**Министерство энергетики Российской Федерации**

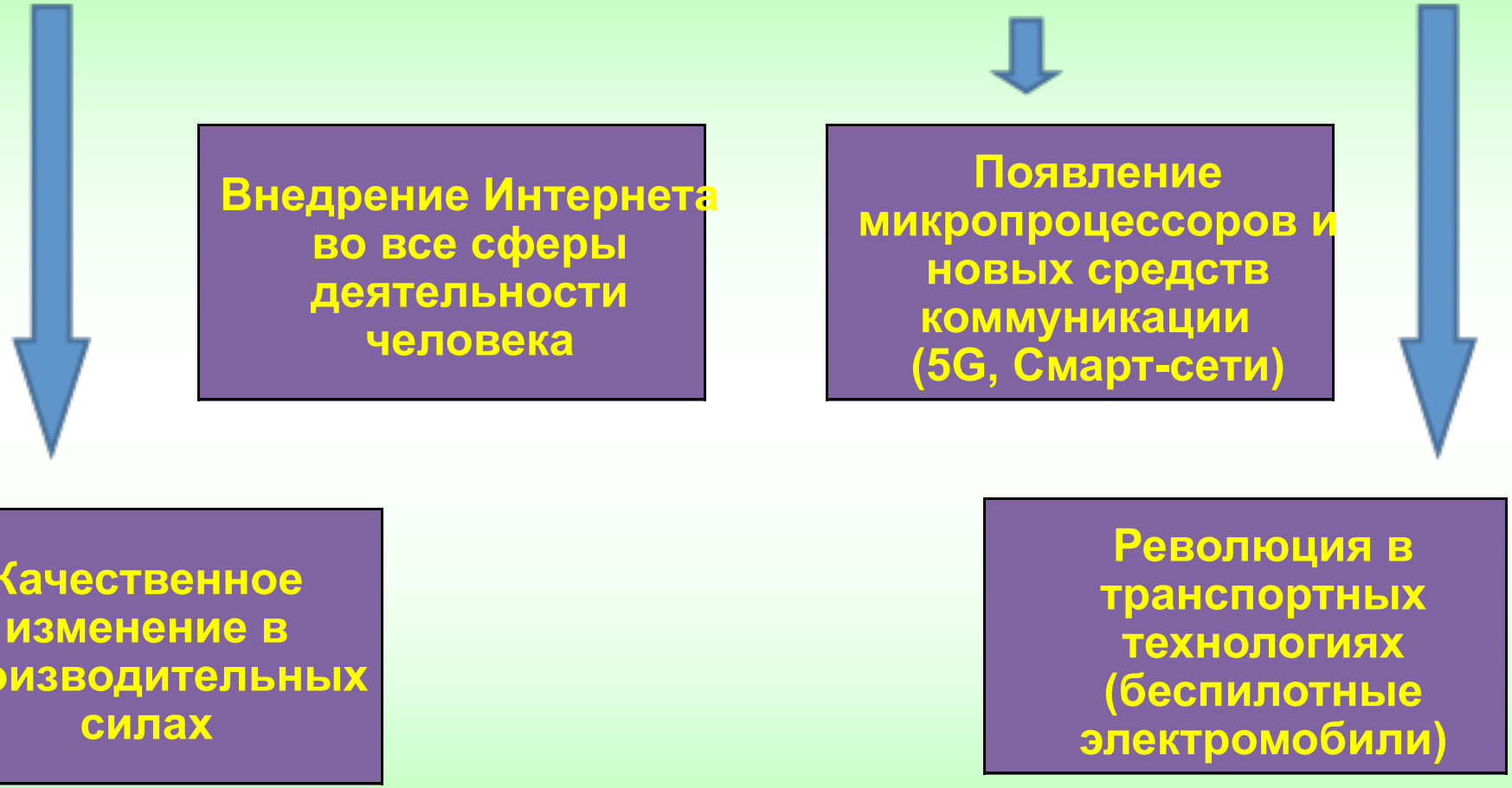
**14 выставка «Информационная безопасность России»**

