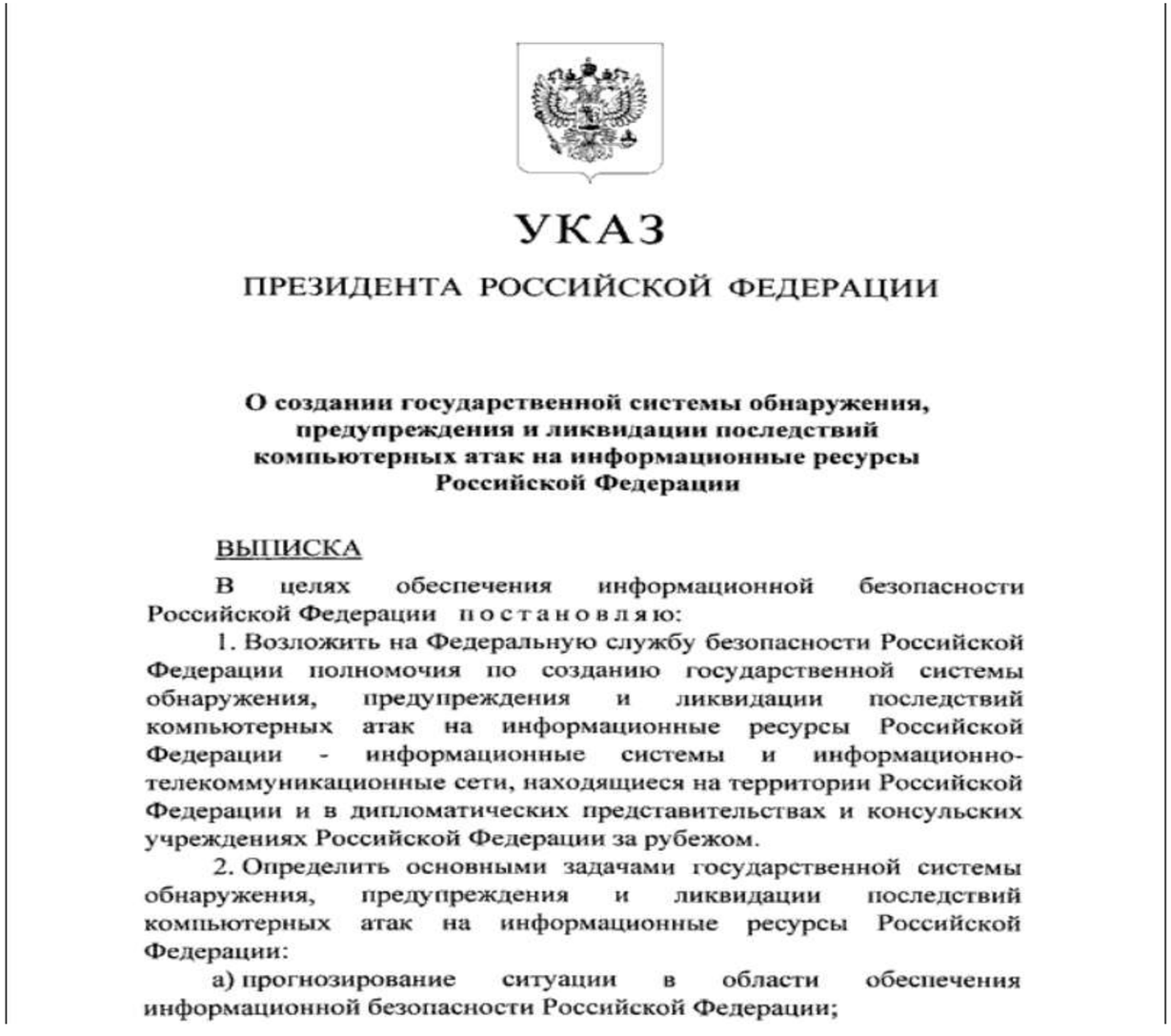
Изменения и дополнения в регулировании деятельности по обеспечению безопасности КИИ Российской Федерации

Законодательство России о безопасности КИИ

- Конституция Российской Федерации.
- Стратегия развития информационного общества в Российской Федерации на 2017-2013 годы.
- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Уголовный кодекс Российской Федерации.
- Подзаконные нормативные правовые акты: Указы Президента Российской Федерации, постановления Правительства Российской Федерации, приказы ФСТЭК России, ФСБ России и Минцифры России.

