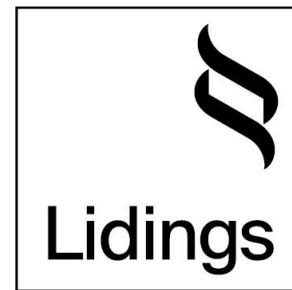


14 ноября 2024 года

Конференция «Управление юридическими рисками: статус 2024»
Dialog Management



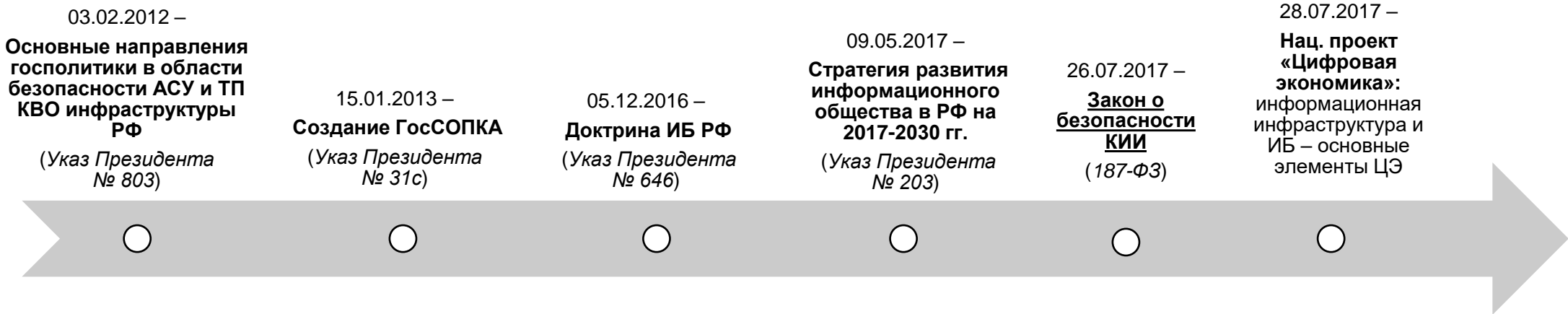
Безопасность критической информационной инфраструктуры (КИИ): правовой аспект

Наталья Тотихева, адвокат, советник Lidings

План

- Безопасность КИИ: основные понятия и актуальность
- Сферы деятельности по 187-ФЗ: объекты и субъекты КИИ, методология определения субъекта КИИ
- Типовые объекты КИИ: примеры индустрии Pharma и FMCG
- План действий потенциального субъекта КИИ
- Внутренняя оценка относимости субъекта: основные проблемы, роли и процедуры
- Государственный контроль и ведомственный мониторинг
- Правоприменительная практика: риски и ответственность
- Кейсы Lidings: рекомендации и выводы

Безопасность КИИ: основные понятия



- **КИИ** – объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов
- **Объекты КИИ** – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления (АСУ) субъектов КИИ. ЗОКИИ – значимые объекты КИИ
- **Потенциальные субъекты КИИ** – государственные органы, государственные учреждения, российские юридические лица и (или) ИП

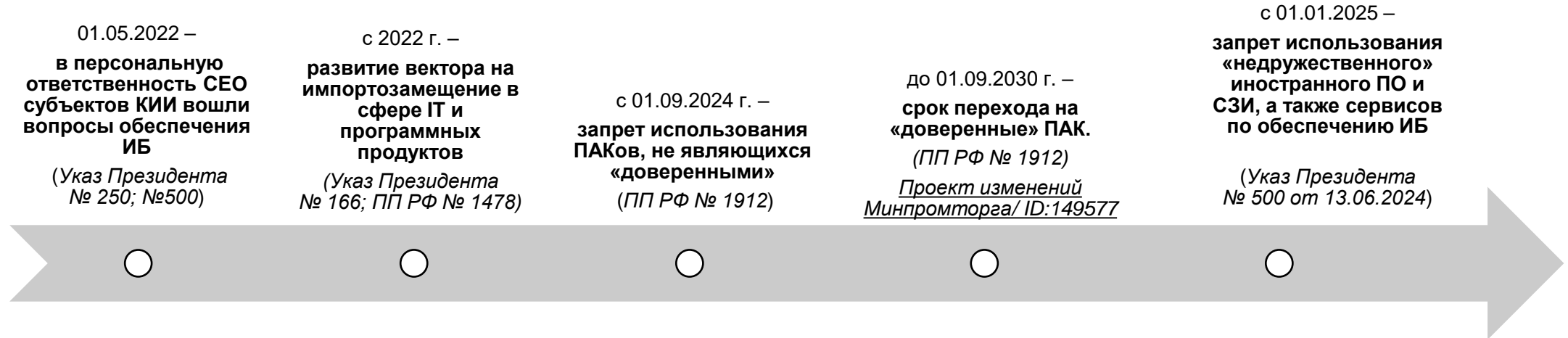
**Новые требования к субъектам КИИ,
дополнительные разрешительные
процедуры и ограниченные сроки
реализации требований по
импортозамещению**

