ФЗ о безопасности КИИ

Цель закона (ст.1)
Настоящий ФЗ регулирует отношения в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак

Основные понятия (ст.2)
- Автоматизированная система управления
- Безопасность КИИ
- Значимый объект КИИ
- Компьютерная атака
- Компьютерный инцидент
- Критическая информационная инфраструктура
- **Объекты КИИ**
  - **Информационные системы**
  - **Информационно-телекоммуникационные сети**
  - **Автоматизированные системы управления**
- **Субъекты КИИ**
  - Кто?
    - Госорганы и госучреждения
    - Российские юрлица и ИП
  - Как принадлежит?
    - Право собственности
    - Аренда
    - Иные законные основания
  - Что принадлежит?
  - В каких сферах?
    - **Здравоохранение**
    - **Наука**
    - **Транспорт**
    - **Связь**
    - **Энергетика**
    - **Банковская сфера и иные сферы финансовой сферы**
    - **Топливно-энергетический комплекс**
    - **Область атомной энергии**
    - **Промышленность**
      - **Оборонная**
      - **Ракетно-космическая**
      - **Горнодобывающая**
      - **Металлургическая**
      - **Химическая**
  - Кто ещё?
    - **Российские юрлица и ИП, обеспечивающие взаимодействие указанных систем или сетей**

Чем регулируется безопасность КИИ? (ст. 3)
- Конституция РФ
- Общепризнанные принципы и нормы международного права
- Настоящим ФЗ
- Другими ФЗ и иными НПА
- 126-ФЗ «О связи» в части сетей связи общего пользования

Принципы обеспечения безопасности КИИ (ст.4)
- Законность
- Непрерывность и комплексность
  - За счет взаимодействия уполномоченных ФОИВ и субъектов КИИ
- Приоритет предотвращения компьютерных атак

ГосСОПКА (ст.5)
- ФОИВ, уполномоченный в области ГосСОПКА)
  - Кто занимается?
    - Национальный координационный центр по компьютерным инцидентам
    - Подразделения и должностные лица субъектов КИИ
  - Кто его создаёт и определяет положение о деятельности?
- Какие средства применяются?
  - Технические, программные, программно-аппаратные и иные средства,...
  - ...для обнаружения, предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, а также криптографические средства защиты такой информации.
- Откуда поступает информация?
  - Средства ГосСОПКА
  - От субъектов КИИ
  - От ФОИВ, уполномоченного в области обеспечения безопасности КИИ
  - От иных организаций, в том числе иностранных и международных
- Кто определяет порядок предоставления и обмена информацией?
  - ФОИВ, уполномоченный в области ГосСОПКА
  - Для сведений, составляющих гостайну, особый порядок

Полномочия (ст.6)

Президент РФ определяет
- Основные направления госполитики в области обеспечения безопасности КИИ
- ФОИВ, уполномоченный в области обеспечения безопасности КИИ
- ФОИВ, уполномоченный в области ГосСОПКА
- Порядок создания и задачи ГосСОПКА

Правительство РФ устанавливает
- Показатели критериев значимости объектов КИИ и их значения
- Порядок и сроки категорирования объектов КИИ
- Порядок осуществления госконтроля для значимых объектов КИИ
- Порядок подготовки и использования ресурсов единой сети электросвязи РФ для обеспечения функционирования значимых объектов КИИ

ФОИВ, уполномоченный в области обеспечения безопасности КИИ (ФСТЭК России)
- Вносит предложения о совершенствовании законодательства Президенту и Правительству
- Утверждает порядок ведения реестра значимых объектов КИИ
- Утверждает форму направления сведений о результатах категорирования
- Устанавливает требования по обеспечению безопасности значимых объектов КИИ
- Устанавливает требования к созданию систем безопасности значимых объектов КИИ
- Осуществляет госконтроль в области обеспечения безопасности значимых объектов КИИ
- Утверждает форму акта проверки по итогам контроля

ФОИВ, уполномоченный в области ГосСОПКА (ФСБ России)
- Вносит предложения о совершенствовании законодательства Президенту и Правительству
- Создает национальный координационный центр по компьютерным инцидентам и утверждает положение о нем
- Координирует деятельность субъектов КИИ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты
- Организует и проводит оценку безопасности КИИ
- Определяет перечень информации, представляемой в ГосСОПКА
- Утверждает порядок информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак в отношении значимых объектов ИИ
  - В банковской и иных сферах финансового рынка порядок согласовывается с Центробанком
- Утверждает порядок обмена информацией о компьютерных инцидентах между
  - Субъектами КИИ
  - Субъектами КИИ и и уполномоченными органами иностранных государств, международным, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты
- Утверждает порядок получения субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения
- Организует установку на значимых объектах КИИ и в сетях электросвязи, используемых для организации взаимодействия этих объектов средств ГосСОПКА
- Устанавливает требования к средствам ГосСОПКА
- Утверждает порядок, технические условия установки и эксплуатации средств ГосСОПКА
  - ...за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи
  - В банковской и иных сферах финансового рынка порядок согласовывается с Центробанком

