kaspersky

Kaspersky Industrial Cybersecurity Conference 2021

Дмитрий Хижкин

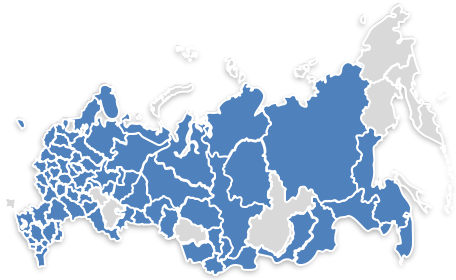
Заместитель начальника Департамента обеспечения безопасности, Россети, Россия khizhkin-di@rosseti.ru

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

РОССЕТИ

ЦИФРОВАЯ ЭЛЕКТРИЧЕСКАЯ СЕТЬ



28 сетевых компаний
субъекты критической информационной инфраструктуры

80 субъектов РФ
география присутствия

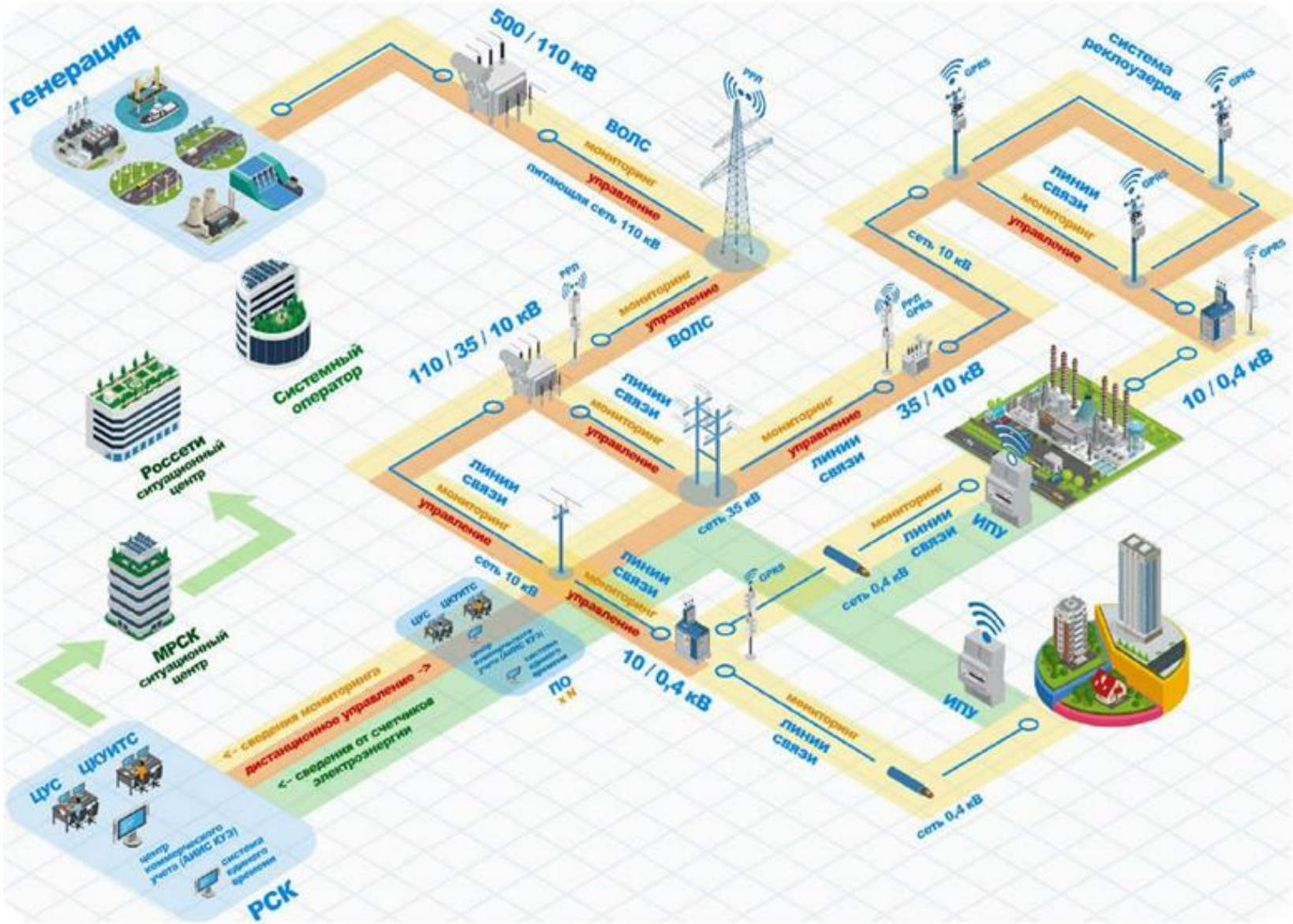
802 тыс. МВА
установленная мощность

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

125 тыс. ед.
автоматизированных рабочих мест

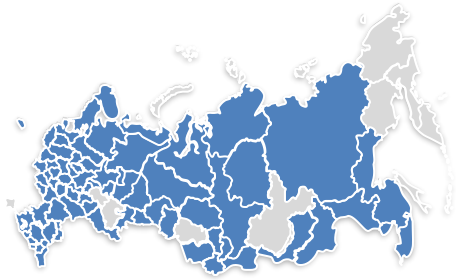
517 тыс. ед.
подстанций

217 тыс. чел.
Среднесписочная численность персонала



РОССЕТИ

ЦИФРОВАЯ ЭЛЕКТРИЧЕСКАЯ СЕТЬ



28 сетевых компаний
субъекты критической информационной инфраструктуры

80 субъектов РФ
география присутствия

802 тыс. МВА
установленная мощность

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	Определены обязанности и ответственность субъектов критической информационной инфраструктуры	Значимые объекты критической информационной инфраструктуры включены в реестр значимых ОКИИ
Доктрина энергетической безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 13 мая 2019 г. № 216	Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	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

Стратегия

Стратегия

Определены стратегические цели и КПЭ

Долгосрочная программа развития группы компаний «Россети» до 2030 года

Достижение КПЭ

Утверждена методика расчета технико-экономической целесообразности реализации мероприятий по Информационной безопасности

Приказ ПАО «Россети» от 15.20.2020 № 581

Программа «Информационная безопасность» группы компаний «Россети»

