Проблемные вопросы реализации законодательства Российской Федерации о безопасности критической информационной инфраструктуры

КУБАРЕВ Алексей Валентинович
Заместитель начальника управления ФСТЭК России

Тренд 2020: удалёнка

Социальная инженерия

Незащищенные рабочие станции

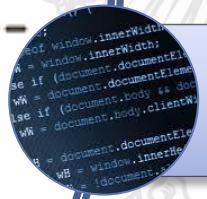
Незащищенные каналы связи

Уязвимые веб-сервисы

Тренд 2020: атаки на науку и здравоохранение

Май. Fresenius, крупнейший в Европе оператор частных больниц. Компьютеры компании были взломаны, и кибератака затронула каждую часть деятельности компании по всему миру

Октябрь. Индийский фармацевтический гигант Dr Reddy's. был вынужден отключить все свои серверы центров обработки данных по всему миру на целый день после того, как подвергся кибератаке



Октябрь. Американский поставщик программного обеспечения для здравоохранения eResearchTechnology. подвергся атакам операторов вымогательского ПО, в результате которых были замедлены некоторые медицинские исследования

Сентябрь. Universal Health Services (UHS), предоставляющая услуги в области здравоохранения, была вынуждена отключить свои компьютерные системы вследствие кибератаки

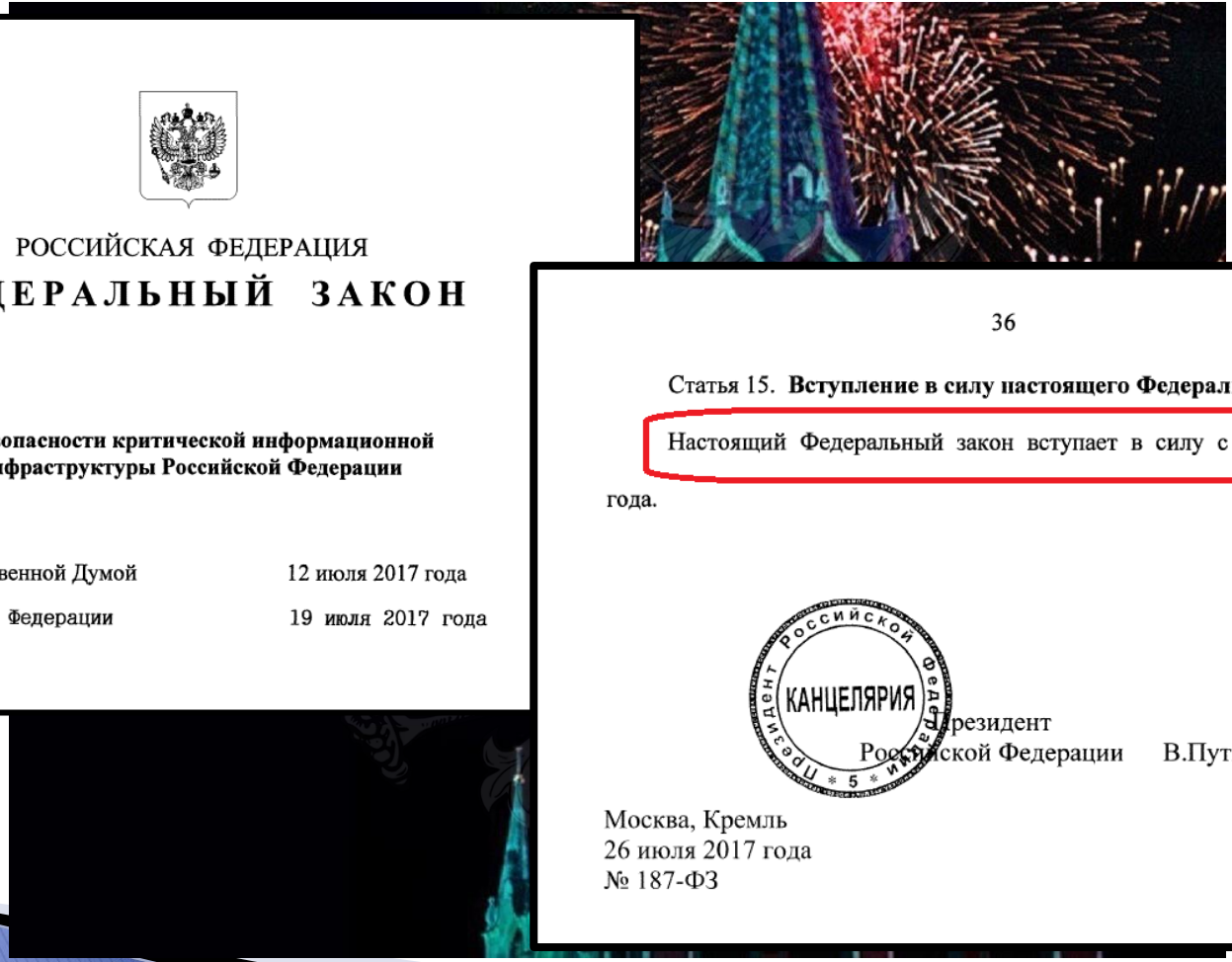
В центре внимания 2020: supply chain-атаки