ФОИВ, уполномоченный в области связи (Минкомсвязь)
- Утверждает по согласованию с ФОИВ, уполномоченным в области ГосСОПКА порядок, технические условия установки и эксплуатации средств ГосСОПКА в сетях электросвязи

Категорирование объектов КИИ (ст.7)
- Исходя из чего осуществляется?
  - Социальная значимость
    - Ущерб жизни и здоровью людей
    - Возможность прекращения или нарушения функционирования:
      - объектов обеспечения жизнедеятельности населения
      - транспортной инфраструктуры
      - сетей связи
    - Максимальное время отсутствия доступа к государственной услуге для получателей такой услуги
  - Политическая значимость
    - Оценка возможного ущерба интересам РФ в вопросах внутренней и внешней политики
  - Экономическая значимость
    - Оценка возможного причинения прямого и косвенного ущерба:
      - субъектам КИИ
      - бюджетам РФ
  - Экологическая значимость
    - Оценка уровня воздействия на окружающую среду
  - Значимость объекта КИИ для обеспечения обороны страны, безопасности государства и правопорядка
- Сколько категорий?
  - Три – первая, вторая и третья
  - Если объект КИИ не соответствует критериям значимости, показателям этих критериев и их значениям, ему на присваивается ни одна из категорий
- Кто присваивает?
  - Субъекты КИИ в соответствии с порядком категорирования
- Куда направлять?
  - В ФОИВ, уполномоченный в области обеспечения безопасности КИИ
  - ...в 10дневный срок со дня проведения категорирования
- Кто проверяет?
  - ФОИВ, уполномоченный в области обеспечения безопасности КИИ
  - ...в 30дневный срок со дня получения
- Категорирование проведено правильно?
  - ДА
    - Сведения о значимом объекте КИИ вносятся в реестр
    - Субъект КИИ уведомляется в 10дневный срок
    - Сведения об отсутствии необходимости присвоения категории значимости направляются в ГосСОПКА
  - НЕТ
    - Субъекту КИИ направляется письменное мотивированное обоснование причин возврата
    - ...в 10дневный срок
    - ...на устранение недостатков субъекту КИИ отводится 10 дней
  - НЕ СДЕЛАНО В СРОК
    - ФОИВ, уполномоченный в области обеспечения безопасности КИИ, направляет субъекту КИИ требование о необходимости соблюдения требований законодательства
- Как может быть изменена категория объекта КИИ?
  - По решению ФОИВ, уполномоченного в области обеспечения безопасности КИИ, по итогам проверки в рамках госконтроля
  - При изменении самого объекта КИИ (таком, что изменились показатели его значимости)
  - При ликвидации, реорганизации субъекта КИИ и (или) изменения его организационно-правовой формы (такие, что он перестал быть субъектом КИИ)

Реестр значимых объектов КИИ (ст.8)
- Ведёт ФОИВ, уполномоченный в области обеспечения безопасности КИИ
- Содержит сведения
  - Наименование значимого объекта КИИ
  - Наименование субъекта КИИ
  - Сведения о взаимодействии объекта КИИ и сетей электросвязи
  - Сведения о лице, эксплуатирующем значимый объект КИИ
  - Категория значимости значимого объекта КИИ
  - Сведения об используемых программных и программно-аппаратных средствах
  - Меры, применяемые для обеспечения безопасности значимого объекта КИИ
- Сведения из реестра направляются в ГосСОПКА
- В случае утраты категории значимости объект исключается из реестра

Права и обязанности субъектов КИИ (ст.9)
- Субъекты КИИ имеют право
  - Получать от ФОИВ, уполномоченного в области обеспечения безопасности КИИ, информацию
    - ...необходимую для обеспечения безопасности своих значимых объектов КИИ
    - ...об угрозах безопасности обрабатываемой их объектами информации
    - ...об уязвимости программного обеспечения, оборудования и технологий, используемых на их объектах
  - В установленном порядке получать от ФОИВ, уполномоченного в области ГосСОПКА информацию
    - ...о средствах и способах проведения компьютерных атак, а также о методах их предупреждения и обнаружения
  - За свой счет приобретать, арендовать, устанавливать и обслуживать средства ГосСОПКА (по согласованию с ФОИВ, уполномоченным в области ГосСОПКА)
  - Разрабатывать и осуществлять мероприятия по обеспечению безопасности значимого объекта КИИ
- Субъекты КИИ обязаны
  - Незамедлительно информировать о компьютерных инцидентах ФОИВ, уполномоченный в области ГосСОПКА
    - ...а также Центробанк (в случае, если субъект КИИ осуществляет деятельность в банковской и иных сферах финансового рынка)
  - Оказывать содействие должностным лицам ФОИВ, уполномоченного в области ГосСОПКА, в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов
  - Обеспечивать выполнение порядка, технических условий установки и эксплуатации средств ГосСОПКА, их сохранность (в случае установки их на объектах)
  - Субъекты КИИ, у которых есть значимые объекты КИИ, дополнительно обязаны
    - Соблюдать требования по обеспечению безопасности значимых объектов КИИ, установленные ФОИВ, уполномоченным в области обеспечения безопасности КИИ
    - Выполнять предписания должностных лиц ФОИВ, уполномоченного в области обеспечения безопасности КИИ, об устранении нарушений в части соблюдения требований по обеспечению безопасности значимого объекта КИИ, выданные этими лицами в соответствии со своей компетенцией
    - Реагировать на компьютерные инциденты в порядке, утвержденном ФОИВ, уполномоченным в области ГосСОПКА, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ
    - Обеспечивать беспрепятственный доступ должностным лицам ФОИВ, уполномоченного в области обеспечения безопасности КИИ, к значимым объектам КИИ при реализации этими лицами полномочий, предусмотренных статьей 13