Указ Президента РФ от 15.01.2013 № 31с



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

ВЫПИСКА

В целях обеспечения информационной безопасности Российской Федерации п о с т а н о в л я ю:

1. Возложить на Федеральную службу безопасности Российской Федерации полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации - информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.

2. Определить основными задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации:

а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

Концепция ГосСОПКА

ВЫПИСКА ИЗ КОНЦЕПЦИИ
государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
(Концепция утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274)

I. Общие положения

1. Настоящей Концепцией определяются назначение, функции и принципы создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее - Система), а также виды обеспечения, необходимые для ее создания и функционирования.

2. Система представляет собой единый централизованный, территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий

ФЗ «О безопасности КИИ РФ»

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 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.

ФЗ «О безопасности КИИ РФ»

Регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Определяет основные принципы обеспечения безопасности, полномочия госорганов, а также права, обязанности и ответственность лиц, владеющих на праве собственности или ином законном основании объектами инфраструктуры, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов.

ФЗ «О безопасности КИИ РФ»

К объектам инфраструктуры отнесены информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Закреплены основные понятия, в т.ч. компьютерной атаки, компьютерного инцидента.

Определен порядок функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы.

ФЗ «О безопасности КИИ РФ»

Предусмотрены категорирование объектов; ведение реестра значимых объектов; оценка состояния защищенности; госконтроль; создание специальных систем безопасности.

Федеральный закон вступил в силу 1 января 2018 г.

Полномочные органы государственной власти в области обеспечения безопасности КИИ

Президент Российской Федерации.

Правительство Российской Федерации.

Федеральная служба по техническому и экспортному контролю Российской Федерации.

Федеральная служба безопасности Российской Федерации.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

Подзаконные нормативные правовые акты

Правила категорирования объектов КИИ РФ.
Перечень показателей критериев значимости объектов КИИ РФ и их значений.

Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ РФ.

Правила подготовки и использования ресурсов единой сети электросвязи РФ для обеспечения функционирования значимых объектов КИИ.

Подзаконные нормативные правовые акты

Порядок ведения реестра значимых объектов КИИ.

Требования к создания систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования.

Требования по обеспечению безопасности значимых объектов КИИ РФ.

Порядок согласования субъектом критической информационной инфраструктуры Российской Федерации с Федеральной службой по техническому и экспортному контролю подключения значимого объекта критической информационной инфраструктуры Российской Федерации к сети связи общего пользования.

Подзаконные нормативные правовые акты

Порядок обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

Порядок получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения.

Подзаконные нормативные правовые акты

Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации.

Подзаконные нормативные правовые акты

Порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ РФ

Ответственность за неправомерное воздействие на КИИ

Установлена уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации в соответствии со статьей 274.1 Уголовного кодекса Российской Федерации.

Изменения в действующем законодательстве и правоприменительной практике

Указ Президента Российской Федерации от 22.12.2017 № 620

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О совершенствовании
государственной системы обнаружения, предупреждения
и ликвидации последствий компьютерных атак
на информационные ресурсы Российской Федерации

В целях совершенствования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и в соответствии со статьей 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" п о с т а н о в л я ю:

1. Возложить на Федеральную службу безопасности Российской Федерации функции федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации - информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской

Изменения в действующем законодательстве и правоприменительной практике

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 17 февраля 2018 г. № 162

МОСКВА

Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

В соответствии с пунктом 2 части 2 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" Правительство Российской Федерации **п о с т а н о в л я е т :**

Утвердить прилагаемые Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

Председатель Правительства Российской Федерации Д.Медведев

Изменения в действующем законодательстве и правоприменительной практике

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК России)

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА

Старая Басманная, д. 17, Москва, 105066
Тел., факс (495) 696-49-04
E-mail: postin@fstec.ru

20.03.2020 № 240/84/389

На №_____

Субъектам критической
информационной инфраструктуры
Российской Федерации

Рекомендации по обеспечению безопасности
объектов критической информационной инфраструктуры
при реализации дистанционного режима исполнения должностных обязанностей
работниками субъектов критической информационной инфраструктуры

Изменения в действующем законодательстве и правоприменительной практике

Уточнение приказа ФСТЭК России от 21.12.2017 № 235 **«Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их безопасности»:**

С 01.01.2021 вступили в силу требования, предъявляемые к руководителям и работникам структурного подразделения по безопасности, в части наличия у них специального высшего образования и необходимости повышения квалификации не реже одного раза в 5 лет.

