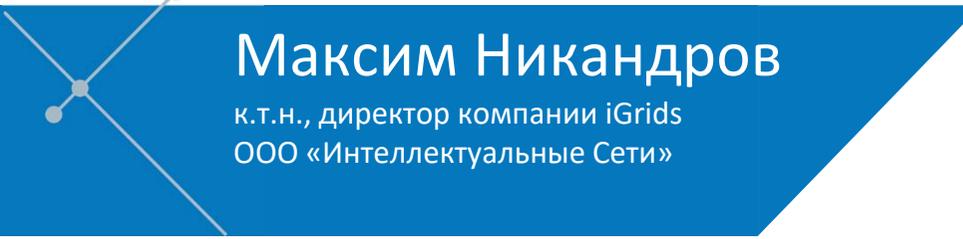




**Отраслевая система аттестации устройств РЗА.  
Сертификация микропроцессорных устройств РЗА на  
соответствие требованиям информационной  
безопасности в системе ФСТЭК России**



**Максим Никандров**

к.т.н., директор компании iGrids  
ООО «Интеллектуальные Сети»





РОССИЙСКАЯ ФЕДЕРАЦИЯ  
**ФЕДЕРАЛЬНЫЙ ЗАКОН**

**О безопасности критической информационной  
инфраструктуры Российской Федерации**

Принят Государственной Думой	12 июля 2017 года
Одобен Советом Федерации	19 июля 2017 года

**Статья 1. Сфера действия настоящего Федерального закона**

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также – критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

## Изменение законодательства

**ФЕДЕРАЛЬНЫЙ ЗАКОН от 26.07.2017 № 187-ФЗ  
«О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ  
ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ  
РОССИЙСКОЙ ФЕДЕРАЦИИ»**

**(принят ГД ФС РФ 12.07.2017)**



Публичное акционерное общество  
«Российские сети»

## РАСПОРЯЖЕНИЕ

30.05.2017

Москва

№

282р

Об утверждении требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса Группы компаний «Россети»

В целях нейтрализации угроз информационной безопасности электросетевого комплекса Группы компаний «Россети»:

1. Утвердить требования к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса Группы компаний «Россети» (далее - Требования) согласно приложению 1 к настоящему распоряжению.

2. ДЗО ПАО «Россети», указанным в приложении 2 к настоящему распоряжению, привести внутренние документы ДЗО об обеспечении информационной безопасности в соответствии с Требованиями.

Срок: в течение 1 месяца с даты выхода настоящего распоряжения.

3. Контроль за исполнением настоящего распоряжения оставляю за собой.

# Изменение законодательства

## Распоряжение ПАО «Россети» №282р от 30.05.2017

### «Об утверждении требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса Группы компаний «Россети»

## Изменение законодательства

Компоненты АСТУ, поставляемые и эксплуатируемые на объектах электросетевого комплекса Группы компаний «Россети», должны обладать ВСЗИ. Изготовитель АСТУ и/или электрооборудования обязан подтвердить соответствие ВСЗИ настоящим Требованиям в форме сертификации указанного оборудования и/или программного обеспечения в системе сертификации ФСТЭК России на соответствие:

- ЗБ, разработанному с учетом Требований настоящего документа (с предоставлением, при необходимости, Обоснования соответствия – см. ниже);
- требованиям руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» по 4 уровню контроля.

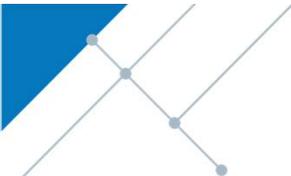
**Сертификации  
оборудования и/или  
программного обеспечения  
в системе сертификации  
ФСТЭК России по НДВ4 и  
ОУД4+**

## Получение сертификатов ФСТЭК

Технические, криптографические, программные и другие средства, **предназначенные для защиты сведений, составляющих государственную тайну**, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках системы сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных Федеральной службой безопасности Российской Федерации.





## Запросы в ФОИВ

Распоряжение 282р ПАО «Россети» и приказ № 55 ФСТЭК России приравнивали контроллеры АСУТП и программное обеспечение систем управления в промышленности к **средствам технической защиты информации и обеспечения безопасности информационных технологий**. В итоге предъявляемые требования в большинстве своем избыточны, а иногда не реализуемы для технологических систем управления.

В настоящее время компании-разработчики электротехнического оборудования не имеют лицензий ФСТЭК, так как обеспечение безопасности информационных технологий и выпуск защищенных средств обработки информации не являются профильными для данных организаций. **Получение лицензии требует дополнительных разовых и долгосрочных финансовых затрат, наличия в штате дефицитных специалистов по информационной безопасности, что, в свою очередь, приведет к существенному удорожанию конечного продукта для конечного заказчика и снижению конкурентоспособности производителей оборудования.**

**Обращение в Министерство  
энергетики РФ, Министерство  
промышленности и торговли РФ,  
ФСТЭК России**

## Запросы в ФОИВ

Законодательством Российской Федерации установлена обязательность применения сертифицированных средств для защиты информации, содержащей сведения, составляющие государственную тайну, а также информации ограниченного доступа, являющейся государственным информационным ресурсом.

Автоматизированные системы управления промышленными и энергетическими комплексами, как правило, не предназначены для обработки указанной информации. Следовательно, сертифицированные средства защиты информации могут применяться в данных автоматизированных системах в случае принятия субъектом критической информационной инфраструктуры такого решения.

**Ответ ФСТЭК России от  
28.02.2019**

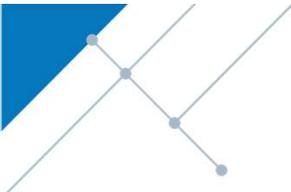
## Запросы в ФОИВ

Таким образом, Минэнерго России поддерживается сертификация средств защиты информации по требованиям безопасности информации, а также средств контроля (анализа) исходных текстов программного обеспечения на отсутствие недекларированных возможностей организациями с лицензией, соответствующей действующему законодательству.

Для разработки специальных профилей отдельного класса автоматизированных систем управления промышленными и энергетическими комплексами со встроенными средствами защиты требуется: определение подходов к их разработке, разработка, а также оценка последствий их применения как для действующих на объектах энергетики Российской Федерации интеллектуальных систем управления, разрабатываемых систем управления, так и для иных отраслей (далее – модель оценки).

В этой связи, предлагаем направить в установленном действующим законодательством Российской Федерации порядке предложения по разработке профилей защиты с учетом требуемой модели оценки.

**Ответ Министерства  
энергетики РФ от 21.03.2019**



## Запросы в ФОИВ

«О безопасности критической информационной инфраструктуры Российской Федерации», требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом ФСТЭК России от 25 декабря 2017 г. № 239 и Требованиями к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденными приказом ФСТЭК от 21 декабря 2017 г. № 235, для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться сертифицированные на соответствие требованиям по безопасности информации средства защиты информации или средства, прошедшие оценку соответствия в форме испытаний или приемки в соответствии с Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

**Ответ Министерства  
промышленности и торговли  
РФ от 19.03.2019**



## Запросы в ФОИВ

Одновременно с этим, отмечаем важность указанных Вами ожидаемых эффектов от реализации предложений, указанных в Обращении, и считаем необходимым провести дополнительную проработку вопроса в рамках межведомственного взаимодействия совместно с Минэнерго России, ФСТЭК России и ПАО «Россети» по вопросам, находящимся в компетенции Минпромторга России.

**Ответ Министерства  
промышленности и торговли  
РФ от 19.03.2019**