# Вопросы создания комплексной системы обеспечения информационной безопасности центрального аппарата Минэнерго России

**Выступление заместителя начальника отдела информационных технологий Министерства энергетики Российской Федерации Юрия Михайловича Погожева**
**E-Mail: PogozhevYM@minenergo.gov.ru**
**Тел. +7 916 211 06 91;  (495)631 98 13**

Министерство энергетики Российской Федерации

# ЦИФРОВИЗАЦИЯ МИРОВОЙ ЭКОНОМИКИ. XXI ВЕК



**Министерство энергетики Российской Федерации**

# Распоряжением Правительства Российской Федерации от 28.07.2017 года №1632-р утверждена программа «Цифровая экономика Российской Федерации»

**Электронная (цифровая, веб, интернет) экономика — экономическая деятельность, основанная на цифровых технологиях. Это не столько разработка и продажа программного обеспечения, сколько электронные товары и сервисы, производимые электронным бизнесом и электронной коммерцией.**

**Дмитрий Медведев 16.10.2018 на ежегодном форуме «Открытые инновации»: Стоимость программы – 1 трлн рублей, всего на развитие «цифры» направим 2 трлн рублей государственных инвестиций.**

# Направления кибератак

**Банки, банкоматы**

**корпоративный сектор**

**блокчейн и криптовалюты**

**Интернет вещей (автомобили, приборы)**

**Домашние гаджеты (роутеры, веб-камеры, датчики)**

# Технологические особенности:

- **Автоматизация кибератак** на банкоматы. В 2017 году **вредоносные программы** для банкоматов стали предоставляться **как услуги** (ATM malware-as-a-service);
- **Снижение квалификации атакующих**, использующих общедоступные инструменты, в том числе созданные для тестирования систем защиты;
- Рост активности в тематических Telegram-каналах, предлагающих **обучение взлому и «сотрудничеству»** с целью заработать на создании **ботнет-сетей.**

Директор проектного направления Group-IB Антон Фишман
Атаки WannaCry, NotPetya, Bad Rabbit показали всему миру, насколько легко сделать эффективный шифровальщик, способный вывести из строя серверы организаций в разных странах мира.
Молниеносная и зачастую довольно простая атака на криптовалютные сервисы и блокчейн-стартапы приносит киберпреступникам "миллионы долларов прибыли с минимальным риском".

**Министерство энергетики Российской Федерации**

**Отчет Anti-Phishing Working Group - публикация агентства Reuters 24.05.2018**

**с начала 2017 года похищено $1,2 млрд в криптовалюте**

**Алиса Мельникова, Центробанк РФ на Московском биржевом форуме 10.04.2018**

**с начала 2018 года совершены 22 крупные мошенические схемы похищено $1,36 млрд в криптовалюте**

**Д. Медведев: За счет кибератак Россия в 2017 году потеряла 600 млрд руб мировые потери - $ 1 трлн**

Методы доступа (Microsoft Advanced Threat Protection на основе анализа данных второго полугодия 2017 пользователей Office 365):

**Фишинг – 53%;** Ежемесячно 189-200 млн фишинговых писем; по России -7,01 фишинговых сайтов на 1000 хостов в мире -5,85

**Вредоносное ПО – 29%; Java-бэкдоры – 11%; Остальное – 7 %.**

**Министерство энергетики Российской Федерации**

**Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТа) Центробанка**

## Уязвимости, из-за которых кибератаки на банки были проведены успешно:

- человеческий фактор;
- отсутствие актуальных обновлений на используемых операционных системах и программах;
- слабые пароли;
- несегментированные сети;
- проблемы с системами управления событиями информационной безопасности;
- неправильная настройка межсетевого экранирования;
- использование устаревших антивирусов.

**Министерство энергетики Российской Федерации**

**Ответ государства:**

## Указ Президента Российской Федерации от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

"Возложить на Федеральную службу безопасности РФ функции федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ - информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории РФ, в дипломатических представительствах и консульских учреждениях РФ"

**Министерство энергетики Российской Федерации**

**Ответ государства:**

В США создано — **Агентство по кибербезопасности и защите инфраструктуры**.
Соответствующий законопроект в середине ноября 2018 года подписал американский президент Дональд Трамп. Ведомство будет сформировано на базе Министерства внутренней безопасности.