протокол Совета директоров от 07.10.2020 № pr434/1

Единая техническая политика в электросетевом комплексе

протокол Совета директоров от 8 ноября 2019 г. №378

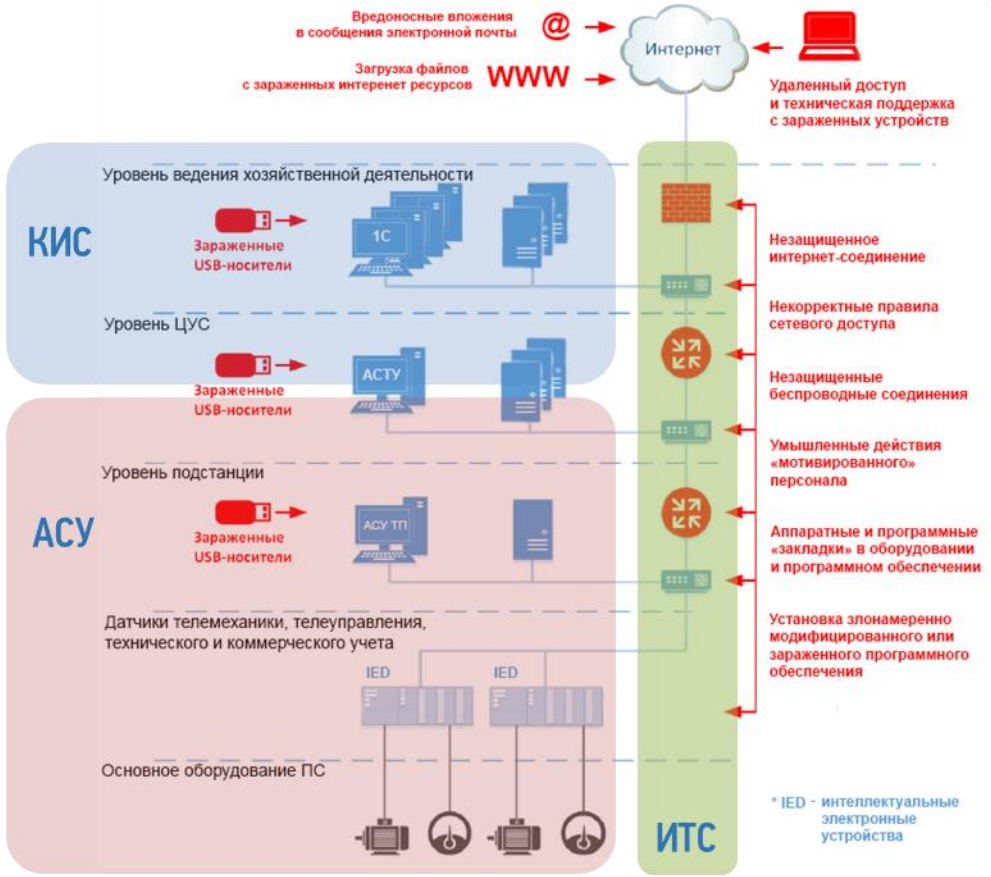
Цели, принципы, эффективные технические, технологические и организационные требования и решения по созданию системы информационной безопасности и обеспечению ее функционирования в рамках жизненного цикла ОКИИ

РИСКИ И АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ

ОБЪЕКТЫ КИИ

КИС	корпоративные информационные системы, ИСУЭ	3 548
АСУ	автоматизированные системы управления, мониторинга и диагностики	4 971
ИТС	корпоративные и технологические информационно-телекоммуникационные сети, ССПИ	1 505

СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ



компьютерные инциденты

ВОЗМОЖНЫЕ ПОСЛЕДСТВИЯ ДЛЯ ОРГАНИЗАЦИЙ ЭЛЕКТРОСЕТЕВОГО КОМПЛЕКСА

ЭКОНОМИЧЕСКИЕ ПОСЛЕДСТВИЯ

Снижение полезного отпуска (выпадающие доходы) вследствие нарушения или прекращения функционирования ОКИИ, деятельность по передаче и распределению электрической энергииэлектросетевого комплекса

Рост операционных расходов связанный с непрогнозируемыми затратами на восстановление информационной инфраструктуры и обрабатываемой информации, простоем персонала

Снижение капитализации

Репутационные и имиджевые риски

может косвенно привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка

СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Система информационной безопасности объектов критической информационной инфраструктуры

Внедрение организационных и технических мер по обеспечению информационной безопасности ОКИИ

2020 - Проверка цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических средств защиты информации в электросетевом комплексе

2021 - Формирование нормативно-технического, научного и методологического обеспечения кибербезопасности

2022 - Проектирование подсистемы безопасности эксплуатируемых ЗОКИИ и обрабатываемой информации

2024 - СМР, ПНР, ввод в эксплуатацию подсистем безопасности ЗОКИИ и обрабатываемой информации

Подразделение, ответственное за обеспечение безопасности ОКИИ, в том числе значимых ОКИИ

Мониторинг и реагирование

Разработка типовых алгоритмов обнаружения, предотвращения и ликвидации последствий компьютерных инцидентов

- Не профильный вид деятельности для энергетической компании
- Высококвалифицированные кадры
- Дежурная смена 24/7

2021

Управление системой информационной безопасности

- Модификации процессов технологического управления электросетевым комплексом в целях обеспечения его информационной безопасности — **2021**

- Укомплектование подразделений по обеспечению безопасности субъектов электроэнергетики специалистами в области информационной безопасности — **2022**

- Внедрение автоматизированных систем управления и поддержки принятия решений в области информационной безопасности — **2027**

- Повышение уровня знаний работников по вопросам ИБ, организация (пере)подготовки инженеров, техников, администраторов и операторов ОКИИ по вопросам ИБ — **пост.**

- Обеспечение эксплуатационно-технического обслуживания внедренных средств защиты информации — **пост.**

Центр управления безопасностью

«Россети Цифра» определено Корпоративным центром кибербезопасности при организации процессов обнаружения, предотвращения, а также реагирования на компьютерные атаки в отношении объектов критической информационной инфраструктуры, принадлежащих группе компаний «Россети» на праве собственности, аренде или ином законном основании

