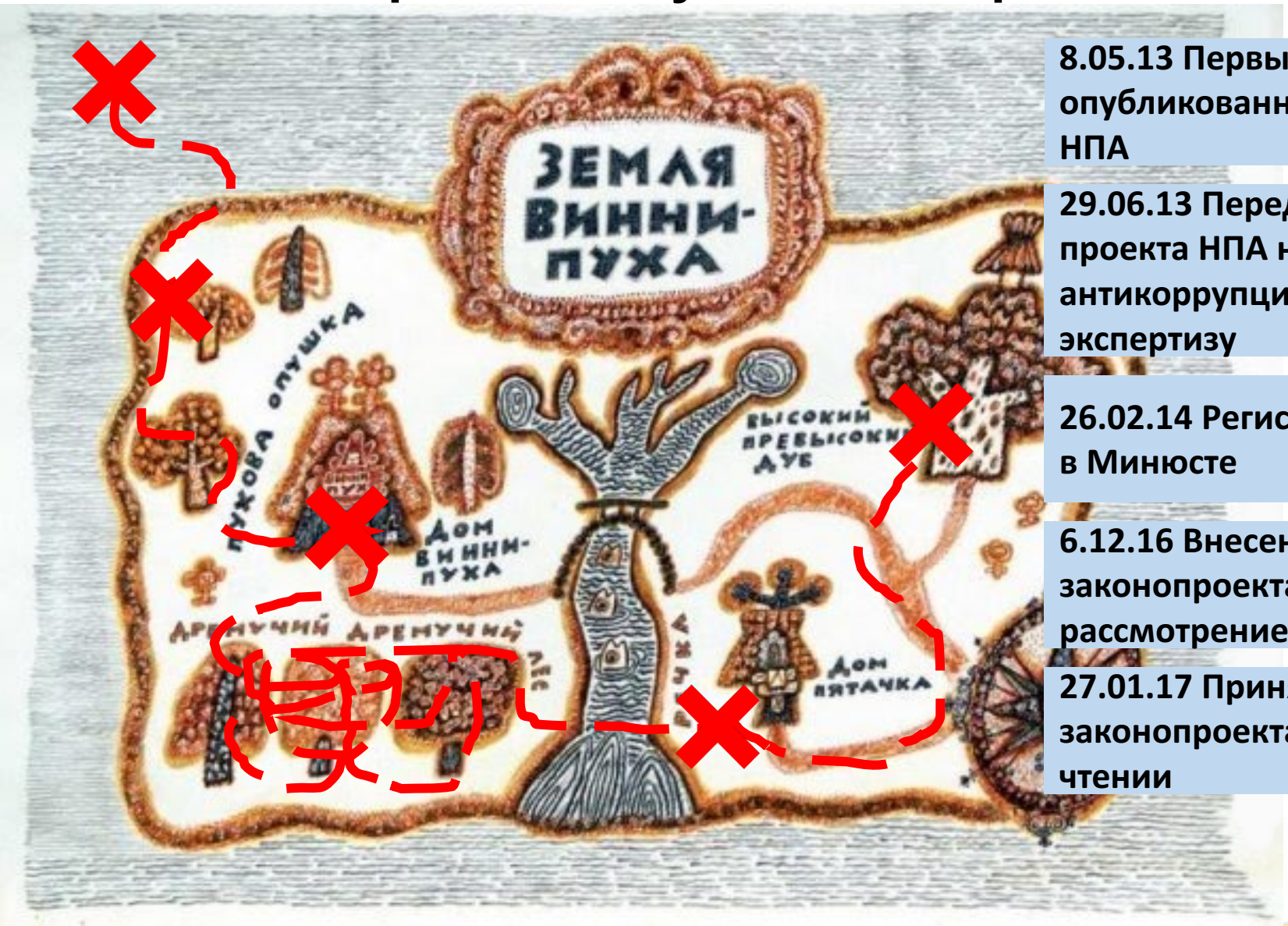
# Проект Федерального закона о безопасности КИИ

Николай Домуховский
Директор ДСИ
ООО «УЦСБ»

# Тернистый путь законопроекта




**8.05.13 Первый опубликованный проект НПА**

**29.06.13 Передача проекта НПА на антикоррупционную экспертизу**

**26.02.14 Регистрация НПА в Минюсте**

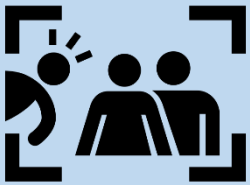
**6.12.16 Внесение законопроекта на рассмотрение в Госдуму**

**27.01.17 Принятие законопроекта в первом чтении**

# Что стоит посмотреть в законопроекте?

**Объекты:**

- Что относится к КИИ?
- На основе чего будут определяться требования по обеспечению ИБ?
- Какие системы обеспечения ИБ будут создаваться?