Эксперты считают, что проблема безопасности в киберпространстве действительно актуальна для Вашингтона, однако её решение — лишь **предлог для развития концепции наступательных операций** в данной сфере. По мнению аналитиков, новое агентство должно «прикрыть тыл» американских войск в развязанных ими кибервойнах.

## Министерство энергетики Российской Федерации

# Объекты информационной системы Минэнерго России, подлежащие защите

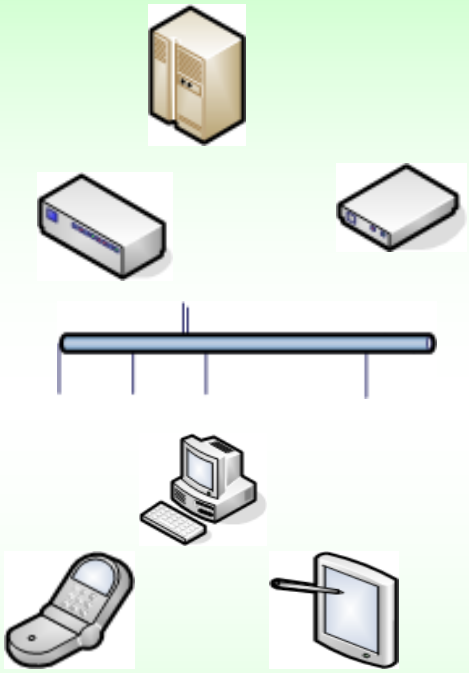
1. Сервера

2. Коммуникационное оборудование

3. Каналы передачи информации

4. Автоматизированные рабочие места

5. Средства «мобильного клиента»



6. Общее программное обеспечение — Операционные системы, офисные приложения, почтовые службы, интернет-браузеры

7. Специальное программное обеспечение — Ведомственная информационная система, бухгалтерские программы, кадровая задача, правовые базы данных

**Министерство энергетики Российской Федерации**

# Факторы, влияющие на развитие информационной системы (ИС) Минэнерго России и используемые ИТ

## Прогноз на увеличение:

- **Числа взаимодействующих сетей (открытых и закрытых):** СМЭВ, МЭДО, ЕСИА, ГАСУ и т.д.
- **- количества сервисов / услуг, доступных как из сети Интернет, так и из внутренней сети;**
- **централизация всей информации на серверах ИС (виртуализация);**
- **использования мобильных устройств для доступа к ресурсам ИС;**
- **риски использования аутсорсинговых ИТ-компаний.**

**Министерство энергетики Российской Федерации**

## Базовые меры кибербезопасности :

| | |
|---|---|
| **Безопасность приложений** | **Аудит программного кода, защита сессий, контроль корректности вводимых данных, безопасность скриптов** |
| **Безопасность серверов и рабочих станций** | **Защита от вредоносных программ, обнаружение попыток взлома, контроль системных журналов, защита от вредоносных программ** |
| **Безопасность конечных пользователей** | **Антивирусные средства, использование фильтров фишинга, безопасное выполнение скриптов, защита от атак социальной инженерии** |
| **Защита от атак и утечек** | **Использование межсетевых экранов, применение SIEM и DLP систем** |

**Министерство энергетики Российской Федерации**

## Система комплексной защиты информационных ресурсов Минэнерго России должна обеспечивать:

1. Защиту от несанкционированного доступа к информации по установленному классу защищенности

2. Криптографическую защиту данных, передаваемых по каналам связи

3. Межсетевое экранирование, экранирование фрагментов локальной вычислительной сети, разделение ресурсов по правам доступа