**Сложность идентификации
(самоопределение субъекта КИИ)**

**Вопросы ИБ - комплаенса и определение
ответственного лица по вопросам
безопасности КИИ**

**Кратное увеличение процента кибер -
атак и высокий процент латентной
преступности в сфере ИБ**

Изменение вектора и актуальность вопроса



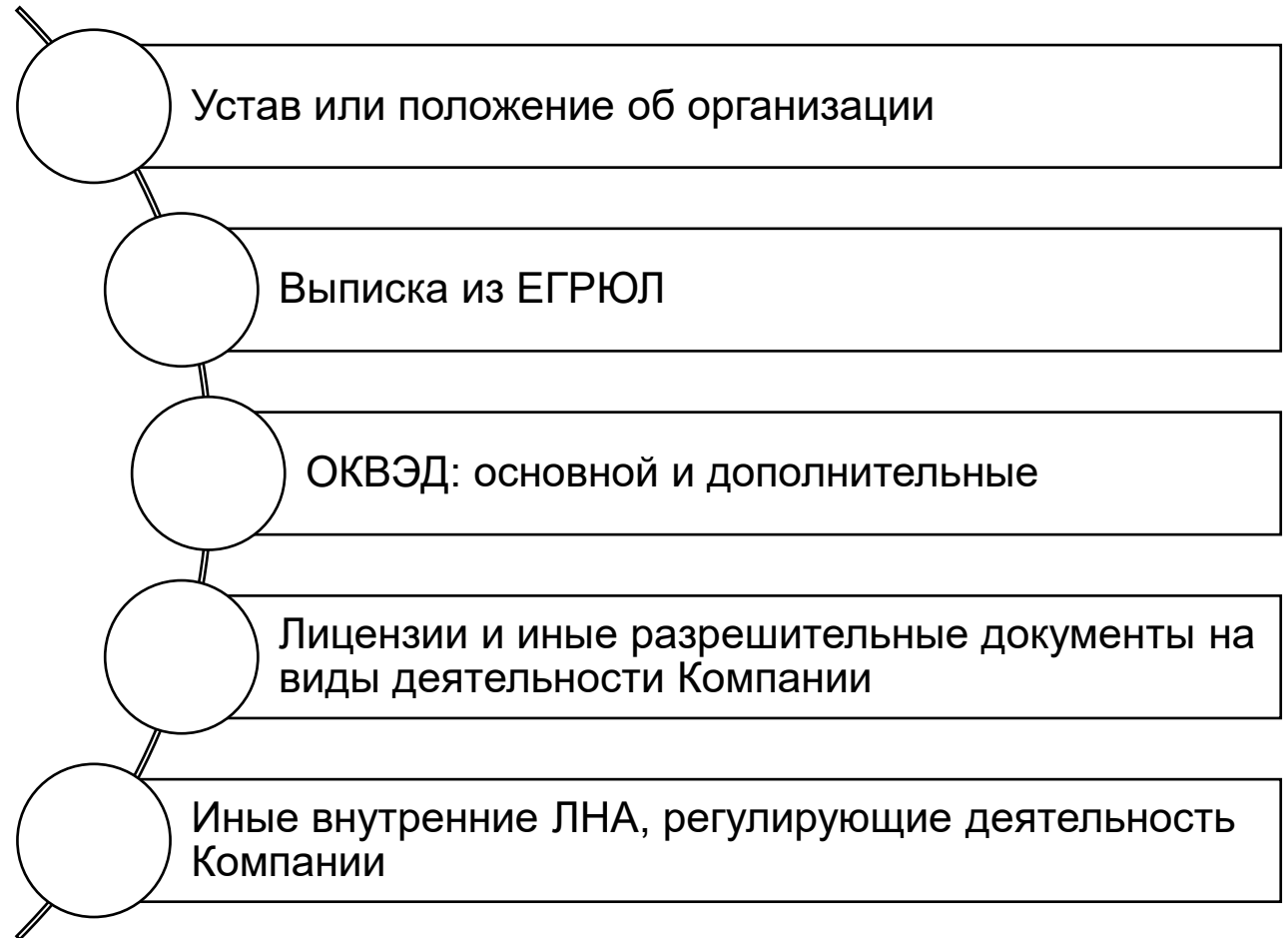
- с 01 сентября 2024 г. - запрет использования ПАКов, не являющихся «доверенными» на ЗОКИИ РФ. Реестр ПО и ПАК ведет Минцифры
- **Предусмотрено исключение:** невозможность замены ПАКов ввиду отсутствия аналогов
- **Исключение подтверждается Минпромторгом**
- **4 месяца** – срок предоставления плана перехода на «доверенные» ПАК