**Субъекты:**

- Кто будет отвечать за выполнение закона?
- Кто будет определять порядок обеспечения ИБ КИИ?
- Кто будет платить?
- Кого в целом затронет законопроект?

**Мероприятия:**

- Какие изменения в правовом поле повлечет принятие законопроекта?
- Какие подзаконные акты и когда будут разработаны?
- В какие сроки и что необходимо будет реализовать ответственным?

# Объекты КИИ

| Информационные системы | Информационно-телекоммуникационные сети | АСУ ТП |
|---|---|---|
| Госорганы | | |
| Оборонная промышленность | | |
| Здравоохранение | | |
| Транспорт | | |
| Связь | | |
| Кредитно-финансовая сфера | | |
| Энергетика | | |
| Топливная промышленность | | |
| Атомная промышленность | | |
| Ракетно-космическая промышленность | | |
| Горнодобывающая промышленность | | |
| Металлургическая промышленность | | |
| Химическая промышленность | | |

# Субъекты КИИ


Владелец КИИ


Президент РФ

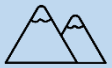

Оператор, эксплуатирующий КИИ


Правительство РФ


Оператор связи, обеспечивающий взаимодействие КИИ


ФОИВ, уполномоченный в области связи


Организации, имеющие лицензии на осуществление деятельности по ТЗКИ

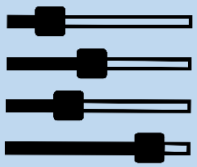

ФОИВ, уполномоченный в области ГосСОПКа


Разработчик (проектировщик) КИИ


ФОИВ, уполномоченной в области обеспечения безопасности КИИ

# Категорирование объектов КИИ

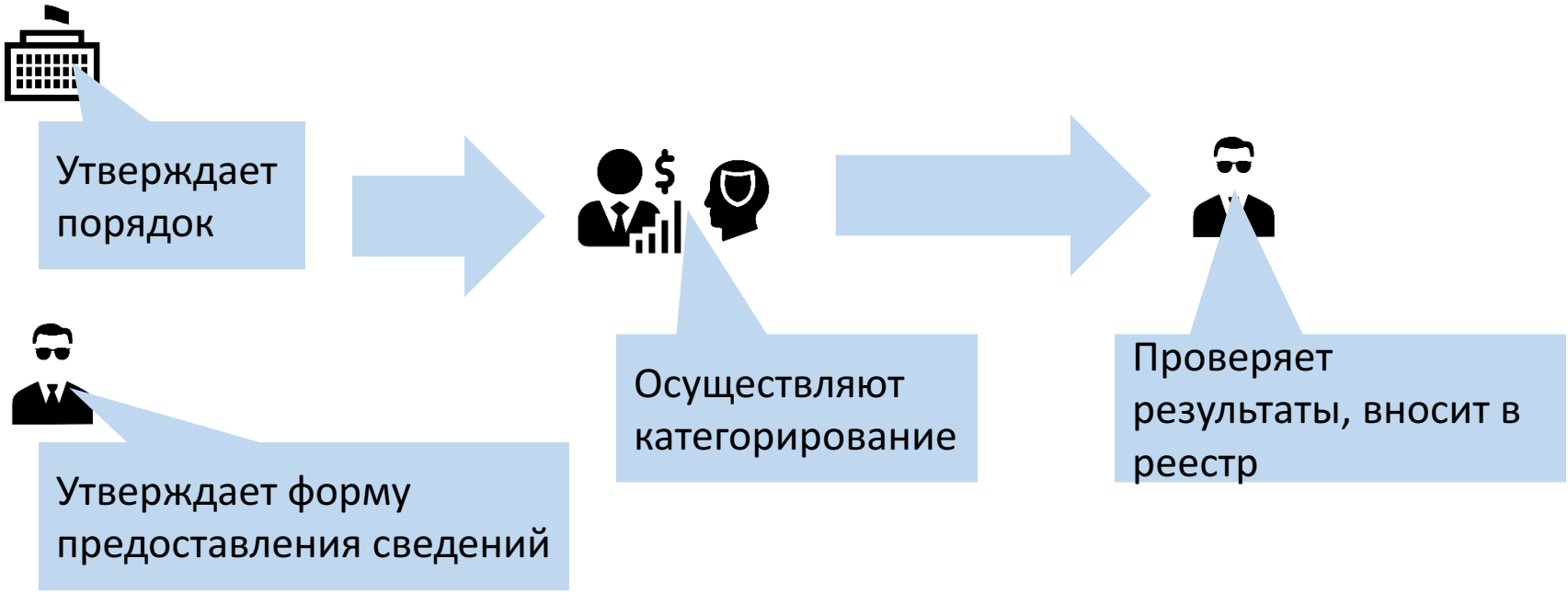
**значимый объект критической информационной инфраструктуры** - объект критической информационной инфраструктуры, которому по итогам категорирования **присвоена одна из категорий значимости** и который включен в реестр значимых объектов критической информационной инфраструктуры