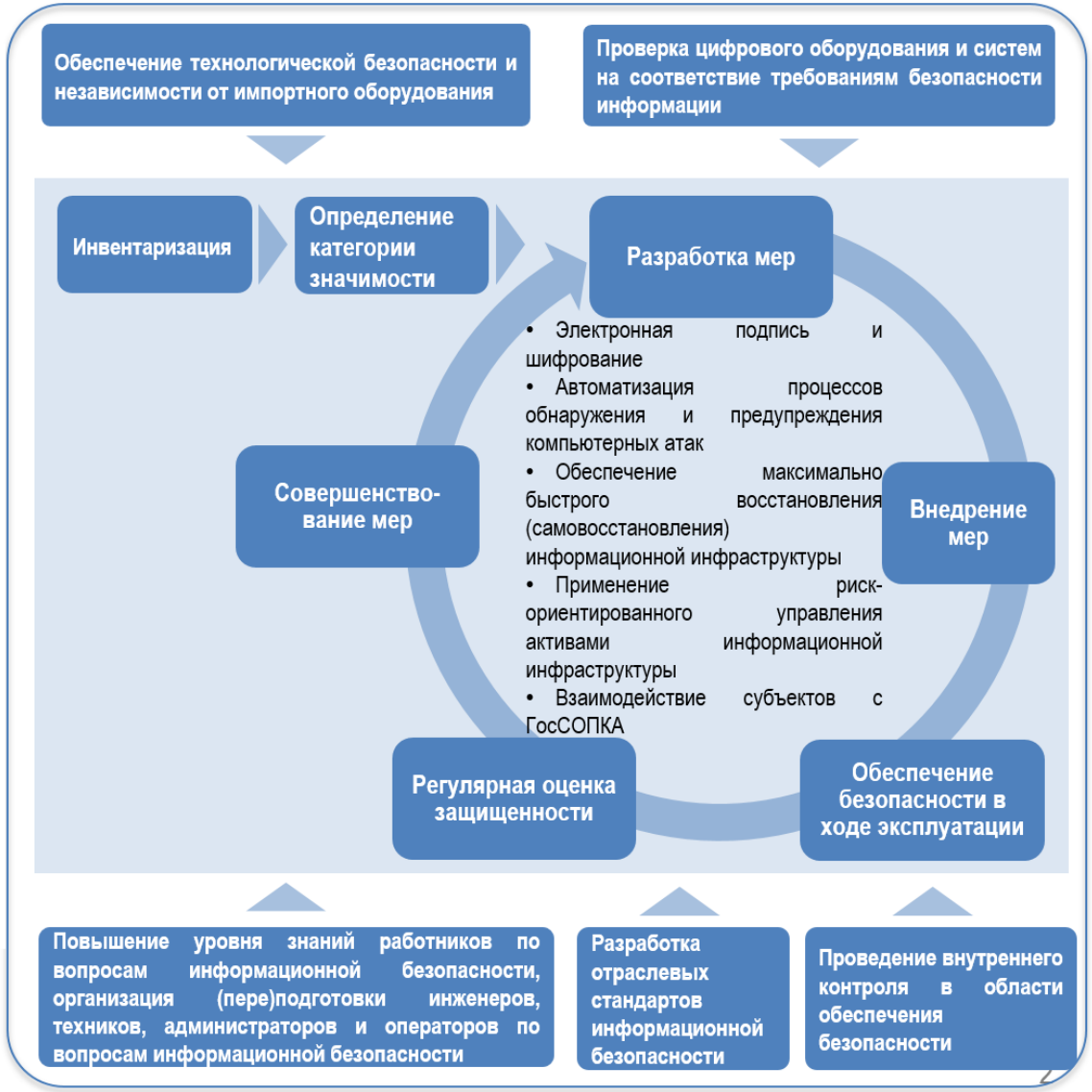
ВНЕДРЕНИЕ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОКИИ

Создается территориально-распределенная система безопасности объектов информационной инфраструктуры, включающая силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивается ее непрерывное функционирование на принципах единства подходов, требований, эффективности и надежности.

Основа стратегии – **наблюдаемость** объектов информационной инфраструктуры и протекающих информационных потоков **и доверие** к процессам

Ввод в эксплуатацию объектов информационной инфраструктуры допускается только при наличии протокола (акта) приемочных испытаний с положительным заключением о соответствии и эффективности подсистемы безопасности установленным требованиям по обеспечению безопасности.

Принципы обеспечения информационной безопасности



ПРОЦЕССЫ И МЕТРИКИ

ОПРЕДЕЛЕНО ПРОЦЕССОВ - 8 ОПРЕДЕЛЕНО ПОДПРОЦЕССОВ - 40 ОПРЕДЕЛЕНО ПОКАЗАТЕЛЕЙ - 168

Процессы	Функции и задачи, реализуемые в рамках процесса
Установление требований к обеспечению безопасности ОКИИ и обрабатываемой информации	Разработка и совершенствование организационно-распорядительных документов по обеспечению безопасности объектов информационной инфраструктуры Рассмотрение проектов ОРД, разрабатываемых по смежным функциональным направлениям деятельности Общества Инвентаризация и категорирование объектов ИИ Включение в техническое задание на создание объекта ИИ и (или) техническое задание (частное техническое задание) на создание подсистемы безопасности объекта ИИ требований к обеспечению безопасности объекта ИИ Участие в составе комиссии в аттестации нового оборудования и систем в электросетевом комплексе, оценке соответствия предлагаемых к применению на объектах электросетевого комплекса оборудования и систем требованиям по безопасности

Процессы	Функции и задачи, реализуемые в рамках процесса
Планирование мероприятий по обеспечению безопасности ОКИИ и обрабатываемой информации	Разработка ежегодного плана мероприятий по обеспечению безопасности объектов ИИ Участие в разработке программ долгосрочного развития, программы цифровой трансформации, пилотных проектов в рамках программы цифровой трансформации, планов импортозамещения Бюджетное планирование Участие в формировании Инвестиционной программы Формирование плана закупок

Процессы	Функции и задачи, реализуемые в рамках процесса
Разработка организационных и технических мер по обеспечению безопасности ОКИИ и обрабатываемой	Анализ угроз безопасности информации и разработка модели угроз безопасности информации или ее уточнение (при ее наличии) Проектирование подсистемы безопасности объекта ИИ Тестирование подсистемы безопасности объекта ИИ в ходе проектирования (макетирование или создание тестовой среды) Разработка рабочей (эксплуатационной) документации на объект ИИ (в части обеспечения его безопасности)

