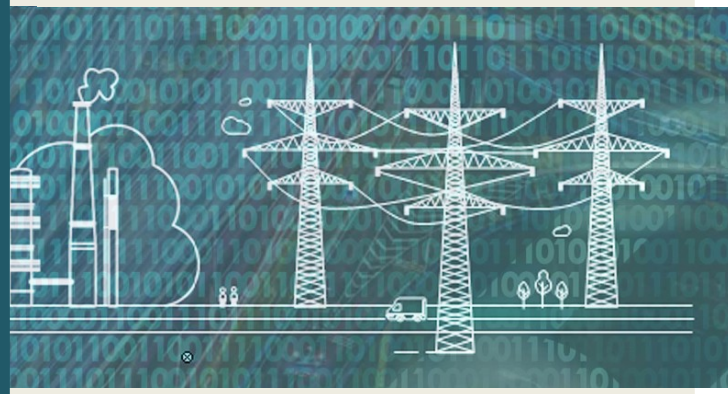
# О критической информационной инфраструктуре



Обзор нормативной базы

ПОЛИКОМ ПРО

# Указы Президента Российской Федерации

**№ 31с от 15.01.2013**

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

**№ 569 от 25.11.2017**

«О внесении изменений в Положение о ФСТЭК России, утвержденное Указом Президента Российской Федерации от 16.08.2004 г. N 1085»

**№ 620 от 22.12.2017**

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

**№ 98 от 02.03.2018**

«О внесении изменения в перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203»

«О внесении изменений в Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (проект)


# Федеральные законы

**№ 187-ФЗ**
**от 26.07.2017**

«О безопасности критической информационной инфраструктуры Российской Федерации»

**№ 193-ФЗ**
**от 26.07.2017**

«О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Закона «О безопасности КИИ»

**№ 194-ФЗ**
**от 26.07.2017**

«О внесении изменений в УК и УПК Российской Федерации в связи с принятием Закона «О безопасности КИИ»

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

# Постановления Правительства Российской Федерации

**№ 127**
**от 08.02.2018**

«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»

**№ 162**
**от 17.02.2018**

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

# Регуляторы и участники

| | |
|---|---|
| **ФОИВ ГосСОПКА** | Уполномоченные подразделения ФСБ России (включая Национальный координационный центр по компьютерным инцидентам – НКЦКИ: http://gov-cert.ru), статус закреплён Указом Президента Российской Федерации № 620 от 22.12.2017 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» |
| **ФОИВ КИИ** | ФСТЭК России, статус закреплён Указом Президента Российской Федерации № 569 от 25.11.2017 г. «О внесении изменений в Положение о ФСТЭК России» |
| **Субъекты КИИ** | Обладатели на праве собственности, аренды или на ином законном основании объектов КИИ |
| **Силы ОПЛ КА** | Уполномоченные подразделения ФСБ России (включая НКЦКИ), соответствующие подразделения и должностные лица субъектов КИИ |


# Основные понятия (187-ФЗ)

Объекты КИИ – информационные системы (ИС), информационно-телекоммуникационные сети (ИТС), автоматизированные системы управления (АСУ) субъектов КИИ

Значимый объект КИИ – объект КИИ, прошедший категорирование, по результатам которой ему была присвоена первая, вторая или третья категория

Критическая информационная инфраструктура Российской Федерации (КИИ) – совокупность объектов КИИ

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА)– единый территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (далее – силы ОПЛ КА и средства ОПЛ КА)

Средства ОПЛ КА – программно-технические средства для обнаружения, предупреждения, ликвидации последствий компьютерных атак


# Что такое ГосСОПКА?

Совокупность технической составляющей, обслуживающего персонала и регламентов, предназначенная для обеспечения и контроля состояния информационной безопасности в Российской Федерации и диппредставительствах страны за рубежом

Техническая составляющая (средства ОПЛ КА) будет состоять из центров ГосСОПКА, объединённых в иерархическую структуру по ведомственно-территориальному признаку, и подключённых к ним технических средств, установленных в конкретных объектах КИИ

Государство – регулятор и координатор (***не собственник***)

Единого собственника не будет, каждый из элементов системы ГосСОПКА будет принадлежать тому, кто за него заплатил

