ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С. П. КОРОЛЕВА»

**Краткий анализ документов по обеспечению безопасности критических информационных инфраструктур (КИИ)**

Выполнил:

Барсуков М.Н.

гр. 6313-100503D

Самара 2024

Обеспечение безопасности объектов критической информационной инфраструктуры (КИИ) является одной из ключевых задач государственной политики России. Необходимость защиты информационных ресурсов становится более актуальной. Важную роль играют федеральные законы и указы, которые регулируют деятельность в области обеспечения безопасности КИИ.

**1. Федеральный закон 194 "О безопасности критической информационной инфраструктуры Российской Федерации"**

Федеральный закон 194, принятый в 2017 году, стал основополагающим актом, определяющим правовые основы для обеспечения безопасности КИИ. Он вводит понятие "критическая информационная инфраструктура", которое охватывает объекты, жизненно важные для функционирования государства и общества. Это могут быть энергетические системы, транспорт, здравоохранение, финансовые учреждения и другие важные секторы.

Закон устанавливает четкие обязанности для операторов КИИ, включая:

* Внедрение систем защиты информации: Операторы обязаны разрабатывать и внедрять системы защиты информации, соответствующие современным стандартам.
* Проведение регулярных проверок: необходимо проводить регулярные проверки и аудит безопасности информационных систем, что позволяет выявлять и устранять уязвимости

Закон вводит механизмы государственного контроля за соблюдением требований безопасности. Это включает:

* Мониторинг и оценка: Государственные органы имеют право проводить мониторинг и оценку уровня защищенности объектов КИИ.
* Ответственность за нарушения: Установлены меры ответственности за нарушение требований безопасности, что подчеркивает важность соблюдения законодательства.

**2. Федеральный закон 193 "О безопасности информации"**

Федеральный закон 193, акцентирует внимание на защите информации, что является критически важным для обеспечения безопасности КИИ. Основные положения включают:

* Классификация данных: Закон требует классификации информации в зависимости от ее важности и уровня конфиденциальности, что позволяет определить необходимые меры защиты.
* Меры по предотвращению утечек: Установлены конкретные меры, направленные на предотвращение утечек информации, включая технические и организационные решения.

Закон обязывает операторов КИИ взаимодействовать с правоохранительными органами, что включает:

* Предотвращение инцидентов: Операторы должны сообщать о потенциальных угрозах и инцидентах, что способствует более эффективному реагированию на кибератаки.
* Расследование инцидентов: Правоохранительные органы имеют право проводить расследования в случае возникновения инцидентов, что позволяет выявлять и пресекать преступные действия.

**3. Указ Президента РФ № 98 "О национальной политике в области безопасности"**

Указ 98, изданный в 2016 году, определяет стратегические направления государственной политики в области безопасности. Основные акценты:

* Защита КИИ как приоритет: Подчеркивается важность защиты объектов КИИ как одного из ключевых направлений государственной безопасности.
* Национальная безопасность: Указ связывает защиту КИИ с общими задачами национальной безопасности, что подчеркивает необходимость комплексного подхода.

Указ описывает механизмы взаимодействия между различными государственными органами, включая:

* Создание рабочих групп: для решения вопросов безопасности КИИ создаются межведомственные рабочие группы, что способствует более эффективному обмену информацией и ресурсами.
* Координация действий: Установлены механизмы координации действий между различными органами власти, что позволяет более эффективно реагировать на угрозы.

**4. Указ Президента РФ № 620 "О мерах по обеспечению безопасности КИИ"**

Указ 620, принятый в 2018 году, конкретизирует меры, направленные на защиту КИИ:

* Формирование групп: Указ предписывает создание межведомственных рабочих групп для разработки и внедрения мер безопасности, что позволяет объединить усилия различных ведомств.
* Обмен опытом: Рабочие группы занимаются обменом опытом и лучшими практиками в области обеспечения безопасности

Указ устанавливает требования к разработке стандартов безопасности для объектов КИИ:

* Создание стандартов: Разработка стандартов безопасности позволяет унифицировать подходы к обеспечению защиты информации и инфраструктуры.
* Обеспечение соответствия: Стандарты помогают обеспечить соответствие требованиям законодательства и международным нормам.

**5. Указ Президента РФ № 250 "О дополнительных мерах по обеспечению информационной безопасности"**

Указ 250, изданный в 2022 году, вводит дополнительные меры по обеспечению безопасности КИИ:

* Ответственные лица: Руководители органов и организаций должны назначить заместителей, отвечающих за информационную безопасность, что повышает уровень ответственности.
* Создание структурных подразделений: Необходимо создать или назначить существующее подразделение для выполнения функций по обеспечению информационной безопасности.

С 2025 года вводится запрет на использование средств защиты информации, производимых недружественными странами:

* Укрепление внутренней безопасности: Запрет направлен на укрепление внутренней безопасности и снижение зависимости от иностранных технологий.
* Поддержка отечественных разработчиков: Это также создает возможности для развития отечественных производителей и технологий в области информационной безопасности.

Документы, регулирующие безопасность объектов КИИ, представляют собой комплексный подход к защите критической инфраструктуры. Они устанавливают четкие требования и обязанности для операторов, а также механизмы государственного контроля и межведомственного взаимодействия.