Система безопасности значимого объекта КИИ (ст.10
- Субъект КИИ создает систему безопасности значимого объекта КИИ и обеспечивает ее функционирование
- Задачи системы безопасности
  - Предотвращение
    - ...неправомерного доступа к информации, обрабатываемой значимым объектом КИИ
    - ...уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения
    - ...иных неправомерных действий в отношении такой информации
  - Недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта КИИ
  - Восстановление функционирования значимого объекта КИИ
    - (в том числе за счет создания и хранения резервных копий необходимой для этого информации)
  - Непрерывное взаимодействие с ГосСОПКА

Требования по обеспечению безопасности значимых объектов КИИ (ст.11)
- Устанавливаются ФОИВ, уполномоченным в области обеспечения безопасности КИИ
- Дифференцируются в зависимости от категории значимости объектов КИИ
- Требованиями предусматриваются
  - Планирование, разработка, совершенствование и осуществление внедрения мероприятий по обеспечению безопасности значимых объектов КИИ
  - Принятие организационных и технических мер для обеспечения безопасности значимых объектов КИИ
  - Установление параметров и характеристик программных и программно-аппаратных средств, применяемых для обеспечения безопасности значимых объектов КИИ
- Дополнительные отраслевые требования
  - Кто их согласует?
    - Государственные органы и российские юридические лица, выполняющие функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности
    - ФОИВ, уполномоченный в области обеспечения безопасности КИИ
  - Содержат особенности функционирования объектов в установленной сфере деятельности

Оценка безопасности КИИ (ст.12)
- Осуществляется ФОИВ, уполномоченным в области ГосСОПКА
- Цели: прогнозирование возникновения возможных угроз безопасности КИИ и выработка мер по повышению устойчивости ее функционирования при проведении в отношении ее компьютерных атак
- При оценке безопасности проводится анализ
  - Данных,...
    - ...получаемых при использовании средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты
    - ...в том числе информации о наличии в сетях электросвязи, используемых для организации взаимодействия объектов КИИ, признаков компьютерных атак
  - Информации, представляемой...
    - ...субъектами КИИ
    - ...ФОИВ, уполномоченным в области обеспечения безопасности КИИ
    - ...иными не являющимися субъектами КИИ органами и организациями, в том числе иностранными и международными
    - Перечень информации и порядок предоставления определяет ФОИВ, уполномоченный в области ГосСОПКА
  - Сведений, представляемых в ГосСОПКА по итогам госконтроля, о нарушении требований по обеспечению безопасности значимых объектов КИИ, в результате которого создаются предпосылки возникновения компьютерных инцидентов
  - Иной информации, получаемой ФОИВ, уполномоченным в области ГосСОПКА, в соответствии с законодательством РФ
- Для оценки безопасности ФОИВ, уполномоченный в области ГосСОПКА, организует установку в сетях электросвязи, используемых для организации взаимодействия объектов КИИ, средств, предназначенных для поиска признаков компьютерных атак в таких сетях электросвязи
- ФОИВ, уполномоченный в области ГосСОПКА, направляет в ФОИВ, уполномоченный в области обеспечения безопасности КИИ, результаты осуществления оценки безопасности КИИ

Госконтроль в области обеспечения безопасности значимых объектов КИИ (ст.13)
- Цель: проверка соблюдения субъектами КИИ, у которых есть значимые объекты КИИ, требований законодательства
- Проводит ФОИВ, уполномоченный в области обеспечения безопасности КИИ
- Проверки бывают плановые и внеплановые
- Основанием для плановой проверки является истечение 3х лет со дня...
  - ...внесения сведений об объекте КИИ в реестр значимых объектов КИИ
  - ...окончания осуществления последней плановой проверки
- Основанием для внеплановой проверки является...
  - ...истечение срока выполнения выданного предписания об устранении выявленного нарушения
  - ...возникновение компьютерного инцидента, повлекшего негативные последствия, на значимом объекте КИИ
  - ...приказ (распоряжение) руководителя ФОИВ, уполномоченного в области обеспечения безопасности КИИ
    - по поручению Президента или Правительства
    - на основании требования прокурора (по поступившим в органы прокуратуры материалам и обращениям)
- По итогам составляется акт проверки по утвержденной форме
- В случае выявления нарушения выдаётся предписание об устранении выявленного нарушения с указанием сроков его устранения

Ответственность за нарушение требований настоящего ФЗ (ст.14 В соответствии с законодательством Российской Федерации

Вступление в силу (ст.15) С 1 января 2018 года