«Формула» субъекта КИИ



Сферы 187-ФЗ и анализ деятельности организации

- **ЗДРАВООХРАНЕНИЕ**
- **НАУКА**
- **ТРАНСПОРТ**
- **СВЯЗЬ**
- **ЭНЕРГЕТИКА**
- **ГОС. РЕГИСТРАЦИЯ ПРАВ НА НЕДВИЖИМОЕ ИМУЩЕСТВО И СДЕЛОК С НИМИ** (*ред. 10.07.2023*)
- **БАНКОВСКАЯ СФЕРА И ИНЫЕ СФЕРЫ ФИНАНСОВОГО РЫНКА**
- **ТЭК**
- **АТОМНАЯ ЭНЕРГИЯ**
- **РАКЕТНО-КОСМИЧЕСКАЯ**
- **ГОРНОДОБЫВАЮЩАЯ**
- **МЕТАЛЛУРГИЧЕСКАЯ**
- **ХИМИЧЕСКАЯ ПРОМЫШЛЕННОСТЬ**
- **ОБОРОНА**



Объекты КИИ и типовые объекты КИИ

с 21 марта 2023 г.
отраслевые ведомства
вправе формировать
перечень типовых
отраслевых объектов КИИ

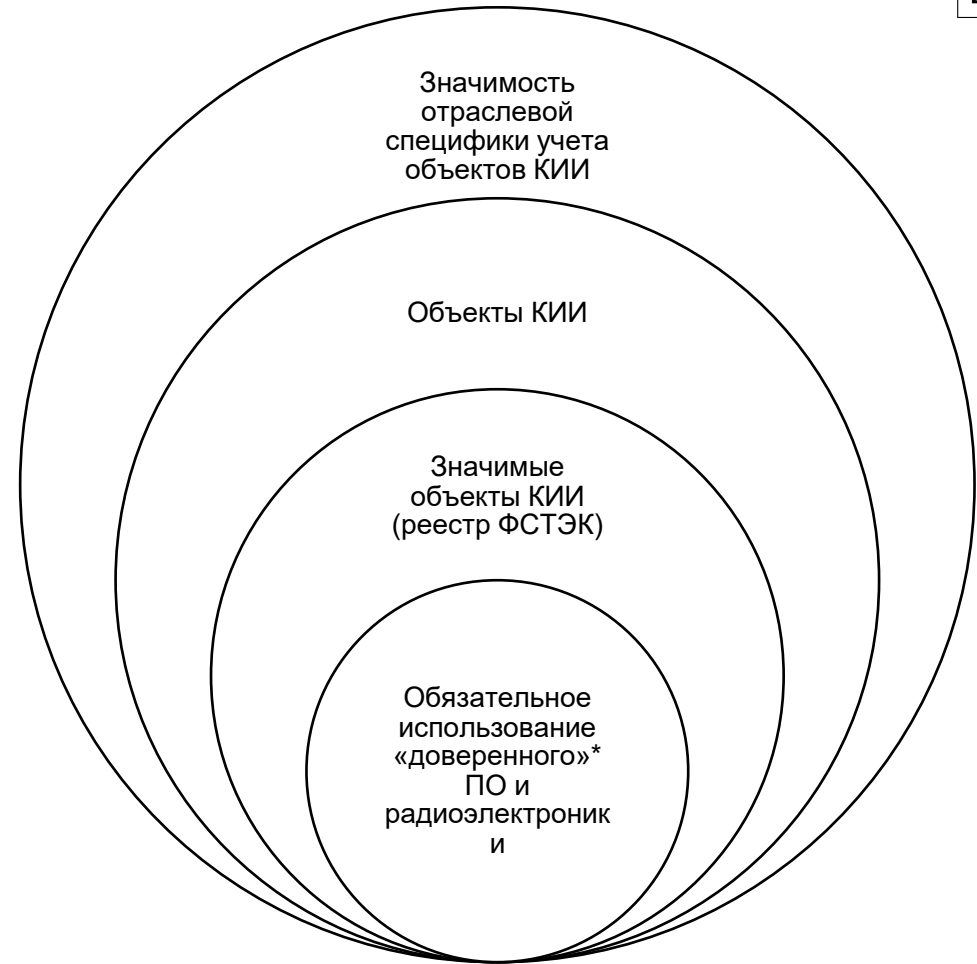
Определение объектов
КИИ осуществляется с
учетом представленных
терминов, а также на
основании
эксплуатационной и
технической документации

