙ СВЯЗИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К НИМ И ПЕРЕДАВАЕМОЙ ПО НИМ ИНФОРМАЦИИ

СЕТЬ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

На границе применяются межсетевые экраны, сертифицированные ФСТЭК России на соответствие требованиям по безопасности информации (тип «А», тип «Б» и тип «Г» в терминах приказа ФСТЭК России от 9 февраля 2016 г. N 9), а также средства обнаружения (предотвращения) вторжений (компьютерных атак) уровня сети

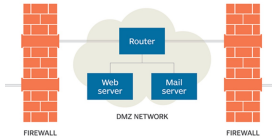
Должна обеспечиваться защита передаваемой по сети связи информации от несанкционированного доступа за счет использования технологии VPN и средств криптографической защиты информации (СКЗИ), если применение СКЗИ обусловлено требованиями действующего законодательства в сфере защиты информации и актуальной моделью угроз безопасности информации

ВЫДЕЛЕННЫЕ СЕТИ СВЯЗИ

В сетях подвижной радиотелефонной связи в стандарте GSM / LTE в договоры на оказание услуг связи должны быть включены требования :

- зафиксировать с оператором связи для сети связи топологию «Звезда» (Hub and Spoke);
- обеспечить изоляцию передаваемых данных за счет технологии APN;
- обеспечить мониторинг извлечения авторизованной SIM карты из модемов для которого она предназначена и информирование Общества о факте извлечения.

ДМЗ



Сегменты сети, которые обслуживают внешние сетевые запросы и соединения и из которых исключена возможность инициации соединений в технологические сегменты сети

ТЕХНОЛОГИЧЕСКИЕ СЕТИ СВЯЗИ

в том числе при организации сетевого взаимодействия с другими ДЗО ПАО «Россети», АО «СО ЕЭС», технологическими сетями связи смежных сетевых организаций

Применяются межсетевые экраны, сертифицированные ФСТЭК России на соответствие требованиям по безопасности информации (тип «Д» в терминах приказа ФСТЭК России от 9 февраля 2016 г. N 9), а также средства обнаружения (предотвращения) вторжений (компьютерных атак) уровня сети

Удалённое управление должно быть организовано по протоколам, обеспечивающим защиту всего передаваемого трафика, включая парольную информацию (например, по протоколу SSH), а также с применением двухфакторной аутентификации

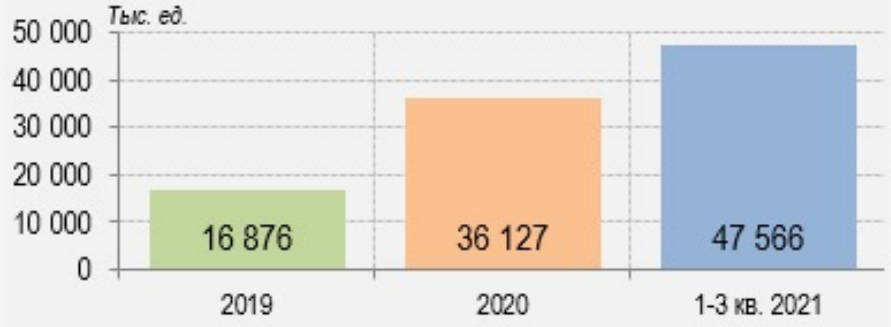
НЕ ДОПУСКАЕТСЯ:

- наличие удаленного доступа непосредственно (напрямую) к программным и программно-аппаратным средствам ИТС и Систем управления для обновления или управления со стороны лиц, не являющихся работниками ДЗО ПАО «Россети»;
- наличие локального доступа к программным и программно-аппаратным средствам ИТС и Систем управления для обновления или управления со стороны лиц, не являющихся работниками ДЗО ПАО «Россети» без контроля со стороны ДЗО ПАО «Россети»;
- передача информации, в том числе технологической информации, разработчику (производителю) программных и программно-аппаратных средств или иным лицам без контроля со стороны работников ДЗО ПАО «Россети».

