Информзащита
Системный интегратор

Обзор законопроекта «О безопасности критической информационной инфраструктуры РФ»

Центр промышленной безопасности
Главный инженер проектов
Кравченко Глеб

Проект Федерального закона «О безопасности Критической Информационной Инфраструктуры Российской Федерации»

- Законопроектом устанавливаются основные принципы обеспечения безопасности критической информационной инфраструктуры, полномочия государственных органов Российской Федерации, а также права, обязанности и ответственность лиц, владеющих объектами критической информационной инфраструктуры, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов.
- 27 января 2017 года законопроект принят в первом чтении

Информзащита
Системный интегратор

Понятие Объект КИИ

Объект КИИ - информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированые системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной промышленности, атомной промышленности, ракетно-космической промышленности и химической промышленности.

Согласно законопроекту, на значимых объектах критической информационной инфраструктуры и в сетях электросвязи должны быть установлены технические средства государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Информзащита
Системный интегратор

Отрасли, которые могут иметь объекты КИИ

- Атомная промышленность
- Оборонная промышленность
- Химическая промышленность
- Топливная промышленность
- Ракетно-космическая промышленность
- Металлургия
- Энергетика
- Горнодобывающая промышленность
- Госорганы
- Кредитно-финансовая сфера
- Здравоохранение
- Транспорт
- Связь