# Функции ФОИВ

## ФСБ России

«точка входа» – НКЦКИ, http://gov-cert.ru

- нормативно-правовое регулирование в области обеспечения безопасности КИИ
- разработка требований к средствам ОПЛ КА
- регулирование и координация деятельности субъектов КИИ в части сил и средств ОПЛ КА
- сбор информации о компьютерных инцидентах
- оценка безопасности КИИ

## ФСТЭК России

«точка входа» otd25@fstek.ru

- нормативно-правовое регулирование в области обеспечения безопасности КИИ
- категорирование объектов КИИ (включая ведение реестра значимых объектов КИИ)
- разработка требований по обеспечению информационной безопасности объектов КИИ и государственный контроль в данной области

## Кто?

- государственные органы
- государственные учреждения
- юридические лица
- индивидуальные предприниматели

## Где? (область обязательного применения):

- здравоохранение
- наука
- транспорт
- связь
- энергетика
- банковская и кредитно-финансовая сфера
- топливно-энергетический комплекс
- область атомной энергии
- оборонная, ракетно-космическая промышленность
- горнодобывающая, металлургическая и химическая промышленность

# Права и обязанности субъектов КИИ

## Права

Получать от ФСБ и ФСТЭК России информацию по линии ответственности

За свой счет приобретать, арендовать, устанавливать и обслуживать средства ОПЛ КА

Обеспечивать безопасность значимых объектов КИИ в зоне своей ответственности

**Все организации, работающие в областях, перечисленных в определении субъекта КИИ, потенциально являются такими субъектами и должны провести инвентаризацию своей информационной инфраструктуры и последующее категорирование объектов КИИ**

## Обязанности

Категорировать объекты КИИ

Выполнять требования по обеспечению безопасности объектов КИИ (ФСТЭК России)

Устанавливать и эксплуатировать средства ОПЛ КА (центры ГосСОПКА и конкретные технические средства – ФСБ России)

Реагировать на компьютерные инциденты, информировать о них и принимать меры по ликвидации последствий (ФСБ России)

Содействовать должностным лицам ФСБ и ФСТЭК России при исполнении ими своих служебных обязанностей

# Ответственность

**Закон (187-ФЗ)**: нарушение положений Закона и принятых в соответствии с ним иных нормативных правовых актов повлечет за собой ответственность в соответствии с действующим законодательством. При наступлении последствий, влекущих административную и/или уголовную ответственность, несоблюдение положений Закона будет отягчающим обстоятельством (наиболее ожидаемо – по составу "Халатность")

## Уголовная (персональная) ответственность 193-ФЗ

В УК РФ была добавлена новая статья 274.1, которая устанавливает уголовную ответственность должностных лиц субъекта КИИ за несоблюдение установленных правил эксплуатации технических средств объекта КИИ или нарушение порядка доступа к ним вплоть до лишения свободы сроком на 10 лет (при совершении преступления группой лиц и наступлении тяжких последствий)

Последственность статьи 274.1 – ФСБ России (статья 151 УПК РФ)

## Ответственность организаций (КОАП)

Статья 13.12:
нарушение правил защиты информации

Дополнения в КОАП
(готовит ФСТЭК России)

# Порядок применения закона субъекта КИИ

Проводится инвентаризация информационной инфраструктуры, выявление потенциальных значимых объектов КИИ и их категорирование, срок – не более года с момента завершения инвентаризации. Результаты инвентаризации направляются во ФСТЭК России

**В случае присвоения объекту КИИ какой-либо категории**:

- данный факт фиксируется ФСТЭК России и сообщается субъектом КИИ в ФСБ России
- субъект КИИ проводит работы по ОИБ категорированных КИИ в зоне своей ответственности, создаёт центр ГосСОПКА и информирует регуляторов о готовности к аттестации системы ОИБ и центра ГосСОПКА
- регуляторы осуществляют оценку результатов деятельности субъекта КИИ в соответствии со своими полномочиями, при отсутствии замечаний осуществляется формальное подключение объектов КИИ к ГосСОПКА и начинается эксплуатация соответствующего центра/сегмента ГосСОПКА, в противном случае субъект исправляет замечания и повторно обращается к регуляторам

В случае не присвоения категории материалы также направляются во ФСТЭК России на согласование

# Категорирование объектов КИИ

Категорированию подлежат объекты КИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ

Объекту КИИ по результатам категорирования присваивается категория значимости с наивысшим значением