1. В настройках телекоммуникационного оборудования должны быть включены функции, защищающие от подмены сетевых адресов и меры защиты от внедрения ложной маршрутной информации в протоколы маршрутизации, а также функции журналирования в объеме, достаточном для проведения расследований технологических нарушений.
2. Все предустановленные «по умолчанию» в настройках телекоммуникационного оборудования пароли, а также учетные записи должны быть изменены.
3. Все функции телекоммуникационного оборудования, незадействованные в процессе передачи информации, должны быть отключены, физические сетевые интерфейсы заблокированы

СТАТИСТИКА ПОПЫТОК СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ АТАК – 3 квартал 2021

ПРЕДОТВРАЩЕНО КОМПЬЮТЕРНЫХ АТАК



ФИШИНГОВЫЕ И SPAM РАССЫЛКИ

ВРЕДОНОСНОЕ ПО И ИНТЕРНЕТ РЕСУРСЫ

СЕТЕВЫЕ АТАКИ

В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ВСЕ ЦИФРЫ ИЗМЕНЕНЫ, НО ОТРАЖАЮТ ОБЩУЮ ТЕНДЕНЦИЮ

ИНТЕРЕСНЫЕ ФАКТЫ ИЗ МИРА КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ, ОКРУЖАЮЩЕГО НАС

Доставка ВПО с обновлениями ПО

В середине 2020 года вместе с обновлениями ПО SolarWinds было разослано вредоносное ПО (бэкдор SunBurst), это позволило хакерам 2 месяца получать удаленный доступ во все инфраструктуры, где использовалось это ПО

Атаки через цепочку поставщиков (supply chain kill)

Как показывает практика сервисные организации уделяют недостаточно внимания вопросам безопасности своей инфраструктуры и рабочих мест. При этом работникам этих организаций предоставляется удаленный доступ к нашей инфраструктуре, чем пользуются хакеры для проникновения в защищенный контур

Человеческий фактор

Некорректные настройки сетевого оборудования или правил маршрутизации приводили к длительной недоступности сервисов по всему миру

Охраняемая компьютерная информация

Расследование ФСБ случаев, связанных с размещением работниками ГК Россети информации о схемах сетей связи, настройках оборудования связи на внешних облачных сервисах (файловые шары, почта)
Ст. 274.1 Уголовного Кодекса Российской Федерации

Незащищенные беспроводные сети

Пользователь «Хабра» рассказал, как взломал Wi-Fi в «Сапсане» и получил доступ к данным пассажиров. В РЖД всё отрицают

Скай фишинг

Спутниковую связь по-прежнему легко прослушать.
Для организации такой станции доступно оборудование стоимостью около $300.
Установка позволяет перехватывать практически все передачи от провайдера пользователю через спутник.

Некорректные парвила сетевого доступа

Извлечение сим-карты из ИУЭ (приборы учета, реклоузеры, шлюзы ТМ) позволяет получить доступ во внутреннюю сеть предприятия

Уязвимости в ПО сетевого оборудования

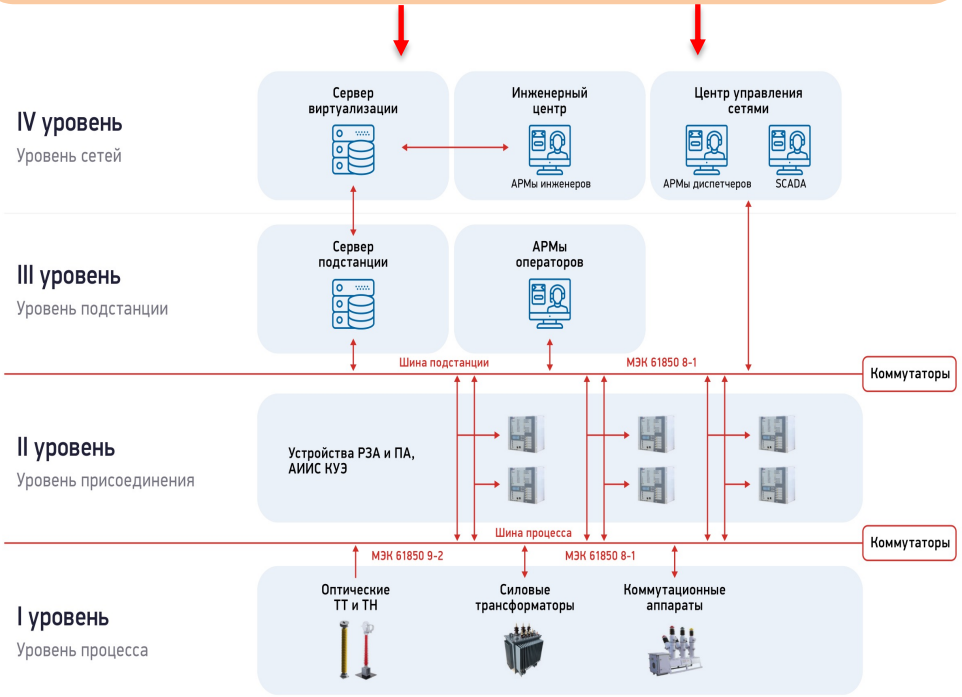
Уязвимости позволяют злоумышленнику удаленно обойти механизм аутентификации и получить доступ с привилегиями администратора, выполнить произвольный код, поменять прошивку, превратить устройство в элемент Ботнет сети