Посредством разработчика

Посредством поставщика

Посредством провайдера

Посредством подрядчика



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой 12 июля 2017 года

Одобрен Советом Федерации 19 июля 2017 года

Статья 15. **Вступление в силу настоящего Федерального закона**

Настоящий Федеральный закон вступает в силу с 1 января 2018 года.

Президент Российской Федерации КАНЦЕЛЯРИЯ * 5 *

Президент
Российской Федерации В.Путин

Москва, Кремль
26 июля 2017 года
№ 187-ФЗ

ФЕДЕРАЛЬНЫЙ ЗАКОН

от 26 июля 2017 г. № 187-ФЗ

«О безопасности критической информационной инфраструктуры Российской Федерации»

Категорирование объектов КИИ

Создание и обеспечение функционирования систем безопасности значимых объектов КИИ

Принятие мер по обеспечению безопасности значимых объектов КИИ

Осуществление взаимодействия с ГосСОПКА

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРА

ПОСТАНОВЛЕНИЕ

от 13 апреля 2019 г. № 452

МОСКВА

Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые изменения, которые вносятся в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений" (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204).

2. Субъектам критической информационной инфраструктуры - государственным органам и государственным учреждениям утвердить до 1 сентября 2019 г. перечень объектов критической информационной инфраструктуры, подлежащих категорированию.

3. Рекомендовать субъектам критической информационной инфраструктуры - российским юридическим лицам и (или) индивидуальным предпринимателям утвердить до 1 сентября 2019 г. перечень объектов критической информационной инфраструктуры, подлежащих категорированию.

Председатель Правительства Российской Федерации Д.Медведев

Определение ОКИИ

Уклонение от реализации («Мы – не субъект КИИ»)

Уклонение от реализации («У нас нет ОКИИ»)

Нарушение сроков представления перечней

Уведомление не обо всех ОКИИ

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 8 февраля 2018 г. № 127

МОСКВА

Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений

УТВЕРЖДЕНЫ
постановлением Правительства
Российской Федерации
от 8 февраля 2018 г. № 127

П Р А В И Л А
категорирования объектов критической информационной инфраструктуры Российской Федерации

Максимальный срок категорирования не должен превышать одного года со дня утверждения субъектом критической информационной инфраструктуры перечня объектов (внесения изменений в перечень объектов).

Категорирование ОКИИ

- Нарушение сроков категорирования
- Искусственное занижение категорий
- Представление недостоверных сведений
- Учет не всех показателей