Процессы	Функции и задачи, реализуемые в рамках процесса
Реализация (внедрение) организационных и технических мер по обеспечению безопасности ОКИИ и обрабатываемой информации	Установка и настройка средств защиты информации, настройка программных и программно-аппаратных средств Разработка ОРД, регламентирующих правила и процедуры обеспечения безопасности объекта ИИ Внедрение организационных мер по обеспечению безопасности объекта ИИ Предварительные испытания объекта ИИ и его подсистемы безопасности Опытная эксплуатация объекта ИИ и его подсистемы безопасности Приемочные испытания объекта ИИ и его подсистемы безопасности

Процессы	Функции и задачи, реализуемые в рамках процесса
Обеспечение безопасности объектов КИИ в ходе эксплуатации	Определение лиц, ответственных за обеспечение безопасности объекта ИИ Управление (администрирование) подсистемой безопасности объекта ИИ Управление конфигурацией объекта ИИ и его подсистемой безопасности Реагирование на компьютерные инциденты в ходе эксплуатации объекта ИИ Обеспечение действий в нештатных ситуациях в ходе эксплуатации объекта ИИ Информирование и обучение персонала объекта ИИ правилам безопасной работы Проведение анализа уязвимостей объекта ИИ (эффективности принимаемых организационных и технических мер)

Процессы	Функции и задачи, реализуемые в рамках процесса
Обеспечение безопасности ОКИИ и обрабатываемой информации при выводе из эксплуатации ОКИИ	Архивирование информации, содержащейся в объекте ИИ Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации Архивирование данных об архитектуре и конфигурации значимого объекта Архивирование или уничтожение эксплуатационной документации на объект ИИ и его подсистему безопасности и ОРД по безопасности объекта ИИ

Процессы	Функции и задачи, реализуемые в рамках процесса
Контроль состояния безопасности ОКИИ и обрабатываемой информации	Определение лиц, ответственных за проведение внутреннего контроля мероприятий по обеспечению безопасности объекта ИИ Проведение внутреннего контроля за выполнением плана мероприятий Проведение внутреннего организационного и технического контроля за организацией работы по обеспечению безопасности Организация проведения внешней оценки (внешнего аудита) состояния безопасности (при необходимости) Сопровождение процесса проведения государственного (внешнего) контроля в области обеспечения безопасности значимых объектов ИИ

Процессы	Функции и задачи, реализуемые в рамках процесса
Совершенствование системы безопасности ОКИИ и обрабатываемой информации	Подготовка информационно-аналитических материалов по вопросам безопасности объектов ИИ Разработка предложений по развитию системы безопасности и меры по совершенствованию безопасности объектов ИИ Повышение осведомленности работников Общества, повышение квалийикации персонала, участие в конгресно-выставочных мероприятиях

ТИПОВАЯ СТРУКТУРА ПОДРАЗДЕЛЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Структурное подразделение, ответственное за обеспечение безопасности объектов критической информационной инфраструктуры, в том числе значимых ОКИИ, обеспечение безопасности информации конфиденциального характера

Направление, ответственное за обеспечение информационной безопасности объектов критической информационной инфраструктуры

Руководитель подразделения - 1
Специалист (технический эксперт) – 5

Установление требований к обеспечению безопасности объектов критической информационной инфраструктуры (КИС, Web-порталы, мобильные приложения, платежные системы клиент-банк, АСТУ, ИСУЭ, ИТС, сети связи);

Планирование мероприятий по обеспечению безопасности объектов критической информационной инфраструктуры;

Разработка организационных и технических мер по обеспечению безопасности объектов критической информационной инфраструктуры;

Реализация (внедрение) организационных и технических мер по обеспечению безопасности объектов критической информационной инфраструктуры;

Обеспечение безопасности объектов критической информационной инфраструктуры при выводе их из эксплуатации;

Контроль состояния безопасности объектов критической информационной инфраструктуры (эффективности принимаемых организационных и технических мер защиты);

Участие в процедурах внутренней аттестации оборудования и ПО АСТУ, АСУЭ, РЗА и связи в части ИБ;

Участие в проектах программы "Цифровая трансформация 2030" в части обеспечения кибербезопасности, разработка программы импортозамещения средств защиты информации.

Направление защиты информации

Специалист (технический эксперт) - 2

Установление требований к обеспечению безопасности обрабатываемой информации конфиденциального характера (98-ФЗ "О коммерческой тайне");

Обеспечение безопасности обрабатываемой информации конфиденциального характера (КТ, ПДн), в том числе с применением средств технической защиты конфиденциальности информации;

Обеспечение работников средствами электронной подписи, Координация и контроль за функционированием внутреннего «Удостоверяющего центра»;

Обеспечение руководства Правительственной специальной телефонной связью, а также связью специальной федеральной подсистемы конфиденциальной сотовой связи, эксплуатационно-технического обслуживание кабельной линии связи УСТМ3 Спецсвязи ФСО России;

Проведение мероприятий по технической защите объектов информатизации, обрабатывающих сведения, составляющие ГТ. Поиск скрытых технических каналов утечки информации перед проведением конфиденциальных переговоров и совещаний закрытого характера с участием Генерального директора;

Координация и контроль деятельности Филиалов и обособленных подразделений по обеспечению безопасности обрабатываемой информации конфиденциального характера;

Разработка предложений по повышению эффективности системы защиты информации.

Направление мониторинга и информационно-аналитического обеспечения (Центр управления безопасностью)

Заместитель руководителя подразделения – руководитель ЦУБ - 1
Специалист (технический эксперт) - 4

Установление требований к обеспечению безопасности объектов критической информационной инфраструктуры в ходе их эксплуатации;

Обеспечение безопасности объектов критической информационной инфраструктуры Общества в ходе их эксплуатации:

- организация мониторинга и реагирования на компьютерные атаки;
- организация эксплуатационно-технического обслуживания средств защиты информации;
- Контроль и координация действий по ликвидации последствий компьютерных инцидентов, участие в расследовании аварий в электроэнергетике;
- информирование и обучение персонала правилам безопасной работы, повышение квалификации специалистов по безопасности, участие в конгресно-выставочных мероприятиях;
- организация контроля (анализ) защищенности значимого объекта КИИ с учетом особенностей его функционирования;

Контроль и координация качества услуг при взаимодействии с центром мониторинга и реагирования на компьютерные атаки Группы компаний «Россети»;

Разработка предложений по повышению эффективности системы безопасности объектов критической информационной инфраструктуры, Бюджетное планирование, участие в формировании Инвестиционной программы, формирование Плана закупок, договорная работа в рамках обеспечения деятельности Подразделения;

Подготовка информационно-аналитических материалов по вопросам безопасности объектов критической информационной инфраструктуры и обрабатываемой информации.