ИС (ГИС, МИС, ИСПДн)	ИТКС	АСУ
<ul style="list-style-type: none"> совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (ФЗ №149-ФЗ) 	<ul style="list-style-type: none"> технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (<i>связь, Интернет</i>) 	<ul style="list-style-type: none"> комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами (<i>оптимизация работы предприятий</i>)

Учет отраслевых особенностей...

В июле 2024 г. Государственной думой был принят в первом чтении Законопроект № 581689-8 об изменении 187-ФЗ:

категорирование объектов необходимо осуществлять **с учетом отраслевых особенностей**, типовых объектов и методических указаний утвержденных с участием отраслевых ФОИВ (*Законопроект устанавливает вступление в силу 01.03.25*)



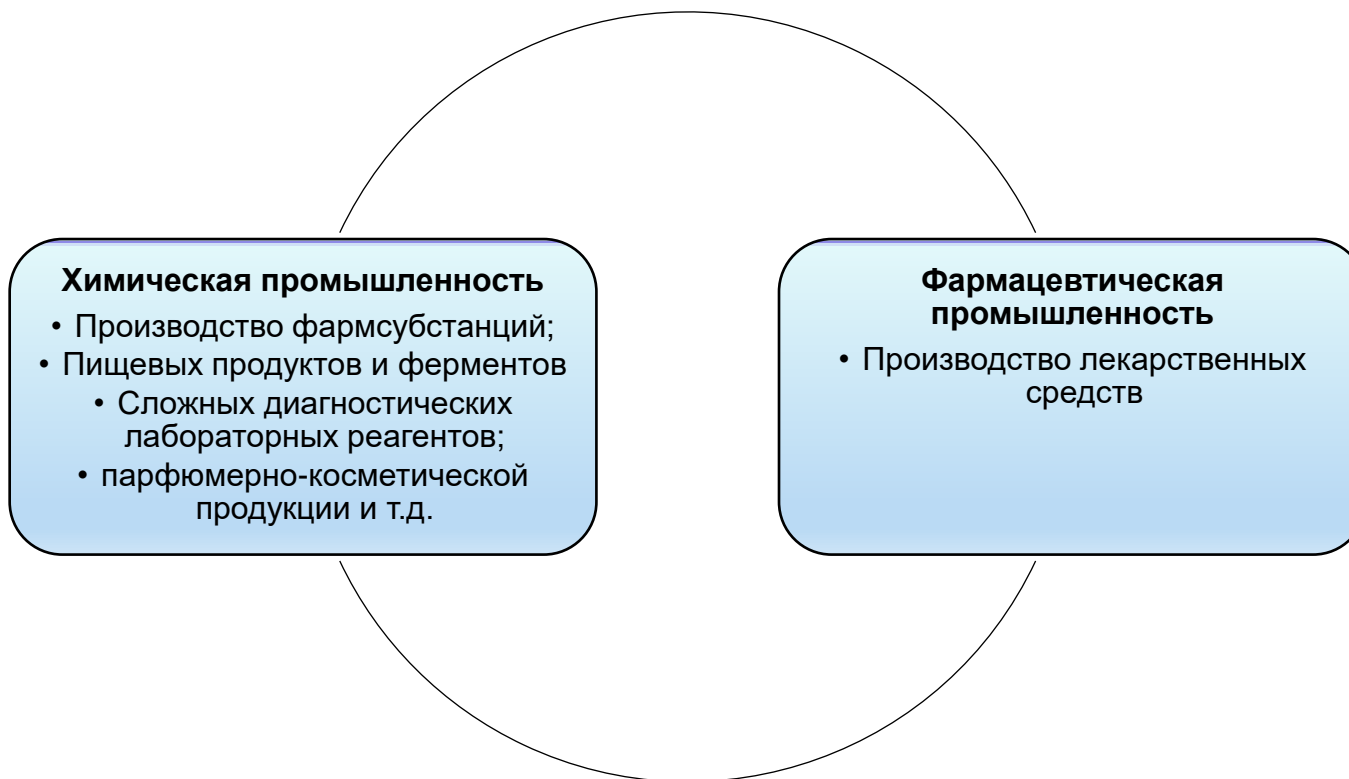
*Реестр Российского и Евразийского ПО и ПАК ведет Минцифры: на сегодня включает около 22 тыс. ПО.