Устанавливаются 3 категории значимости. Самая высокая категория – первая, самая низкая – третья

**Для проведения категорирования решением руководителя субъекта КИИ создается комиссия по категорированию, в которую кроме уполномоченных сотрудников соответствующего субъекта КИИ могут быть приглашены специалисты отраслевого регулятора (по согласованию)**

## Исходные данные:

Сведения об объекте КИИ (назначение, архитектура, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами КИИ, наличие и характеристики доступа к сетям связи)

Выполняемые процессы (управленческие, технологические, производственные, финансово-экономические, иные) и состав обрабатываемой информации

Декларация промышленной безопасности опасного производственного объекта, безопасности гидротехнического сооружения, паспорт объекта топливно-энергетического комплекса в случае, если на них функционирует объект КИИ

Сведения о взаимодействии и/или зависимости от других объектов КИИ

Угрозы безопасности информации в отношении объекта КИИ, данные о компьютерных инцидентах, произошедших ранее на объектах КИИ соответствующего типа

# Показатели критериев значимости объектов КИИ

## Социальная значимость

Причинение ущерба жизни и здоровью людей (3-я категория – до 50 чел.; 2-я – 50-500 чел., 1-я – более 500 чел.)

Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения (в том числе водоснабжения и канализации), транспортной инфраструктуры, сети связи

Отсутствие доступа к государственной услуге (3-я категория – 24-12 часов; 2-я – 12-6 часов, 1-я – менее 6 часов)

## Политическая значимость

Прекращение или нарушение функционирования государственного органа

Нарушение условий международного договора Российской Федерации

## Экологическая значимость

Вредные воздействия на окружающую среду

## Экономическая значимость

Возникновение ущерба субъекту КИИ (снижение уровня дохода на 5-10, 10-15 и более 15% для 3-й, 2-й и 1-й категории соответственно)

Возникновение ущерба бюджетам Российской Федерации

Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом КИИ

## Значимость для обеспечения обороны страны, безопасности государства и правопорядка

Прекращение или нарушение функционирования пункта управления/ситуационного центра, информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, снижение показателей государственного оборонного заказа

# Приказ № 239 ФСТЭК России
## (по обеспечению безопасности значимых объектов КИИ)

### Организационные и технические меры защиты

- идентификация и аутентификация
- управление доступом
- ограничение программной среды
- защита машинных носителей информации
- аудит безопасности
- антивирусная защита
- предотвращение вторжений (компьютерных атак)
- обеспечение целостности
- обеспечение доступности
- защита технических средств и систем
- защита информационной (автоматизированной) системы и ее компонентов
- планирование мероприятий по обеспечению безопасности
- управление конфигурацией
- управление обновлениями программного обеспечения;
- реагирование на инциденты ИБ
- обеспечение действий в нештатных ситуациях
- информирование и обучение персонала

### Средства защиты информации (СрЗИ)

СрЗИ от несанкционированного доступа

Межсетевые экраны

Средства обнаружения (предотвращения) вторжений (компьютерных атак)

Средства антивирусной защиты

Средства (системы) контроля (анализа) защищенности

Средства управления событиями безопасности

Средства защиты каналов передачи данных

# Приказ № 239 ФСТЭК России
## (по обеспечению безопасности значимых объектов КИИ)

**Системы безопасности должны быть созданы для всех значимых объектов КИИ, состоять из Сил (Кадры решают всё!!!) и технических Средств (см. Приказ № 239) и должны:**

Предотвращать неправомерный доступ к информации и иные неправомерные действия с ней

Не допускать воздействия, способные привести к сбоям и нарушениям, позволять восстановление функционирования

Непрерывно взаимодействовать с системой ГосСОПКА

**Организационно-распорядительные документы (утверждаются субъектом КИИ) должны содержать:**

— цели и задачи

— модель угроз и нарушителей

— организационно-технические мероприятия

— состав, структуру и функции Системы безопасности

— порядок применения, формы оценки соответствия значимых объектов КИИ и средств защиты требованиям по безопасности, планы мероприятий по обеспечению безопасности значимых объектов КИИ

— деятельность Сил

— порядок взаимодействия с системой ГосСОПКА

**NB!** Допускается привлечение организаций-лицензиатов в области защиты информации.

**Процессы:**

Ежегодное и перспективное планирование

Разработка, реализация и совершенствование мероприятий по защите

Повышение квалификации Сил (не реже раза в год)

