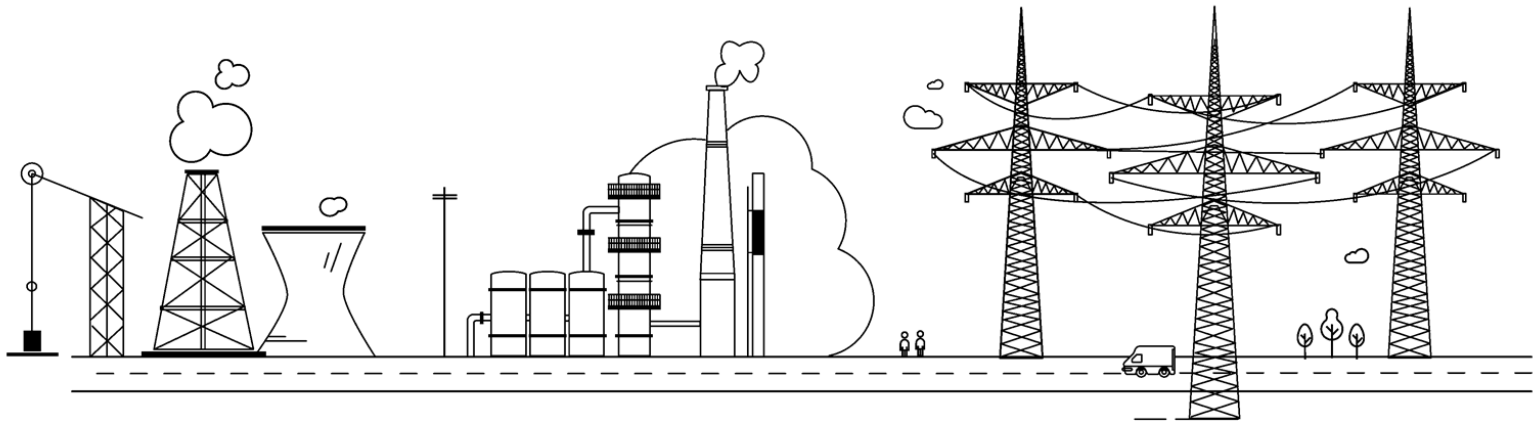
Практика реализации ФЗ-187 и импортозамещения в сфере ИБ: проблемные вопросы



Законодательство о КИИ: ФЗ-187

требования законодательства не вносят практически ничего нового по сравнению с группой стандартов ISO 27xxx (ГОСТ Р ИСО/МЭК 27xxx)

ФЗ-187 ≈ ISO 27xxx

Обязательность исполнения

Рекомендательный характер (Best Practice)

Законодательство о КИИ – новое законодательство (2017г), ещё не избавившееся от «детских болячек».

«Чтоб ты жил во время перемен!»
китайское проклятие

ФЗ-187

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

8) субъекты критической информационной инфраструктуры - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

субъекты КИИ - Организации, которым на законном основании принадлежат ИС, функционирующие в сфере (перечень сфер деятельности)

Казнить нельзя помиловать

субъекты КИИ - Организации, которым на законном основании принадлежат ИС, функционирующие в сфере (…)

ИС, функционирующие в сфере (…)

?

Организации, …, функционирующие в сфере (…)

субъекты КИИ - Организации, которым принадлежат такие ИС

субъекты КИИ – практически все Организации

Казнить нельзя помиловать - 2

ПП-127
Правила категорирования ОКИИ
3. Категорированию подлежат ИС, которые обеспечивают процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры в областях (сферах), установленных пунктом 8 статьи 2 ФЗ-187

процессы … в областях (сферах), установленных ФЗ-187

?

… осуществления видов деятельности субъектов КИИ в областях (сферах), установленных ФЗ-187

Категорированию подлежат ИС, обеспечивающие указанные процессы

Категорированию подлежат все ИС субъекта КИИ

Кто «незаслуженно» попадает под классификацию субъектов КИИ

- Управляющие компании холдингов – по сути предприятия «сдают» в аренду свой персонал, т.е. в своем роде являются «аутстаффинговыми» компаниями. Но по справочнику ОКВЭД ведут деятельность в одной из сфер, указанных в ФЗ-187
- Различные компании, оказывающие услуги субъектам КИИ. Например «бухгалтерская» компания, оказывающая услуги ведения бухгалтерского учета.
- Яркий пример – агентство по продаже авиабилетов (турагентства). Они используют системы бронирования авиакомпаний, по коду ОКВЭД попадают в сферы деятельности из ФЗ-187
- ….

ПП-127

Правила категорирования ОКИИ

5. Категорирование включает в себя:

а) определение процессов, указанных в пункте 3 настоящих Правил;

б) выявление процессов, нарушение которых может привести к негативным последствиям - критические процессы;

в) определение ИС, которые обрабатывают информацию, необходимую для обеспечения критических процессов;

г) формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию (далее - перечень объектов);

д) оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

е) присвоение каждому из объектов критической информационной инфраструктуры одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

Пункты г), д), е) не имеют никакой ссылки к пункту в) !!!

ПП-127

Перечень показателей критериев значимости объектов КИИ и их значений

Показатель		Значение показателя		
		III категория	II категория	I категория
I. Социальная значимость				
3.	Прекращение <1> или нарушение функционирования <2> объектов транспортной инфраструктуры, оцениваемые:			
	а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг;	в пределах территории одного муниципального образования (численностью от 2 тыс. человек) или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования (численностью от 2 тыс. человек) или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения
	б) по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек)	более или равно 2, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000

Несогласованность законодательства о КИИ с другими видами законодательства

Пример: различные системы обеспечения безопасности, в том числе системы видеонаблюдения Предприятий реализуются в автономных контурах, не имеющих связи с общей локальной сетью, выхода в интернет и т.д.

При этом, законодательство о транспортной безопасности обязывает предоставлять удаленный доступ к системам видеонаблюдения правоохранительным органам.

Архитектурное решение по выделению систем безопасности в автономные локальные сети является пожалуй самой эффективной мерой обеспечения ИБ. Предоставление удаленного доступа резко снижает потенциал этой меры.

Импортозамещение

Импортозамещение ПО

- Отсутствие ИТ-специалистов (администраторов Linux)
- Сопротивление пользователей переходу на новое ПО
- Повышение цен на российское ПО после введения обязательности его использования

Импортозамещение оборудования

- Отсутствие Российских аналогов оборудования
- Недостаточные характеристики и параметры надежности Российских аналогов
- Высокие цены на Российское оборудование при фактическом отсутствии производства микроэлектроники