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 8 февраля 2018 г. № 127

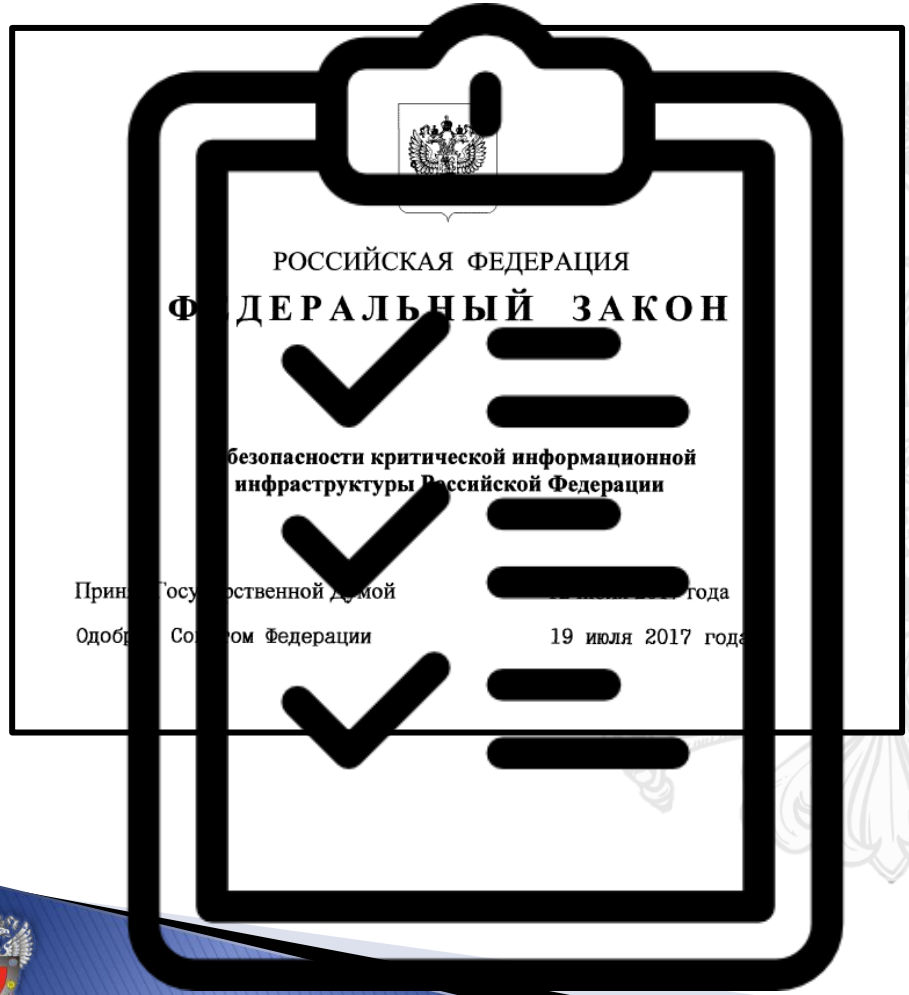
МОСКВА

Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений

УТВЕРЖДЕНЫ
постановлением Правительства
Российской Федерации
от 8 февраля 2018 г. № 127

П Р А В И Л А
категорирования объектов критической информационной инфраструктуры Российской Федерации

По вновь создаваемым объектам критической информационной инфраструктуры сведения, указанные в подпунктах "а" - "в" и "з" пункта 17 настоящих Правил, направляются в течение 10 рабочих дней после утверждения требований к создаваемому объекту критической информационной инфраструктуры, а сведения, указанные в подпунктах "г" - "ж" и "и" пункта 17 настоящих Правил, - в течение 10 рабочих дней после ввода объекта критической информационной инфраструктуры в эксплуатацию (принятия на снабжение).


РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой [illegible] года

Одобрен Советом Федерации 19 июля 2017 года

Статья 9. **Права и обязанности субъектов критической информационной инфраструктуры**

3. Субъекты критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, наряду с выполнением обязанностей, предусмотренных частью 2 настоящей статьи, также обязаны:

1) соблюдать требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

Реализация Требований

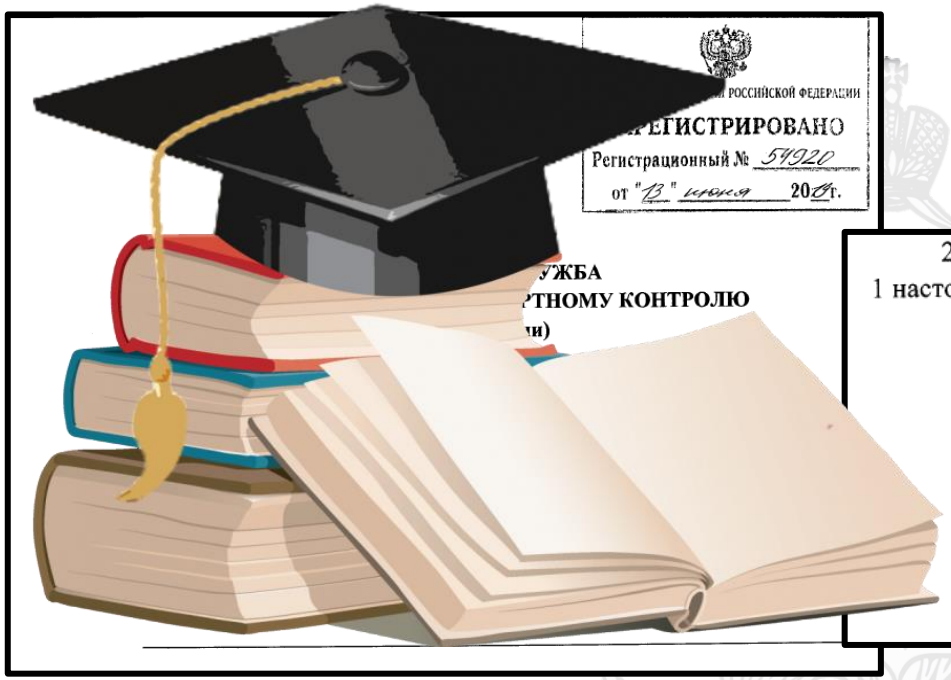
Недооценка потенциала нарушителя

Медлительная реализация

Проблемы с силами безопасности

Проблемы с организацией безопасности

Проблемы со средствами безопасности



РОССИЙСКОЙ ФЕДЕРАЦИИ
ЕГИСТРИРОВАНО
Регистрационный № 54920
от "13" июня 2021 г.