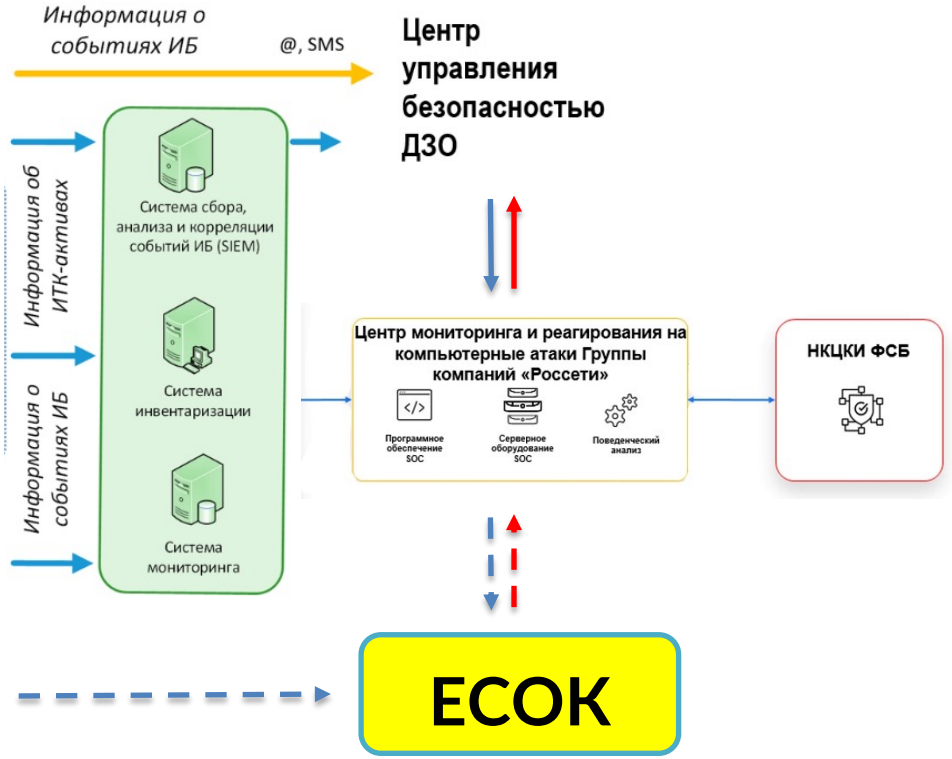
КОНЦЕПЦИЯ ОБНАРУЖЕНИЯ, ПРЕДОТВРАЩЕНИЯ И РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ АТАКИ

- подразделения (работники), эксплуатирующие ОКИИ (средства и системы связи), в том числе значимые ОКИИ
- подразделения (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) ОКИИ, в том числе значимых ОКИИ

расследование аварий (в следствии компьютерных инцидентов)

ликвидация последствий





События информационной безопасности

Информирование участников

Реагирование на компьютерные инциденты

РОССЕТИ

ВОПРОСЫ ?