Структурное подразделение по безопасности, специалисты по безопасности реализуют указанные функции во взаимодействии с подразделениями (работниками), эксплуатирующими значимые объекты критической информационной инфраструктуры, и подразделениями (работниками), обеспечивающими функционирование значимых объектов критической информационной инфраструктуры

ЭФФЕКТИВНОСТЬ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

I Определены категории физических объектов электросетевого комплекса, в отношении которых требуется реализовать мероприятия по защите:

- административные, офисные здания и помещения исполнительных аппаратов, филиалов, производственных отделений, производственных баз, ЦОК, обособленных подразделений, ДЗО;
- ЦОД (РЦОД);
- ЕЦУС (РЦУС), САЦ;
- Пункты управления РЭС филиалов, пункты ОДУ ПС;
- ПС с наличием элементов SCADA верхнего уровня;
- ПС с элементами телемеханики;
- ПС без элементов телемеханики;
- все остальные отдельно размещаемые ТП, реклоузеры, УСПД, приборы учета, микропроцессорное оборудование, монтируемое на ЛЭП и опоры, смартфоны, планшеты, ноутбуки для удаленного доступа.

+

II Определены типы ОКИИ, которые размещаются на физических объектах ЭСК:

- корпоративные информационные системы, обеспечивающие устойчивость финансово-хозяйственной деятельности, в том числе ИСУЭ;
- автоматизированные системы управления, системы мониторинга и диагностики энергетического оборудования, системы сбора и обработки технологической (диспетчерской) информации, обеспечивающие надежное снабжение потребителей электроэнергией;
- корпоративные и технологические информационно-телекоммуникационные сети, формирующие единое информационное пространство и цифровую среду взаимодействия;
- сети электросвязи, используемые для организации взаимодействия объектов КИИ;
- информация конфиденциального характера, в том числе технологическая информация, а также другая информация, представляющая коммерческую ценность в силу неизвестности третьим лицам, персональные данные.

=

III Под каждую категорию значимости, уровень защищенности ИСПДн, с учетом особенностей функционирования, размещения и эксплуатации ОКИИ разработаны **Типовые технические решения** подсистемы безопасности

Утверждена методика расчета технико-экономической целесообразности реализации мероприятий по Информационной безопасности (Приказ ПАО «Россети» от 15.20.2020 № 581)

Стоимость мероприятий по созданию подсистемы безопасности ОКИИ

НЕ ДОЛЖНА ПРЕВЫШАТЬ

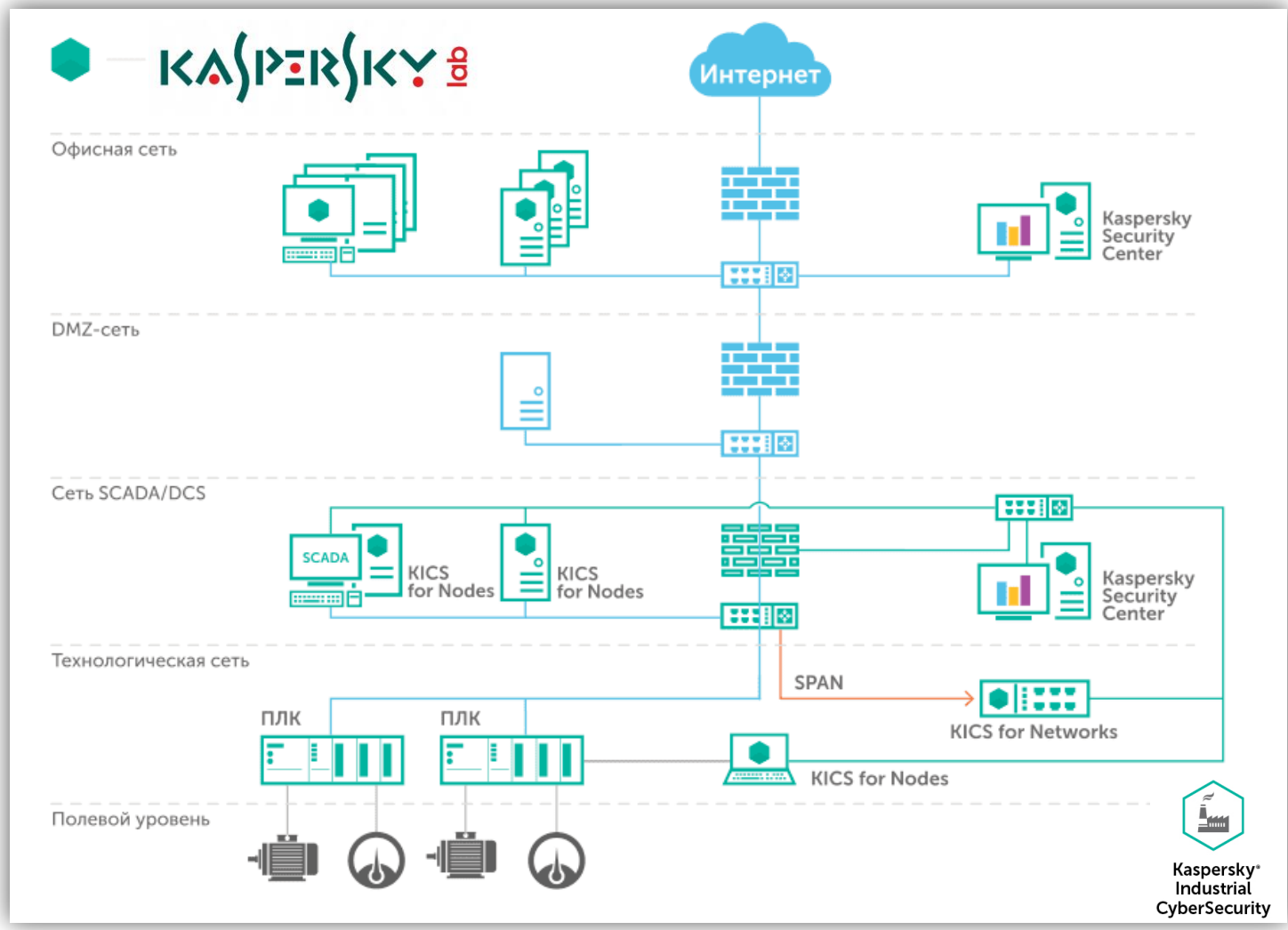
возможный потенциальный ущерб **от прекращения полезного отпуска** + потенциальный ущерб **от простоя административно-управленческого персонала,** а также непрогнозируемых затрат на восстановление

ТЕХНИЧЕСКИЕ РЕШЕНИЯ

Разработан альбом типовых технических решений по информационной безопасности объектов КИИ распределительного электросетевого комплекса (распоряжение от 09.03.2021 №72р)

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 информации и данных при их передаче по каналам связи;
6. Средства защищенного удаленного доступа в ЛВС, в том числе средства терминального доступа;
7. Средства резервного копирования, в том числе средства создания и хранения резервных копий;
8. Средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.