Проекты нормативных правовых актов

Дополнения Кодекса Российской Федерации об административных правонарушениях

ПРАВИТЕЛЬСТВО
РОССИЙСКОЙ ФЕДЕРАЦИИ

«02» ноября 2020 г.

№ 10188п-П4

МОСКВА

Государственная Дума
Федерального Собрания
Российской Федерации

О внесении на рассмотрение
проекта федерального закона

173350 227209
Государственная Дума ФС РФ
Дата 02.11.2020 19:56
№1048574-7; 1.1

В соответствии со статьей 104 Конституции Российской Федерации Правительство Российской Федерации вносит на рассмотрение Государственной Думы Федерального Собрания Российской Федерации проект

Проекты нормативных правовых актов

Дополнения Кодекса Российской Федерации об административных правонарушениях

2) дополнить статьей 13.12[1] следующего содержания:

"Статья 13.12[1]. **Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации**

1. Нарушение требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, если такие действия (бездействие) не содержат уголовно наказуемого деяния, -

Проекты нормативных правовых актов

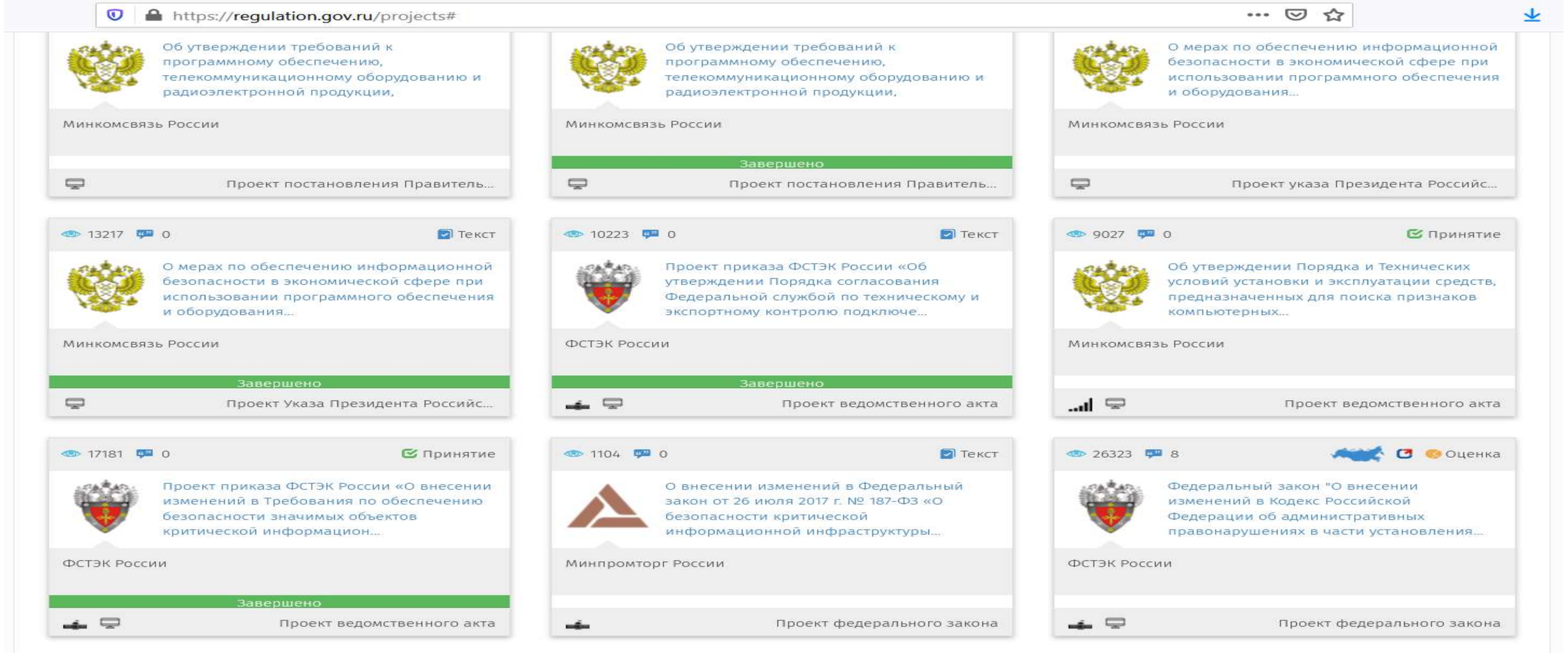
Дополнения Кодекса Российской Федерации об административных правонарушениях

