OVODOV
CyberSecurity

О безопасности критической информационной инфраструктуры

Нормативные документы

1	Федеральный закон от 26.07.2017 №187	« О безопасности критической информационной инфраструктуры РФ»
2	Приказ ФСТЭК России от 06.12.2017 №236	« Об утверждении формы направления сведений о результатах присвоений объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»
3	Приказ ФСТЭК России от 25.12.2017 №239	«Об утверждении требований по обеспечению значимых объектов КИИ РФ»
4	Постановление правительства РФ от 08.02.2018 №127	«Об утверждении правил категорирования объектов критической информационной инфраструктуры РФ, а так же перечня показателей критериев значимости объектов КИИ РФ и их значений
5	Приказ ФСТЭК от 25.12.2017 №235	«Об утверждении требований к созданию системы безопасности значимых объектов КИИ РФ и обеспечению их функционирования»

Основным документом, определяющим, что такое критическая информационная инфраструктура (КИИ) Российской Федерации, является ФЗ-187, который начал действовать с первого января 2018 года. Документ устанавливает:

1. обозначения ключевых понятий;
2. совокупность нормативно-правовой документации, регулирующей деятельность субъектов КИИ;
3. создание системы Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и Национального координационного центра по компьютерным инцидентам (НКЦКИ);
4. перечень прав и обязанностей организаций, подпадающих под действие закона;
5. дифференциацию категорий объектов критической инфраструктуры, а также формирование их реестра;
6. правила проведения проверки уровня защищенности;
7. органы, отвечающие за государственный контроль, и процедуру его проведения.

Субъекты КИИ

- Гос. органы
- Гос. учреждения
- Юридические лица
- Индивидуальные предприниматели

Которым принадлежат

Которые обеспечивают взаимодействие

Объекты КИИ

- Информационные системы
- Информационно-телекоммуникационные сети
- Автоматизированные Системы Управления

Работающие в отраслях

ПРОМЫШЛЕННОСТЬ

- Горно-добывающая
- Металлургическая
- Химическая
- Оборонная
- Ракетно-космическая

- Энергетика
- Атомная энергетика
- ТЭК
- Связь
- Транспорт
- Здравоохранение
- Банки
- Финансовая сфера
- Наука

15 сфер критических информационных инфраструктур

Энергетика

Ракетно-космическая промышленность

Горнодобывающая промышленность

Металлургическая и химическая промышленность

Наука, транспорт, связь

ЮЛ и ИП, которые обеспечивают взаимодействие с системами КИИ

Сфера государственной регистрации прав на недвижимое имущество и сделок с ним

Военно-промышленный комплекс

Атомная промышленность

Топливно-энергетический комплекс

Банковская сфера и иные сферы финансового рынка

Здравоохранение

3 этапа выполнения ФЗ №187 от 26.07.2017

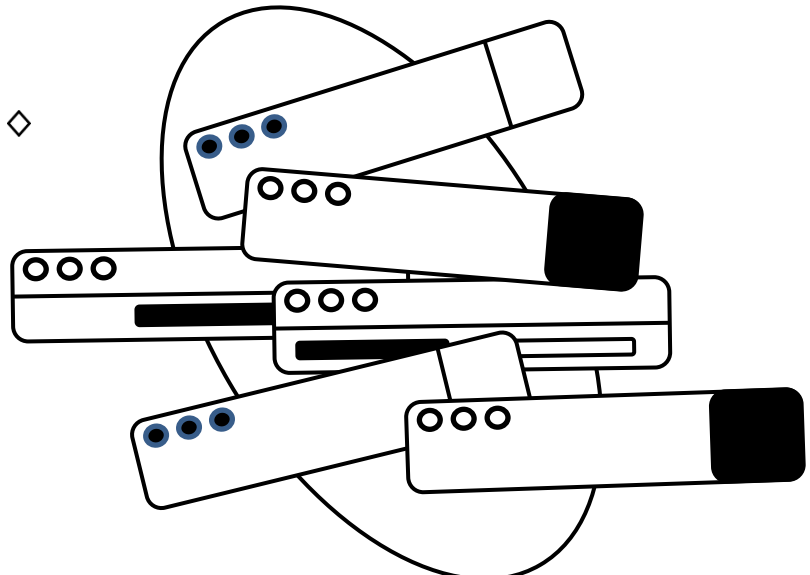
1. Категорирование объектов КИИ
2. Обеспечение безопасности значимых объектов КИИ
3. Подключение значимых объектов КИИ к государственной системе обнаружения и ликвидации последствий компьютерных атак

Этапы категорирования

1. Формирование комиссии
2. Определение процессов
3. Определение критических процессов
4. Определение объектов КИИ

подготовка перечня

5. Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования
6. Отправка перечня и форм сведений во ФСТЭК



Обязанности субъекта КИИ

1 Провести категорирование объектов КИИ

в соответствии с требованиями 187-ФЗ от 26.07.2017 и Постановления Правительства РФ от 08.02.2018 №127

2 Информировать о компьютерных инцидентах

незамедлительно информировать о компьютерных инцидентах ГосСОПКА

3 Определить ответственные лица

которые принимают участие в обнаружении, предупреждении и ликвидации компьютерных атак и в реагировании на компьютерные инциденты

4 Обеспечивать выполнение порядка

технических условий, установки и эксплуатации таких средств, и их сохранность, в случае установки на объектах КИИ средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

5 Оказывать содействие должностным лицам ФСБ РФ

в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов

Ответственность за несоблюдение 187-ФЗ о безопасности КИИ

26 мая 2021 года были опубликованы поправки в КоАП РФ касательно выполнения требований ФЗ-187 о безопасности КИИ. Согласно обновленной редакции КоАП, штрафы грозят юридическим и должностным лицам в следующих ситуациях:

1. при нарушении установленных законодательством требований по созданию, обслуживанию или обеспечению безопасности значимых объектов КИИ (ЗОКИИ);
2. в случае выявления факта нарушений процесса информирования о компьютерных атаках в отношении ЗОКИИ, реагирования и/или принятия мер по устранению последствий;
3. при несоблюдении порядка обмена данными об инцидентах;
4. при непредоставлении сведений или нарушении установленных законом сроков о передаче данных касательно присвоенной категории значимости объекту КИИ;
5. при несвоевременной передаче сведений в ГосСОПКА или нарушении установленного порядка.