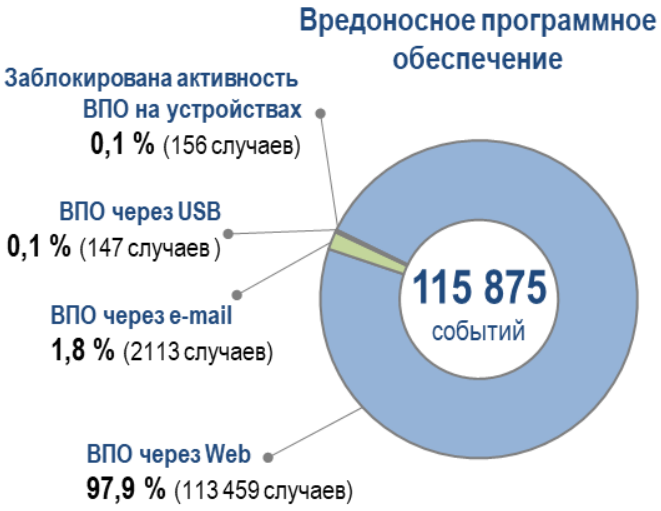
КОРПОРАТИВНЫЙ ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

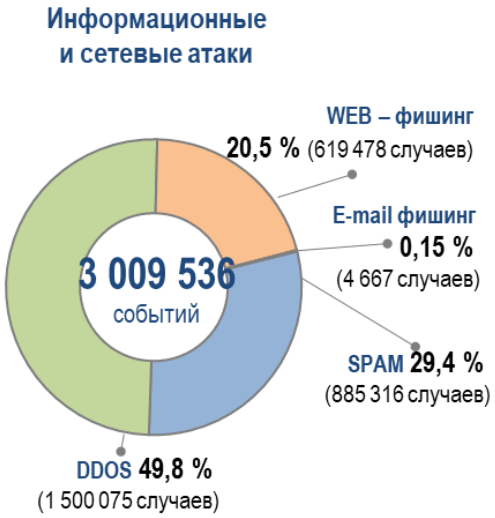
Заключено соглашение о взаимодействии ФСБ РФ, ПАО «Россети», «Россети Цифра» при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак

Получена лицензия ФСТЭК России на деятельность по мониторингу состояния информационной безопасности, приказ ФСТЭК России от 19.02.2021 №34-л

ОСНОВНЫЕ ЗАДАЧИ КОРПОРАТИВНОГО ЦЕНТРА

- формирование и поддержание в актуальном состоянии информации о контролируемых информационных ресурсах, сбор и анализ данных о состоянии информационной безопасности в контролируемых информационных ресурсах
- обнаружение, предупреждение и ликвидация последствий компьютерных атак, направленных на контролируемые информационные ресурсы
- проведение мероприятий по оценке степени защищенности контролируемых информационных ресурсов
- проведение мероприятий по установлению причин компьютерных инцидентов, вызванных компьютерными атаками на контролируемые информационные ресурсы
- осуществление взаимодействия с ГосСОПКА (НКЦКИ ФСБ России), Ведомственным центром ГосСОПКА Минэнерго России, Энерго ЦЕРТ на базе АЦЭ
- информирование субъектов электроэнергетики, которым принадлежат контролируемые информационные ресурсы по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак



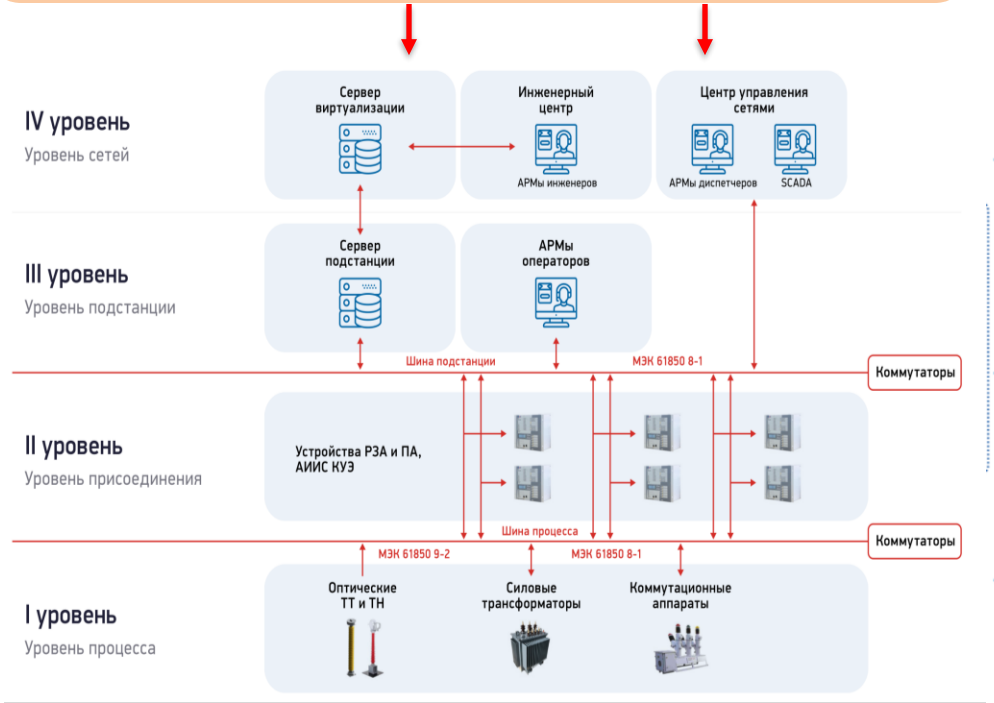


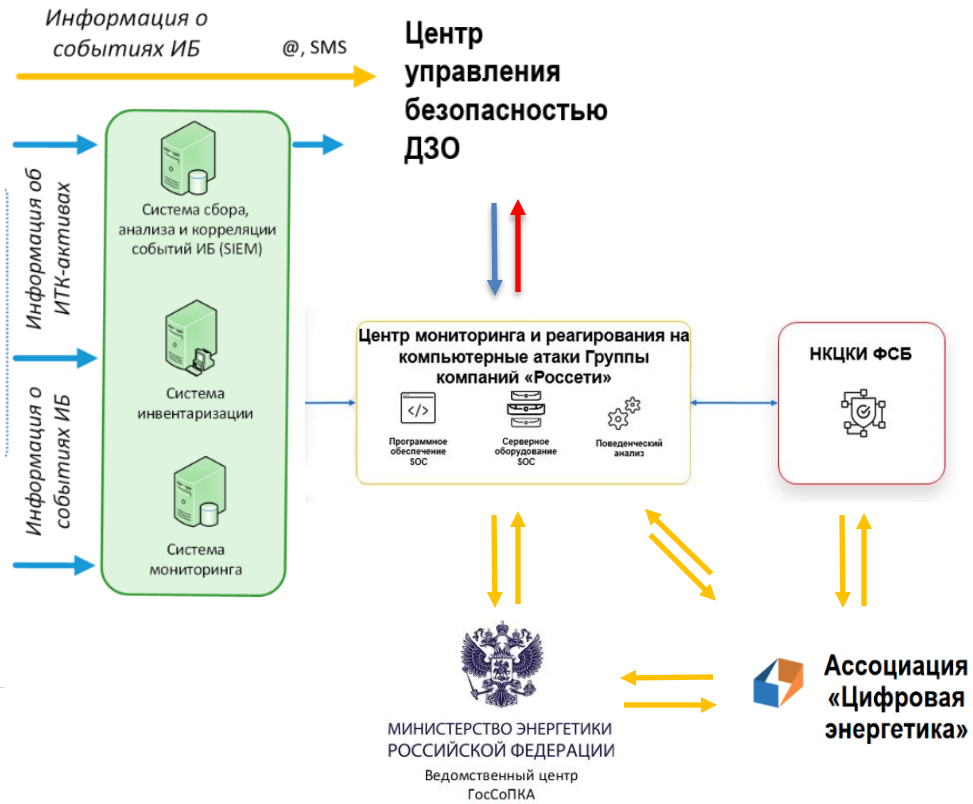
КОНЦЕПЦИЯ ОРГАНИЗАЦИИ ПРОЦЕССОВ ОБНАРУЖЕНИЯ, ПРЕДОТВРАЩЕНИЯ И РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ АТАКИ

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

расследование аварий

ликвидация последствий



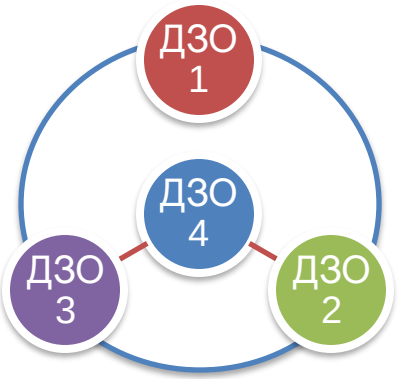


События информационной безопасности

Информирование участников

Реагирование на компьютерные инциденты

АТАКА ЧЕРЕЗ «ПОДРЯДЧИКОВ» (SUPPLY CHAIN)



Threat Intelligence Center

Microsoft

Exchange Servers
with 0-day exploits

02.03.2021

03.03.2021 | **04.03.2021** | **23.03.2021** | **24.03.2021** | **07.05.2021**

SOC@
rosseti.digital

ДЗО 1 → ДЗО 2 → ДЗО 3 → ДЗО 4

Уведомление о 0-day RCE-уязвимости Microsoft Exchange

1. Эксплуатация уязвимости ProxyLogon (CVE-2021-26855)
2. Установка WebShell
3. Загрузка ВПО
4. Получение учетных записей
5. Компрометация АРМ администратора
5. Разведка инфраструктуры
6. Коммуникация с CnC

1. Подключение к прокси серверу, установка ВПО
2. Разведка инфраструктуры
3. Компрометация контроллера домена

1. Компрометация контроллера домена
2. Подключение к АРМ администратора
3. Компрометация прокси, установка ВПО удаленного управления

1. Компрометация контроллера домена
2. Ключ реестра Portproxy
3. Вредоносный драйвер C:/Windows/win.sys
4. Установка сервиса HeadQuaterDep
для запуска вредоносного кода C:\windows\ConsoleApplication8.Exe
5. Действия зафиксированы корпоративным Центром кибербезопасности

КОНТРОЛЬ (АНАЛИЗ) ЗАЩИЩЕННОСТИ ОКИИ

в Группе компаний Россети в конце 2020 года выпущен Стандарт «Руководящие указания по инструментальной оценке (анализу уязвимостей) информационной безопасности объектов информационной инфраструктуры Цифровой сети».

РЕЗУЛЬТАТЫ ПРОВЕДЕНОГО ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ (2020 год)

97 серверов работают на программном обеспечении, имеющем известные уязвимости

48 из них до сих пор уязвимы к атаке «EternalBlue» или «BlueKeep»

16 из них до сих пор уязвимы к атаке «WannaCry», «Petya», «BadRabbit» и т.д.

16 из них используют версию Remote Desktop Services (RDP), которая позволяет атакующему, не прошедшему проверку подлинности, удалённо выполнить произвольный код на атакуемой системе

В соответствии с п. 4 статьи 6. 187-ФЗ Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ФСБ России) проводит оценку безопасности критической информационной инфраструктуры.

В течение 2021 гг. в 6 ДЗО ПАО «Россети» проведены работы по оценке безопасности объектов КИИ с участием представителей ФСБ России

ПОВЫШЕНИЕ КВАЛИФИКАЦИИ, ПОДГОТОВКА (ПЕРЕПОДГОТОВКА) СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Повышение квалификации и переподготовка специалистов

- в течение 2020 года в Группе компаний Россети 40 специалистов по информационной безопасности успешно завершили обучение по программам повышения квалификации;
- в течение 2021 года в ДЗО ПАО «Россети» 35 специалистов по информационной безопасности успешно завершили обучение по программам повышения квалификации.