4) дополнить статьей 19.7[15] следующего содержания:

"Статья 19.7[15]. **Непредставление сведений, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации**

1. Непредставление или нарушение сроков представления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, либо об отсутствии необходимости присвоения ему одной из таких категорий -

Проекты нормативных правовых актов



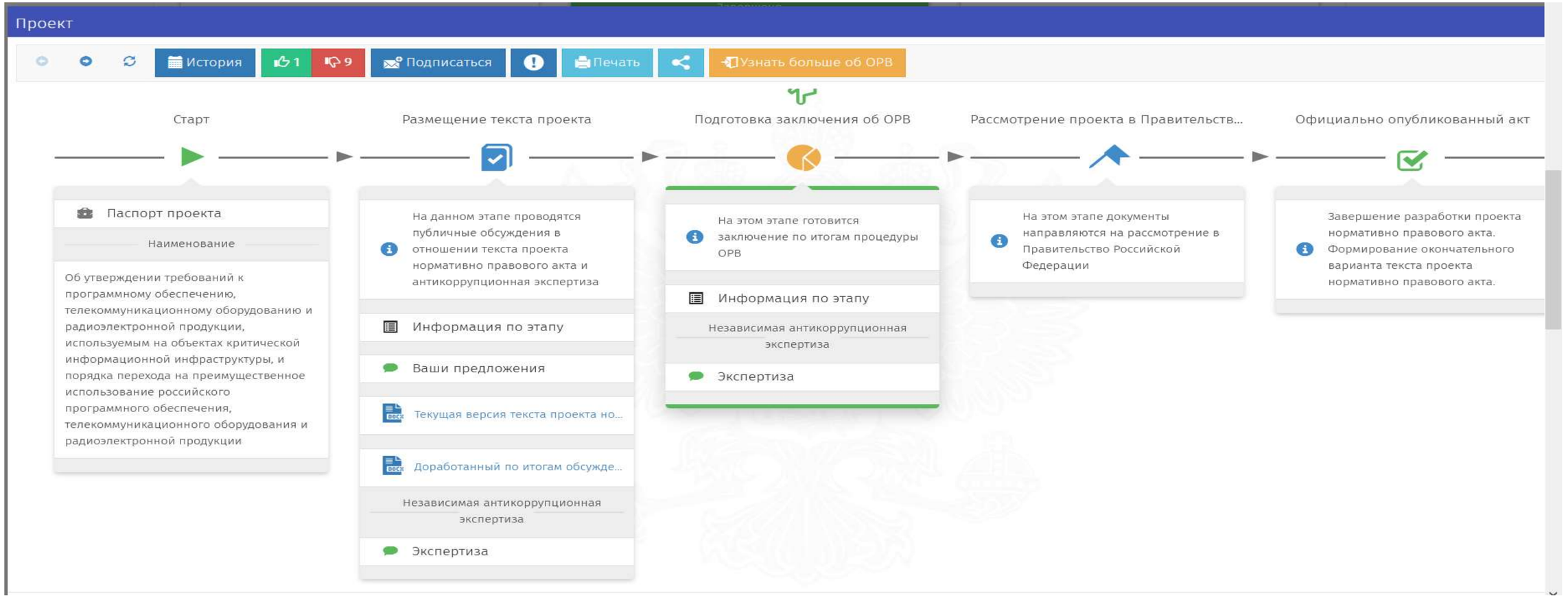
Проекты нормативных правовых актов

Проект Указа Президента Российской Федерации

«О мерах по обеспечению информационной безопасности в экономической сфере при использовании программного обеспечения и оборудования на объектах критической информационной инфраструктуры»