Типовые объекты КИИ: примеры Pharma и FMCG индустрии

- **Минпромторг** – «профильный» ФОИВ для предприятий **оборонной, химической промышленности**
- 25.01.2024 г. – Перечень типовых объектов КИИ РФ, функционирующих в области оборонной промышленности (организации прямо или косвенно участвующие в выполнении ГОЗ). Сводный реестр организаций ОПК ведет Минпромторг (*Приказ от 02.09.2021 № 3436*)
- 12.01.2024 г. – Перечень типовых объектов КИИ РФ в химической промышленности
- Перечни содержат информацию о типовых объектах (ИС, ИТКС, АСУ), критических процессах и видов деятельности, для обеспечения которых используется объект (ОКВЭД)
- **Минздрав** – «профильный» ФОИВ для субъектов в **сфере здравоохранения**
- 27.12.2023 г. – Перечень типовых отраслевых объектов КИИ РФ, функционирующих в сфере здравоохранения
- ОКВЭД: 21.10 – Производство фармацевтических субстанций 21.20 - Производство лекарственных препаратов и материалов для медицинского применения

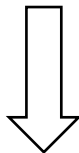
Учет отраслевых особенностей...

Стратегические документы Правительства по развитию технологического суверенитета выделяют фармацевтическую и химическую промышленность
(Постановление Правительства РФ от 15.04.2023 № 603)

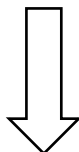


План действий по обнаружению...

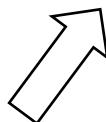
1) Первичный сбор и **анализ данных о деятельности компании и взаимодействии с «регуляторами»**



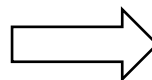
2) «**Инвентаризация**» систем, подпадающих под определение объектов КИИ и оценка их функционирования



3) Анализ соответствия деятельности компании сферам установленным 187-ФЗ, **оценка наличия или отсутствия объектов КИИ**, функционирующих в сфере 187-ФЗ, а также **оснований их принадлежности компании (проверка контрактов с 3 лицами)**

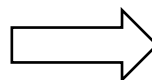


**Оценка относимости
Компании к
субъектам КИИ:
Заключение по
самооценке (Self-
assessment
заключение)**



Наличие обязанностей субъекта 187-ФЗ

- Создание комиссии по категорированию, назначение ответственных
- Сбор дополнительной информации о ОКИИ, определение процессов в рамках выполнения субъектом функций
- Выявление из них критичных процессов
- Определение ОКИИ, связанных с критическими процессами, подлежащий категорированию, направление сведений в ФСТЭК и иное...



Отсутствие обязанностей по 187-ФЗ

Предоставление информации об отсутствии в организации объектов КИИ или о том, что организация не является субъектом КИИ РФ в ФСТЭК России в соответствии с законодательством о безопасности КИИ РФ **не требуется** (*Информационное сообщение ФСТЭК России от 17 апреля 2020 г. № 240/84/611*)

Права субъектов КИИ	Обязанности субъектов КИИ
<ul style="list-style-type: none">▪ Получать от ФСБ/ФСТЭК, информацию, необходимую для обеспечения безопасности значимых объектов КИИ▪ При наличии согласия ФСБ ФСТЭК за свой счет приобретать, арендовать, устанавливать и обслуживать средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты▪ Разрабатывать и осуществлять мероприятия по обеспечению безопасности значимых объектов КИИ	<ul style="list-style-type: none">▪ Категорировать объекты КИИ▪ Выполнять требования по обеспечению безопасности объектов КИИ (ФСТЭК России)▪ Устанавливать и эксплуатировать средства обнаружения, предупреждения и ликвидации последствий компьютерных атак (центры ГосСОПКА и тех. средства ФСБ)▪ Реагировать на компьютерные инциденты, информировать о них и принимать меры по ликвидации последствий▪ Содействовать должностным лицам при исполнении ими своих служебных обязанностей

Оценка относимости Компании: нюансы проверки

Кто может быть ответственным за соблюдение законодательства о безопасности КИИ?