Административная ответственность

- законом предусмотрены штрафы для **должностных лиц от 10 до 50 тысяч рублей** по всем нарушениям, кроме нарушения порядка обмена информацией (в этом случае минимальная сумма повышена **до 25 тысяч рублей**);

для юридических лиц:

- **от 50 до 100 тысяч рублей** при выявлении ошибок по организации и обеспечению безопасности, нарушений по срокам предоставления информации об утвержденной категории КИИ;

- **от 100 до 500 тысяч рублей** при несоблюдении установленного порядка работы с компьютерными инцидентами, в том числе по обмену информацией, срокам и порядку передачи данных в ГосСОПКА.

Уголовная ответственность

- при нарушении правил использования, передачи или хранения сведений, повлекшем вред КИИ, наказание может ограничиться принудительными работами на срок до 5 лет или лишением свободы **на срок до 6 лет**;

- при разработке, распространении и применении вредоносных, в том числе вирусных программ, а также получении неправомерного доступа к сведениям или правонарушении, описанном в предыдущем пункте, группой лиц по предварительному сговору или лицом, использующим служебное положение, предусмотрено наказание в виде лишения свободы сроком **от 3 до 8 лет**;

- если описанные в предыдущих пунктах деяния повлекли тяжкие последствия, то обвиняемым грозит лишение свободы на срок **от 5 до 10 лет**.

Во всех этих пунктах также добавлено право судьи лишить обвиняемого или группу лиц права занимать конкретные должности или работать в конкретной сфере.

Уголовная ответственность может наступить как в результате намеренных действий, так и в результате бездействия (например, при необновлении вирусных баз или пароля для доступа к данным КИИ). Что касается категоризации тяжести причиненного вреда, под крупным ущербом понимается ущерб в **размере 1 млн рублей**, под тяжкими последствиями могут подразумеваться гибель людей, разрушения зданий и инфраструктуры, нанесение вреда безопасности РФ и прочее.

Постановление Правительства № 127 (ред. от 09.09.2024г, действ. с 16.09.2024г)

- Убрали перечень объектов КИИ

  Теперь при появлении объекта требуется сразу его категорировать и направлять во ФСТЭК

Указ Президента РФ № 250 (от 13.06.2024г)

Установить, что с 1 января 2025 г. органам (организациям) запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации,
находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними, *а также пользоваться сервисами*

(работами, услугами) по обеспечению информационной безопасности, предоставляемыми (выполняемыми, оказываемыми) этими организациями.

Постановление Правительства № 1912

С 1 сентября 2024 года запрещается покупать и эксплуатировать для значимых объектов КИИ не доверенные ПАК.

Доверенный ПАК:

- Реестр Минпромторга;
- Реестр отечественного ПО;
- Если выполняет функции СрЗИ – сертифицированный ФСТЭК.

Полный переход на использование доверенных ПАК на ЗОКИИ должен быть осуществлен до 1 января 2030 года.

Можно купить не доверенный ПАК при наличии заключения об отнесении продукции к промышленной продукции, не имеющей произведенных в Российской Федерации аналогов, выданные Министерством промышленности и торговли Российской Федерации.

Почему 75% клиентов работает с нами более 5 лет?

Потому что Вы получаете самый лучший клиентский сервис по информационной безопасности

1. **Скорость коммуникации** - персональный менеджер, быстро отвечаем на запросы и всегда с вами на связи;
2. **Уведомления об этапах выполнения работ** - вы понимаете процесс оказания услуги и результат, который получите, ваше спокойствие и уверенность в том, что все идет по плану;
3. **Собственная многоканальная тех. поддержка** - после оказания услуги вы получаете сопровождение на 1 год;
4. **Активное/Крутое ИБ сообщество** - для вас бесплатные вебинары, бизнес-завтраки и оффлайн мероприятия, 1000+ участников в телеграмме-канале для обмена опытом и знаниями;
5. **Индивидуальный подход** - предлагаем несколько вариантов решений и выбираем вместе лучшее для вас;
6. **Инструктажи при выполнении работ,** которые повышают осведомленность и компетентность руководства и всех участников процессов ИБ.

Что вы получаете, работая с нами?

- **Полный пакет документов «под ключ» для отправки во ФСТЭК**
- **Гарантию согласования сведений о результатах категорирования с ФСТЭК РФ на объекты КИИ;**
- **Подготовку проектов ответов на запросы контролирующих органов;**
- **Сопровождение при проверках ФСТЭК, ФСБ и прокуратуры;**
- **Финишную презентацию при сдаче наших работ – Вы будете понимать какие работы были проведены, какой результат получен и рекомендации по дальнейшим шагам.**

Что такое «Быстро» для нас?

- **К нам обратился клиент с проблемой о необходимости срочно прокатегорироваться;**
- **Через полчаса у нас с ним ВКС со всеми ключевыми специалистами;**
- **На следующий день наш специалист проводит выездное обследование на территории заказчика;**
- **Через неделю готов полный пакет документов для отправки;**
- **Заказчик избегает административной ответственности.**

Спасибо за внимание!

OVODOV
CyberSecurity