Проекты нормативных правовых актов

Проект постановления Правительства Российской Федерации



Проекты нормативных правовых актов

Проект методического документа ФСТЭК России

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ
о разработке проекта методического документа ФСТЭК России
«Рекомендации по оценке показателей критериев экономической значимости
объектов критической информационной инфраструктуры
Российской Федерации»

от 16 февраля 2021 г. № 240/84/18

В соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, ФСТЭК России разработан проект методического документа «Рекомендации по оценке показателей критериев экономической значимости объектов критической информационной инфраструктуры Российской Федерации».

Документ детализирует порядок оценки показателей критериев экономической значимости объектов критической информационной инфраструктуры Российской Федерации, проводимой в соответствии с Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127.

Проекты нормативных правовых актов

Проект приказа ФСБ России

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ Москва № _____

Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием средств криптографической защиты информации

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и пунктом 1 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960,

Проекты нормативных правовых актов

Проект ГОСТ Р

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

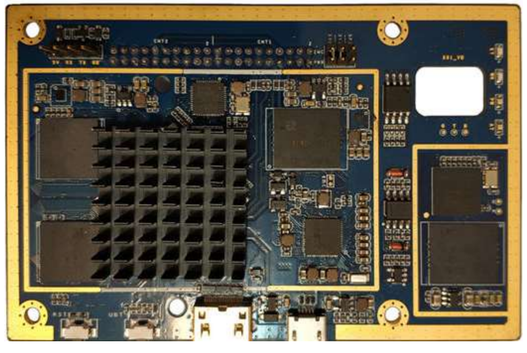
НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р
(проект,
первая редакция)

Защита информации
ОБНАРУЖЕНИЕ, ПРЕДУПРЕЖДЕНИЕ И ЛИКВИДАЦИЯ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК И РЕАГИРОВАНИЕ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ
Термины и определения