Отчётность (периодическая) и контроль (не реже раза в год)

# НКЦКИ (Приказ ФСБ России № 366 от 24.07.2018)

## Задача

Координация деятельности субъектов КИИ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (далее – ОПЛпКА и РнКИ)

## Функции

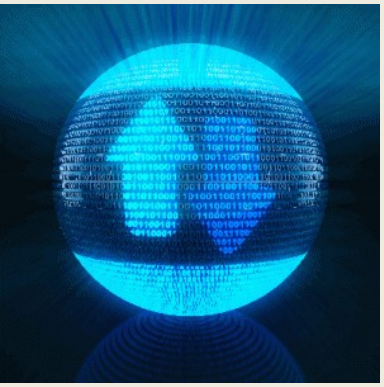
- Координация мероприятий по реагированию на компьютерные инциденты и участие в них
- Организация и осуществление обмена информацией о компьютерных инцидентах между субъектами КИИ и с зарубежными партнёрами
- Методическое обеспечение деятельности субъектов КИИ по вопросам ОПЛпКА и РнКИ и участие в соответствующих мероприятиях
- Обеспечение своевременного доведения до субъектов КИИ информации о средствах и способах проведения КА, методах их обнаружения и предупреждения, а также другой значимой информации по защите КИИ
- Сбор, хранение и анализ информации о КИ и КА, анализ эффективности мероприятий по ОПЛпКА и РнКИ

## Права

- Направлять запросов субъектам КИИ и зарубежным партнёрам по вопросам ОПЛпКА и РнКИ
- Создавать рабочие группы из представителей субъектов КИИ, привлекать сторонних экспертов
- Публиковать материалы по вопросам ОПЛпКА и РнКИ, участвовать в научно-практических мероприятиях, в т.ч. Международных
- Заключать соглашения о сотрудничестве в области ОПЛпКА и РнКИ

# Порядок обмена информацией о компьютерных инцидентах

## (Приказ ФСБ России № 368 от 24.07.2018, приложение 1)



- НКЦКИ информируется в ***обязательном порядке*** **http://gov-cert.ru**
- Субъект КИИ ***сам*** определяет, кому ещё, кроме НКЦКИ, предоставлять информацию о компьютерных инцидентах
- Формат предоставления такой информации должен соответствовать формату НКЦКИ
- При подключении к НКЦКИ обмен должен осуществляться с использованием инфраструктуры НКЦКИ
- При наличии секретных сведений обмен должен соответствовать требованиям действующего законодательства в области защиты гостайны
- Обмен информацией с зарубежными партнёрами ***осуществляет*** НКЦКИ (за исключением действующих международных договоров, когда соответствующее сообщение дублируется в НКЦКИ)

# Требования ФСБ России к средствам ГосСОПКА

**Это – технические, программные, программно-аппаратные и иные средства:**


- обнаружения компьютерных атак
- предупреждения компьютерных атак
- ликвидации последствий компьютерных атак
- поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ
- обмена информацией, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак
- криптографической защиты информации субъектов КИИ

# Персонал субъекта КИИ

## ИБ-подразделение

### Задачи:

- Мониторинг и выявление инцидентов
- Реагирование и расследование
- ИБ (предоставление рекомендаций, закрытие инцидентов и т.д.)
- Анализ вредоносного ПО и обратная разработка

### Решение:

**Программы обучения**

- Цифровая криминалистика
- Реагирование на инциденты
- Выявление вредоносного ПО (YARA и т.д.) (начальный и экспертный уровни)

**Сервисы**

- Аутсорсинг услуг ИБ
- Информирование (аналитические отчеты об угрозах, дайджесты и т.д.)
- Реагирование на инциденты

## ИТ-подразделение

### Задачи

- Идентификация инцидента
- Сбор первичных данных для последующего анализа

### Решение

- Курсы и тренинги по ИБ для IT-специалистов
- Курсы по продуктам

## Пользователи

### Задача

- осведомлённость об угрозах ИБ

### Решение

- курсы/тренинги

# Благодарю за внимание!

Крупеников Александр
руководитель направления
информационной безопасности

тел: + 7 (812) 325 84 00
e-mail: akrupenikov@polikom.ru

ПОЛИКОМ ПРО