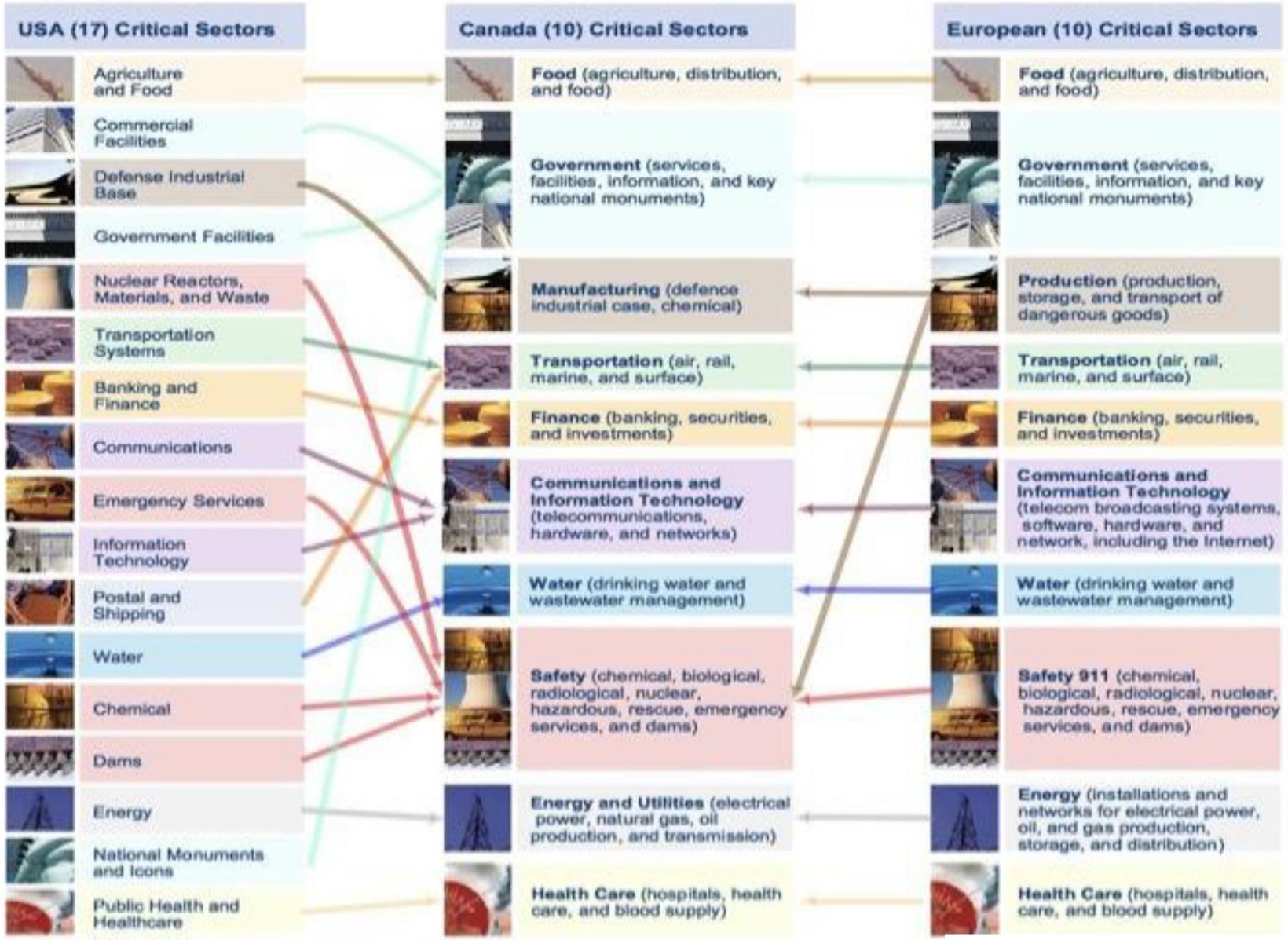
Информзащита
Системный интегратор

Отрасли, исключенные из законопроекта

- Водоснабжение
- Гидротехнические сооружения
- Правоохранительные структуры
- Географические и навигационные системы
- Телерадиовещание
- Системы спецназначения

Информзащита
Системный интегратор

Отраслей, содержащие объекты КИИ, согласно зарубежным нормативно-правым актам



Информзащита
Системный интегратор

Категорирование объектов КИИ

Критерии значимости объекта КИИ:

- ***социальная значимость***, выражающаяся в том числе в оценке ущерба здоровью людей, возможности прекращения (нарушения) функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимального времени недоступности государственной услуги для определенного количества получателей такой услуги;
- ***политическая значимость***, выражающаяся в оценке ущерба интересам Российской Федерации во внутриполитической и внешнеполитической сферах;
- ***экономическая значимость***, выражающаяся в оценке снижения экономических показателей, прямых и косвенных финансовых потерь Российской Федерации;
- ***экологическая значимость***, выражающаяся в оценке вреда, причиняемого окружающей среде;
- ***значимость для обеспечения обороноспособности, безопасности государства и правопорядка.***

- объекты КИИ необходимо категорировать
- эту работу субъект КИИ проводит либо сам, либо привлекает лицензиата ФСТЭК по ТЗКИ.
- результаты вносит в реестр ФО1

Информзащита
Системный интегратор

Регуляторы

Задачи ФО1 (ФСТЭК):

- проверяет правильность категорирования
- устанавливает требования к безопасности по каждой категории за исключением объектов связи.

ФО2 (ФСБ)

- координирует деятельность субъектов КИИ
- организует и проводит проверку защищенности КИИ
- утверждает порядок реагирования на инциденты
- утверждает порядок обмена информацией
- устанавливает требования к техническим средствам

- проверки - плановые - раз в три года
- проверки – внеплановые – при нарушениях

Информзащита
Системный интегратор

Реестр КИИ

Закон предполагает создание реестра критической информационной инфраструктуры, куда будут вноситься сведения о программном обеспечении объекта, мерах и средствах, применяемых для обеспечения его безопасности.

Субъекты этого реестра, должны, помимо прочего, обеспечивать «беспрепятственный доступ должностных лиц федерального органа исполнительной власти (...) к значимому объекту критической информационной инфраструктуры».

Функциональные требования к Системе безопасности

- Предотвращение неправомерного доступа, уничтожения, модифицирования и т.п информации
- Недопущение воздействия, которое может привести к нарушению или прекращению функционирования объекта КИИ
- Обнаружение и предупреждение компьютерных атак
- Восстановление работоспособности
- Сбор, анализ и хранение сведений о проведенных компьютерных атаках
- Непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Информзащита
Системный интегратор

Ответственность

За создание программ для атак на объекты информационной инфраструктуры – штраф от пятисот тысяч до миллиона рублей либо принудительные работы или лишение свободы на срок до пяти лет;

За неправомерный доступ к охраняемой информации (с причинением вреда инфраструктуре) – штраф от одного до двух миллионов рублей или лишение свободы на срок до шести лет со штрафом от пятисот тысяч до одного миллиона рублей.

За нарушение правил эксплуатации технических средств критических систем – принудительные работы на срок до пяти лет с лишением права занимать определенные должности на срок до трех лет, либо лишение свободы на срок до шести лет.

Если совершение всех правонарушений повлекло тяжелые последствия или «создало угрозу их наступления» – оно наказывается лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности на срок до пяти лет.

Информзащита
Системный интегратор

Спасибо за внимание!

Центр промышленной безопасности
Главный инженер проектов
Кравченко Глеб