Решения ОКБ САПР

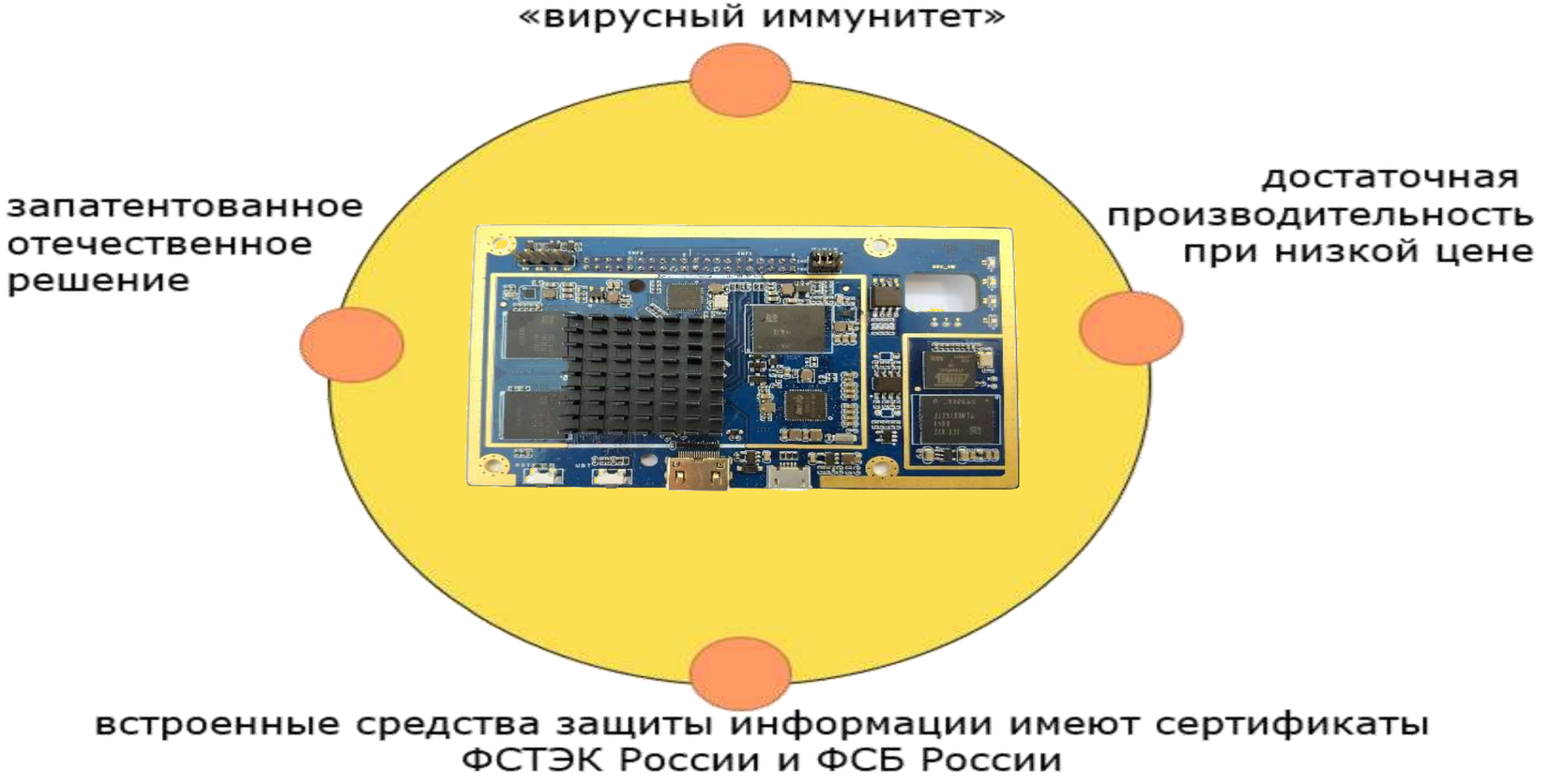
Для обеспечения защищённой сетевой коммуникации между элементами критической информационной инфраструктуры ОКБ САПР предлагает одноплатный компьютер Новой гарвардской архитектуры «m-TrusT». Конструктивно этот компьютер включает в себя док-станцию, которая стационарно включается в состав элемента КИИ, и подключаемого к ней универсального по своему аппаратному исполнению модуля (мезонина).



Док-станция предназначена для того, чтобы корректно подключить m-TrusT к тому или иному конкретному элементу КИИ, поэтому её конструктивное решение и набор портов могут существенно различаться, ведь такими элементами могут быть самые разные объекты – от локомотивов до банкоматов, от газовых счетчиков до терминалов управления АЭС.

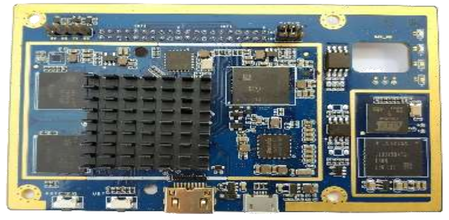
Защищенные микрокомпьютеры Новой гарвардской архитектуры: m-TrusT

m-TrusT – это промышленное решение, предназначенное для применения на объектах критических информационных инфраструктур.



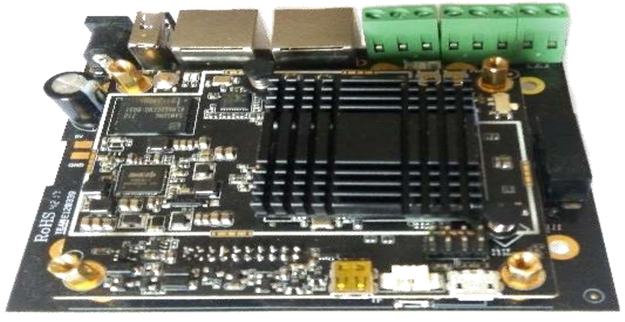
m-TrusT: универсальная платформа

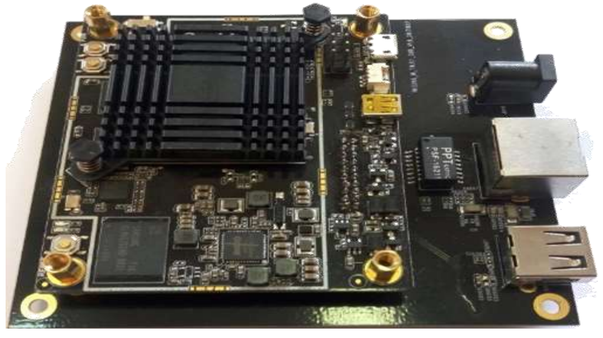
Особенность аппаратного решения в том, что оно состоит из универсального ядра и интерфейсной платы, которая, без изменения ядра, изменяется под особенности оборудования на конкретном объекте КИИ.