4. Автоматическую регистрацию событий информационной безопасности

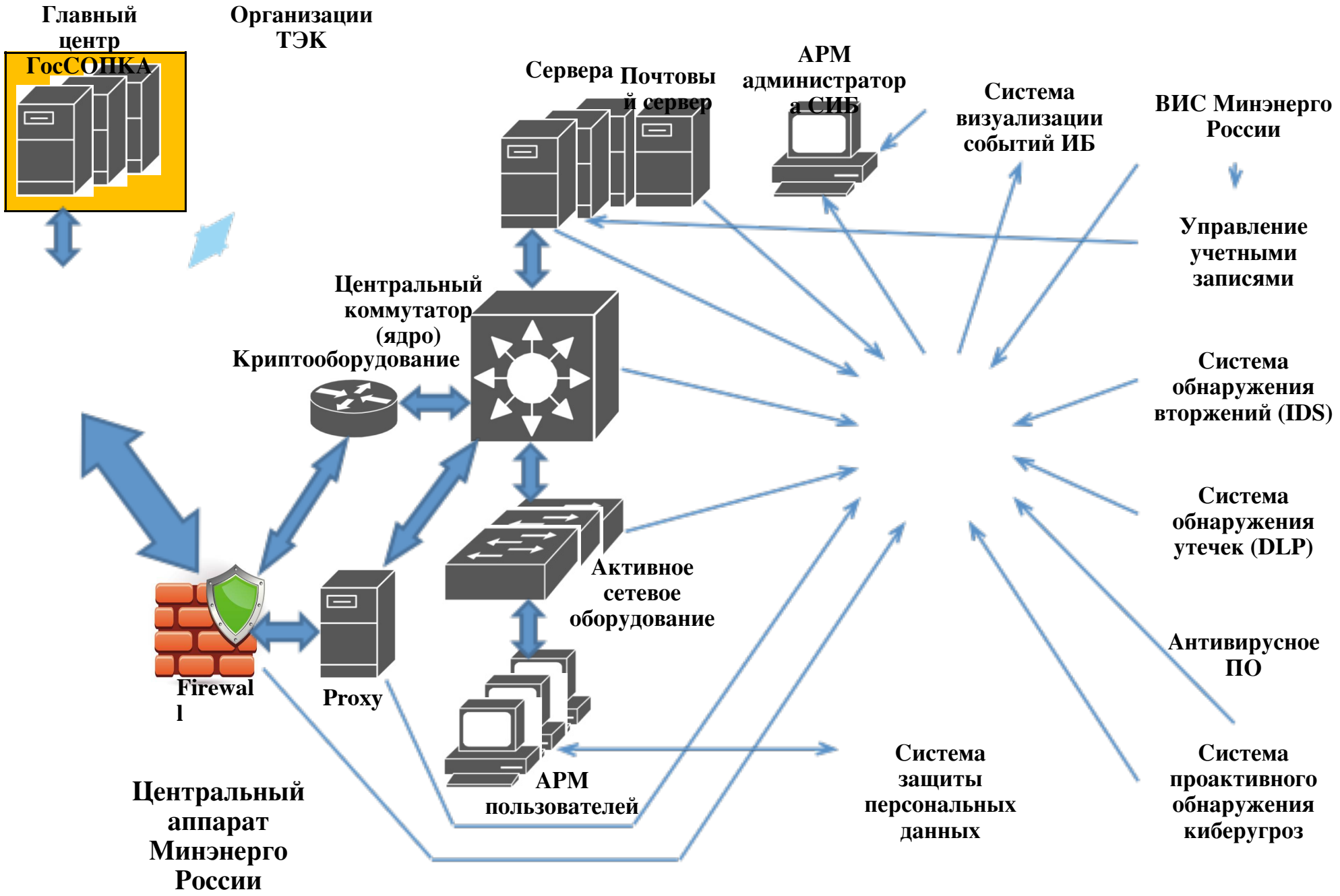
5. Комплексную антивирусную защиту программного обеспечения

6. Инвентаризацию и аудит программного и аппаратного обеспечения

7. Защиту персональных данных

8. Контроль за подозрительной активностью программного обеспечения

# Структурная схема СИБ Минэнерго России



**Министерство энергетики Российской Федерации**

# Спасибо за внимание!

**Контакты:**
**Отдел информационных технологий**
**Департамент проектного управления и обеспечения деятельности Министерства Минэнерго России**
**Погожев Юрий Михайлович**
**E-Mail: PogozhevYM@minenergo.gov.ru**
**Тел. +7 916 211 06 91;  (495)631 98 13.**