УЖБА
РТНОМУ КОНТРОЛЮ
ии)

2. Установить, что изменения, предусмотренные подпунктом 4 пункта 1 настоящего приказа, вступают в силу с 1 января 2021 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

4) пункт 12 изложить в следующей редакции:

«12. Работники структурного подразделения по безопасности, специалисты по безопасности должны соответствовать следующим требованиям:

наличие у руководителя структурного подразделения по безопасности высшего профессионального образования по направлению подготовки (специальности) в области информационной безопасности или иного высшего профессионального образования и документа, подтверждающего прохождение обучения по программе профессиональной переподготовки по

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 8 июня 2019 г. № 743

МОСКВА

Об утверждении Правил подготовки и использован
ресурсов единой сети электросвязи Российской Федер
для обеспечения функционирования значимых объе
критической информационной инфраструктуры

3. Настоящее постановление вступает в силу с 1 января 2

Допускается использование ресу общего пользования в целях обеспечения функционир ых объектов при отсутствии технической возможност ия ресурсов сетей электросвязи, не присоединенных к се пользования, либо необходимости дополнительного рез налов связи при условии согласования субъектом информационной инфраструктуры подключения значимог ральной службо по техническому и экспортному ко достаточнос применяемых при таком подключении программных средств обеспечения безоп Порядок указанного согласования определя по техническому и экспортному контролю. не требуется для субъекта критической информационно уры, являющегося оператором связи и предоставляющего услуги связи в сети связи общего пользования.

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 59866
от "15" сентября 2020.

ФЕДЕРАЛЬНАЯ СЛУЖБА
СКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«18 »

Москва № 75

О

ядка согласования субъектом критической
инфраструктуры Российской Федерации
й по техническому и экспортному контролю
ого объекта критической информационной

9, № 24, ст. 3099), **П Р И К А З Ы В А Ю**:

ый Порядок согласования субъектом критической
руктуры Российской Федерации с Федеральной
и экспортному контролю подключения значимого
информационной инфраструктуры Российской
бщего пользования.

ЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Времени на раскачку нет

- Проверки органами прокуратуры
- Подключаем профильные ФОИВ
- Подключаем ОГВ субъектов Федерации
- Официальное взаимодействие напрямую

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой 12 июля 2017 года

Одобрен Советом Федерации 19 июля 2017 года

Статья 13. **Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры**

2. Основанием для осуществления плановой проверки является истечение трех лет со дня:

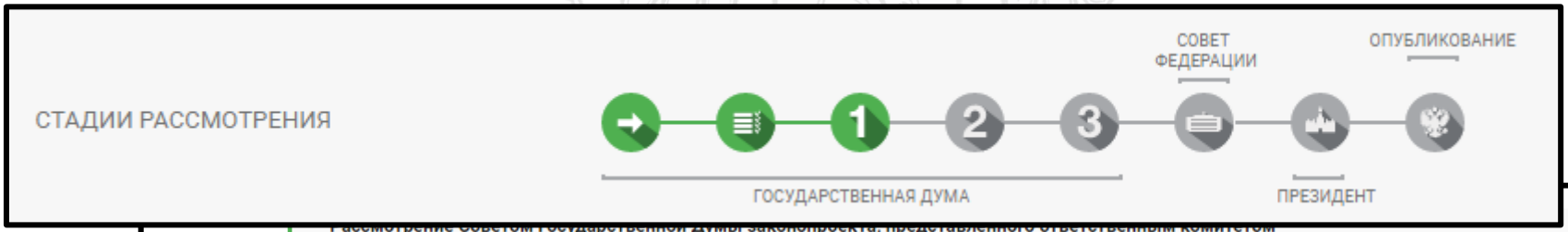
1) внесения сведений об объекте критической информационной инфраструктуры в реестр значимых объектов критической информационной инфраструктуры;

Вносится Правительством
Российской Федерации

N1048574-7 Проект

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации



25.01.2021	внести законопроект на рассмотрение Государственной Думы (27.01.2021)	301, п.27
	Рассмотрение законопроекта Государственной Думой	
27.01.2021	принять законопроект в первом чтении; представить поправки к законопроекту (Срок представления поправок в тридцатидневный срок со дня принятия постановления; 25.02.2021)	9721-7 ГД

Первая заповедь ИБ

Общая защищенность системы равняется защищенности наименее защищенной её части

Условия обеспечения ИБ

Знания

Личная ответственность

Дисциплина

Контроль

Спасибо за внимание!

Вопросы?

Проблемные вопросы реализации законодательства Российской Федерации о безопасности критической информационной инфраструктуры

КУБАРЕВ Алексей Валентинович
Заместитель начальника управления ФСТЭК России