**Критерии категорирования:**

- социальная значимость
- политическая значимость
- экономическая значимость
- экологическая значимость
- значимость для обеспечения обороноспособности , безопасности государства  и правопорядка

# Категорирование объектов КИИ




**Что попадет в реестр:**

- Наименование объекта
- Владелец
- Основание для создания объекта
- Тип объекта
- Разработчик (проектировщик)
- Оператор
- Категория
- Сведения о ПО и ТС
- Меры обеспечения ИБ
- Средства обеспечения ИБ

# Права и обязанности субъектов КИИ

Владелец КИИ

**Имеет право:**

- Получать метод. материалы, а также сведения из ГосСОПКА
- Ставить средства ГосСОПКА за свой счет
- Строить систему обеспечения ИБ КИИ сверх обязательной программы

**Обязан:**

- Информировать о компьютерных инцидентах
- Оказывать содействие органам
- Обеспечить условия функционирования средств ГосСОПКА

Владелец значимого КИИ

**Дополнительно обязан:**

- Выполнять требования по обеспечению ИБ значимых КИИ
- Выполнять предписания ФСТЭК/ФСБ
- Принимать меры по ликвидации последствий компьютерных атак
- Обеспечивать беспрепятственный доступ должностных лиц на объект (для проверок)

# Что будет представлять собой СОИБ КИИ

**Мероприятия:**

- Защита информации в КИИ (от НСД, модификации, уничтожения)
- Предотвращение воздействия на ТСОИ, которое может нарушить работу КИИ
- Обнаружение и предотвращение компьютерных атак
- Восстановление функционирования, в том числе, за счет резервного копирования информации
- Интеграция с ГосСОПКА
- Сбор, анализ и хранение сведений о проведенных в отношении КИИ компьютерных атаках

**Что можно планировать закупать ☺:**

- Endpoint Security
- IDS/IPS
- СРК
- ГосСОПКА
- SIEM/TE

# Правовое поле законопроекта

**УК РФ**
- Добавляется статья 274.1 – то же, что в статьях 272-274, но в отношении объектов КИИ (более строгое наказание)

**Закон «О связи»**
- Обязанность оператора связи обеспечить условия эксплуатации средств ГосСОПКА

**УПК РФ**
- Прямая подследственность ФСБ дел по статье 274.1


**Закон «О государственной тайне»**
- Сведения о мерах по защите значимых КИИ, а также об оценке степени защищенности КИИ (всех!) – ГТ

**Закон «О защите прав юридический лиц …»**
- Закон не будет применяться при проверках КИИ

# Что после часа «Ч»?

**Час «Ч»**

- Вступление в силу ФЗ
- Проверка выполнения требований с 1 января 2018 г. (может измениться во втором чтении)

**Час «Ч» + 6 месяцев**

- Официально назначат ФСБ России и ФСТЭК России
- Новые требования для операторов связи

**Час «Ч» + 9 месяцев**

- Порядок реагирования на инциденты от ФСБ России
- Порядок передачи сведений в ГосСОПКА и получения их из нее
- Требования к техническим средствам ГосСОПКА, условиям их эксплуатации
- Положение о Национальном координационном центре
- Порядок установки и эксплуатации средств ГосСОПКА для операторов связи

**Час «Ч» + 12 месяцев**

- Порядок категорирования КИИ
- Порядок гос. контроля
- Форма предоставления сведений о категорировании
- Правила ведения реестра КИИ
- Требования по обеспечению безопасности значимых КИИ
- Требования по обеспечению безопасности объектов связи и сетей (КИИ)