- 1) Для выполнения оценки рекомендуется **сформировать Рабочую группу** (допустимо не включать CEO)
- 2) Провести анализ ЛНА Компании в области ИБ на предмет **положений о безопасности КИИ и оперативном порядке реагирования и выполнения требований законодательства о безопасности КИИ**
- 3) Для проведения полного и достоверного анализа рекомендуется **привлекать сотрудников по ИБ, владеющих информацией о системах компании, юридический/комплаенс департамент, а также держателей основных производственных процессов на «местах»**
- 4) Анализ проводится в отношении непосредственно осуществляемой деятельности, учитывая «прямые» и «косвенные» признаки соответствия сферам 187-ФЗ



Государственный контроль и ведомственный мониторинг

ФСТЭК

- **Государственный контроль в области безопасности КИИ**
- Реестр значимых объектов КИИ
- **Проверка корректности** порядка категорирования и определения категории значимости объекта КИИ и т.д.

ФСБ

- **Безопасность КИИ и предпринятых технических мер:** обнаружение, предупреждение и ликвидация последствий компьютерных атак, реагирование на инциденты (**НКЦКИ**)
- **Координация деятельности субъектов КИИ**
- Функционирование и взаимодействие с **ГосСОПКА**

Ведомственный мониторинг

- С 12.08.2024 рассмотрение перечней из **15 и более** объектов КИИ **в области химической промышленности** - осуществляется центральным аппаратом ФСТЭК России
- Минпромторг осуществляет **мониторинг актуальности и достоверности представлений в ФСТЭК сведений по категорированию объектов КИИ**

(Постановление Правительства РФ от 08.02.2018 №127)

(Информационное сообщение ФСТЭК России от 12 августа 2024 г. № 240/83/2028)

Виды правовой ответственности

Материальная, дисциплинарная, гражданско-правовая

- Неисполнение или ненадлежащее исполнение возложенных трудовых обязанностей (ст. 192 ТК РФ)
- Материальная ответственность работника (глава 39 ТК РФ)
- Ответственность ЮЛ или гражданина за вред причиненный его работником (ст. 1068 ГК РФ)

Административная

- Нарушение требований в области обеспечения безопасности КИИ (ст. 13.12.1 КоАП)
- – **штрафы до 500 000 руб для ЮЛ, до 50 000 для ДЛ**
- Нарушение правил защиты информации (ст. 13.12 КоАП)
- – **штраф и конфискация несертифицированных средств**
- Непредоставление сведений о КИИ (*в том числе предоставление недостоверных сведений*) (ст. 19.7.15 КоАП)
- – **штраф до 100 000 руб. для ЮЛ, до 200 000 руб. (за повторное правонарушение)**
- Неповиновение законному распоряжению должностного лица органа, осуществляющего государственный надзор (контроль) (ст. 19.4 КоАП)

Уголовная

- Неправомерный доступ к компьютерной информации (ст. 272 УК РФ)
- Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)
- Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ)
- Халатность (ст. 293 УК РФ)
- **Неправомерное воздействие на КИИ РФ (274.1 УК РФ)** – предмет доказывания по данному составу будет включать в себя **определение объектов КИИ (ПП ВС №37)**

Судебная практика

«При рассмотрении **уголовных дел** о преступлениях, предусмотренных ст. 272, 273, 274 и 274.1. УК РФ следует руководствоваться положениями законов, в частности 149-ФЗ, 187-ФЗ и других ФЗ, подзаконных актов, технических регламентов, а также ратифицированных международных договоров и соглашений...», в т.ч. **ратифицированное Соглашение СНГ о сотрудничестве в борьбе с преступлениями в сфере информационных технологий, 2021 г.)**

(Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37)

Большинство дел по 274.1 УК РФ приходятся на сферу здравоохранения – внесение недостоверных сведений о **Covid-сертификатах в ЕГИСЗ***