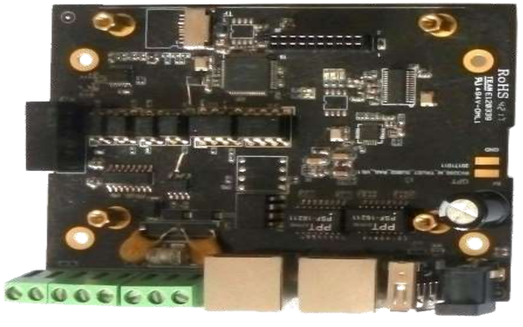


Мезонин m-TrusT (слева)

M-TrusT на интерфейсных платах (справа)







Интерфейсные платы

m-TrusT сервер

Для центральных узлов объекта выпускается исполнение в стойку. Таким образом исключаются проблемы интеграции – это одно и то же устройство в разных форм-факторах.

Программа повышения квалификации

ОКБ САПР совместно с МФТИ предлагает пройти повышение квалификации по специальной программе, предназначенной для специалистов, работающих в области обеспечения безопасности значимых объектов КИИ.

Программа согласована с ФСТЭК России.

Объём курса – 216 академических часов.

Формат обучения – очно-заочный с применением дистанционных технологий.

Национальный исследовательский университет
«Московский физико-технический институт (государственный университет)»
(МФТИ)

СОГЛАСОВАНО
Руководитель 1 Управления
ФСТЭК России
(Н.М. Мартинец)
«__» _____ 2019 г.
М.П.

УТВЕРЖДАЮ
Ректор МФТИ
д-р физ.-мат. наук,
профессор,член-корреспондент
РАН
(Н.Н. Кудрявцев)
«__» _____ 2019 г.
М.П.

СОГЛАСОВАНО
Генеральный директор
ЗАО «ОКБ САПР»
(И.Г. Назаров)
«16» сентября 2019 г.
М.П.

ПРОГРАММА ПОВЫШЕНИЯ
КВАЛИФИКАЦИИ
специалистов, работающих в области обеспечения безопасности значимых
объектов критической информационной инфраструктуры

Программа повышения квалификации

Программа повышения квалификации состоит из 4-х модулей:

1. Основы обеспечения безопасности значимых объектов КИИ.
2. Организация работ по обеспечению безопасности значимого объекта КИИ.
3. Контроль за обеспечением безопасности значимого объекта.
4. Организация защищенной сетевой коммуникации между элементами КИИ с применением микрокомпьютеров «m-TrusT».

Программа повышения квалификации

Программа повышения квалификации носит практико-ориентированный характер: 94 академических часа отведены под лабораторные работы, практические и семинарские занятия.

Программа повышения квалификации

Итоговый документ – **удостоверение МФТИ о повышении квалификации** установленного образца.


МФТИ

Настоящее удостоверение свидетельствует о том, что

прошел(а) повышение квалификации в (на)

УДОСТОВЕРЕНИЕ

О ПОВЫШЕНИИ КВАЛИФИКАЦИИ

772409757594

по дополнительной профессиональной программе

Документ о квалификации

Регистрационный номер

в объёме

Город

Дата выдачи

М.П. *Руководитель*

Секретарь

ОБРАЗЕЦ

КОНТАКТЫ

Учебный центр ОКБ САПР совместно с МФТИ

Каннер Татьяна Михайловна

Телефон	+7-926-235-14-67
Сайт	https://www.okbsapr.ru/education/education-centre
E-mail	tatianash@okbsapr.ru

Центр дополнительного профессионального образования МФТИ

Вещезерова Улганым Бижановна

Телефон	+7-916-819-08-29
Сайт	https://mipt.ru/cdpo
E-mail	cdpo@phystech.edu

Спасибо за внимание!