# Что может измениться ко второму чтению?

# Что может измениться ко второму чтению?

С учетом целей принятия проекта, по нашему мнению, нуждается в уточнении предложенный механизм категорирования объектов критической информационной инфраструктуры (статья 6 проекта). На наш взгляд, присвоение указанным объектам соответствующей категории значимости должно осуществляться соответствующим федеральным органом исполнительной власти на основании информации, представленной субъектом критической информационной инфраструктуры, с одновременным внесением сведений о таком объекте в реестр значимых объектов критической информац
целесообразным предусмотреть для субъе
инфраструктуры сроки выполнения ими соотв
для присвоения принадлежащим им объектам

Законопроектом предлагается установить (часть 3 статьи 6 законопроекта), что категорирование объектов критической информационной инфраструктуры Российской Федерации осуществляется самостоятельно субъектами критической информационной инфраструктуры. Такой подход с точки зрения интересов государственного регулирования в сфере информационной безопасности нуждается в содержательном пересмотре в пользу позиции о необходимости осуществления категорирования объектов критической информационной инфраструктуры не самостоятельно собственниками и пользователями имущества, относящегося к объектам критической информационной инфраструктуры, не по результатам плановых и внеплановых проверок в рамках государственного надзора (контроля), а непосредственно силами и средствами федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры.

# Что может измениться ко второму чтению?

Кроме того, законопроектом предусматривается, что федеральный закон вступает в силу с 1 января 2017 года (за исключением статей 6 – 8, 13 и 14). В этой связи требуется внести изменения, устанавливающие иной срок вступления федерального закона в силу.

# Что может измениться ко второму чтению?

Принимая во внимание стратегическое значение энергетической отрасли для экономики, обороноспособности, энергообеспечения и безопасности Российской Федерации, Комитет предлагает дополнительно рассмотреть возможность регламентации особого статуса объектов ТЭК, внеся ко второму чтению проекта федерального закона № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации» корреспондирующие ему изменения в Федеральный закон от 21.07.2011 г. № 256-ФЗ «О безопасности топливно-энергетического комплекса России».

# Что может измениться ко второму чтению?

КУРИННЫЙ А. В. Дмитрий Владиславович, у меня конкретный вопрос. То, что отражено в законопроекте, - это в основном борьба программными методами, то есть речь идёт о вредоносных программах, хакерских атаках и противодействии этому с помощью той программы, на которую сегодня выделены деньги из федерального бюджета. А вот что касается инфраструктуры, электронной в том числе, в которой, к сожалению, доля наших, отечественных продуктов или, так скажем, отечественных объектов достаточно низка, - ведь в объектах электронной инфраструктуры есть специальные чипы, которые передают информацию, более того, такие чипы сейчас есть в некоторых промышленных изделиях, в современных станках, которые установлены на наших военных предприятиях и по команде извне могут быть отключены, например не в рамках каких-то хакерских атак, а в рамках некоего государственного давления. Что в законопроекте есть по этому поводу?

ШАЛЬКОВ Д. В. Спасибо, Алексей Владимирович, за вопрос. Всё это нами учтено, и в рамках реализации данного закона будет использоваться только отечественное оборудование.

КОЛОМЕЙЦЕВ Н. В., фракция КПРФ.

Уважаемый Дмитрий Владиславович, я не знаю, каким образом вы это сделаете. Вот есть у меня официальная справка: из всего нашего рынка радиоэлектронной аппаратуры только 36 процентов составляет отечественная, половина устройств обеспечения безопасности импортируется из-за рубежа. Каким образом будут контролироваться эти агрегаты?

ШАЛЬКОВ Д. В. Спасибо за вопрос. Ещё раз повторяю, все средства, которые будут использоваться при реализации данного закона, будут отечественного производства.

# Что может измениться ко второму чтению?

Подпунктом 4 пункта 3 статьи 7 законопроекта установлена обязанность обеспечения беспрепятственного доступа субъектом критической информационной инфраструктуры (при признании объекта электроэнергетики значимым объектом критической информационной инфраструктуры) должностных лиц федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры. Комитет обращает внимание, что техника безопасности при работе с электрооборудованием предусматривает приобретение компетенции в вопросах электробезопасности, которая закрепляется присвоением персоналу соответствующей группы допуска для обслуживания электроустановок. Для определенной группы устанавливается предельное напряжение и другие параметры доступа к электроустановкам. Персоналу, не имеющему соответствующей группы допуска по электробезопасности, категорически запрещен доступ к электроустановкам.

# Благодарю за внимание!

**Николай Домуховский**

**ООО «УЦСБ»**
**620100, Екатеринбург, ул. Ткачей, д.6**
**Тел.: +7 (343) 379-98-34**
**Факс: +7 (343) 382-05-63**
**info@ussc.ru**
**www.USSC.ru**