**Определение Шестого кассационного суда общей юрисдикции от 08.11.2023 по делу № 77-4565/2023; Определение Первого кассационного суда общей юрисдикции от 28.08.2023 по делу № 88-22756/2023
приговор Кизилюртовского городского суда Республики Дагестан от 23.12.2021 по делу № 1-148/2021*



Судебная практика: административные дела

Решение Арбитражного суда города Санкт-Петербурга и Ленинградской области от 16.08.2024 по делу № А56-41598/2024:

Фабула: ООО «СТЦ» включённое в реестр ОПК, не представило в т.ч. по требованию сведения о категорировании объектов и было привлечено к ответственности по ч.1 ст. 19.7.15 КоАП

Требование: оспаривание решения о привлечении к ответственности по ст. 19.7.15 КоАП РФ

Решение: Суд признал виновность ООО «СТЦ», однако заменил административное наказание в виде административного штрафа предупреждением (*ввиду совершения правонарушения впервые*)

Решение Ахтубинского районного суда Астраханской области от 04.08.2023 № 12-49/2023:

Фабула: ЮЛ осуществляющее деятельность в области теплосетей было привлечено к ответственности **определило отсутствие объектов КИИ**, но было привлечено в ходе прокурорской проверки по ч. 6 ст. 13.12 КоАП (нарушение правил защиты информации)

Решение: несмотря на позицию прокурора о том, что деятельность организации относится к сфере 187-ФЗ, суд пришел к выводу о том, что **«наличие/отсутствие объектов КИИ является обстоятельством, имеющим значение для правильного разрешения дела»**

Дело прекращено: с учетом 1) истечения 3-месячного срока исковой давности 2) юридически значимые обстоятельства по делу не установлены

Транснациональный производитель продуктов питания

- **Задача:** анализ деятельности (в т.ч. лицензируемых видов деятельности) компании, а также имеющихся производственных процессов на предмет соответствия сферам, установленным 187-ФЗ и оценка необходимости соблюдения требований 187-ФЗ
- **Решение:** поскольку у компании отсутствовали на праве собственности, ином законном основании объекты КИИ, а также основная деятельность компании не соответствовала сферам, установленным 187-ФЗ, результатом анализа стал вывод **об отсутствии соответствия Клиента понятию субъекта КИИ, установленному 187-ФЗ**

Международная фармацевтическая компания

- **Задача:** определение необходимости осуществления требований 187-ФЗ, анализ осуществляемых производственных процессов на предмет их соответствия сферам, установленным 187-ФЗ
- **Решение:** поскольку Компания имела на праве собственности, ином законном основании объекты КИИ, а основная деятельность компании была связана со сферой химической промышленности (производство лекарственных средств и фармацевтических субстанций) Клиент **был определен как соответствующий понятию субъекта КИИ, установленному 187-ФЗ**

Выводы и рекомендации

Вывод:

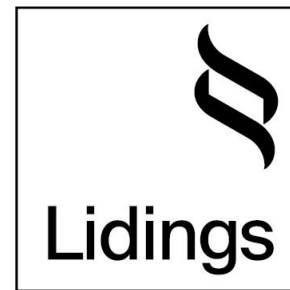
Вопрос о необходимости соблюдения новых требований о безопасности КИИ и иных обязанностей субъектов КИИ необходимо решать после проведения внутренней оценки деятельности потенциального субъекта КИИ с учетом положений законодательства, отраслевой специфики и комплексной оценки деятельности компании

Рекомендуем:

- Провести анализ ЛНА Компании в области ИБ на предмет **положений о безопасности КИИ и оперативного порядка реагирования и выполнения требований законодательства о безопасности КИИ**
- Определить соответствующих ответственных лиц/ рабочую группу по вопросам законодательства в области КИИ
- Провести внутреннюю оценку деятельности компании и ее соответствия требованиям законодательства о безопасности КИИ
- К оценке необходимо привлекать сотрудников по ИБ, владеющих информацией о системах компании, юридический/комплаенс департамент, а также держателей основных производственных процессов «на местах»

Спасибо за внимание

Вопросы и ответы



Наталья Тотехеваге

Советник практики корпоративного права и M&A,
фармацевтика и здравоохранение

nthotahewage@lidings.com

Башня «Империя»,
Пресненская наб., 6, стр. 2,
123112, Москва, Россия

+7 495 989 44 10
moscow@lidings.com
lidings.com

[Telegram](#)
[LinkedIn](#)
[Youtube](#)