Электронный курс по программе «Информационная безопасность»

разработан электронный учебный курс «Информационная безопасность», предназначенный для обучения основам информационной безопасности работников ПАО «Россети» с возможностью последующего тестирования для проверки усвоенного материала.

Подготовка специалистов по информационной безопасности

НТЦ ФСК и НИУ МЭИ подписали соглашение о создании базовой кафедры кибербезопасности и информационных технологий. Цель создания кафедры - практическая подготовка бакалавров и магистров соответствующего профиля для электроэнергетики.

На кафедре будут реализованы образовательные программы по направлениям «Информационная безопасность» и «Прикладная информатика», а также будут проводиться научно-прикладные исследования в области кибербезопасности систем и средств автоматизации объектов электросетевого комплекса.

В НАСТОЯЩЕЕ ВРЕМЯ В ГРУППЕ КОМПАНИЙ РАБОТАЕТ

БОЛЕЕ 350 СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРОВЕРКА ЦИФРОВОГО ОБОРУДОВАНИЯ И СИСТЕМ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

2022 Обеспечение проверки качества поставляемого цифрового оборудования и программного обеспечения

Приказ ПАО «Россети» от 28.08.2020 № 391 «Об утверждении Методики проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических средств защиты информации в электросетевом комплексе»

2020 Создана лаборатория информационной безопасности на базе АО «НТЦ ФСК ЕЭС»

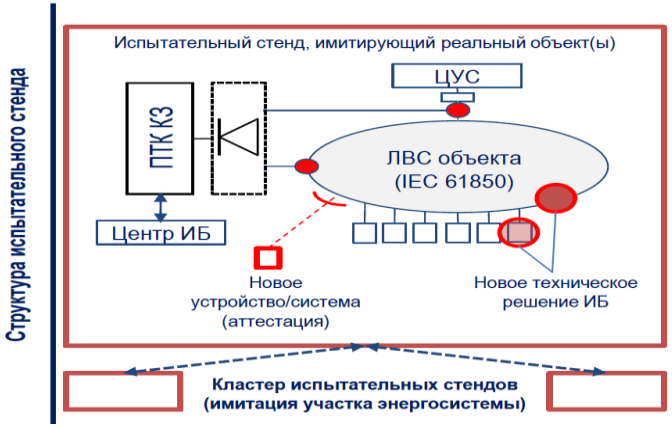
2022 Создание испытательной лаборатории и полигона для проведения киберучений на базе АО «ФИЦ»

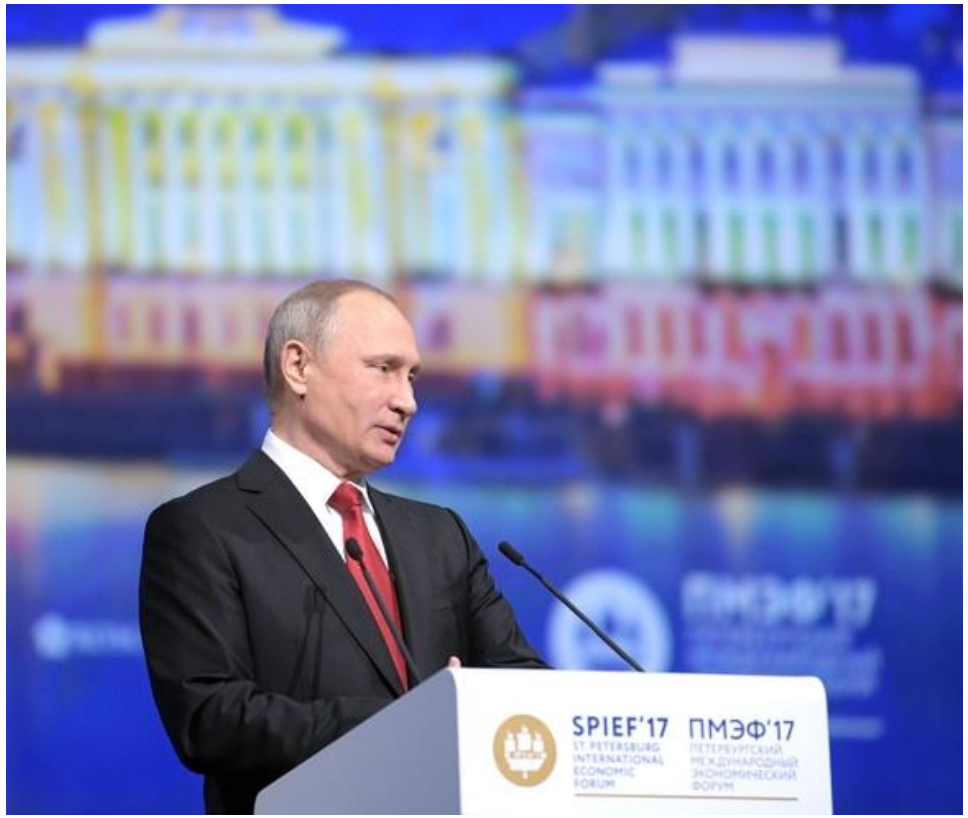
2022 Разработка профилей защиты для оборудования и ПО, применяемых в электросетевом комплексе

Проверка цифрового оборудования и систем на соответствие требованиям безопасности информации в электросетевом комплексе,
в том числе проверка ТСЗИ на совместимость с АСТУ, проводится в соответствии с Положением ПАО «Россети» о Единой технической политике в электросетевом комплексе, утвержденным решением Совета директоров ПАО «Россети» (протокол от 07.10.2019 № 378), Методикой ПАО «Россети» проведения проверки качества (аттестации) оборудования, материалов и систем в электросетевом комплексе, утвержденной приказом ПАО «Россети

ПРОВЕДЕНА ИЛИ ПРОХОДИТ ПРОВЕРКУ

Устройства релейной защиты и автоматики
Средства связи
Средства контроля, измерений и системы мониторинга
Автоматизированные системы управления
Интеллектуальные приборы учета, устройства сбора и передачи информации





Владимир Путин:
«**Все решения должны приниматься с учётом обеспечения информационной безопасности государства, бизнеса и граждан**».

Из выступления на Петербургском международном экономическом форуме,
2 июня 2017 г.