ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 26.07.2017 № 187-ФЗ «О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ». РИСКИ И ПРОБЛЕМАТИКА

А. А. Гришанков, Л. Ю. Застылова

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров

Общие положения

Государственной Думой 12 июля 2017 года был принят, а Советом Федерации 19 июля 2017 года одобрен Федеральный Закон №187 «О безопасности критической информационной инфраструктуры Российской федерации».

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Данный Федеральный закон был проанализирован, для определения рисков обеспечения электроэнергией предприятия 1 категории значимости (ФГУП «РФЯЦ-ВНИИЭФ»), выявление существующих проблем в реализации требований закона и разработка базовых предложений для РФЯЦ-ВНИИЭФ.

Отрасли

Отрасли, которые могут иметь объекты критической информационной инфраструктуры следующие:

1. Атомная промышленность
2. Оборонная промышленность
3. Химическая промышленность
4. Топливная промышленность
5. Энергетика
6. Металлургия
7. Здравоохранение
8. Транспорт и т.д.

В каждой из этих отраслей присутствуют автоматизированные процессы, влияние на которые из вне может привести к экономическим и информационным потерям, причинение вреда жизни и здоровью населения, ухудшению экологической обстановке.

Значимый объект критической информационной инфраструктуры - объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры.

Категорирование

Категорирование осуществляется исходя из:

1) социальной значимости, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги;

2) политической значимости, выражающейся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;

3) экономической значимости, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации;

4) экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду;

5) значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка.

Устанавливаются три категории значимости объектов критической информационной инфраструктуры – первая, вторая и третья.

Ответственность

Данный Федеральный закон предусматривает ответственность за неправомерные действия надо объектами критической информационной инфраструктуры:

1) *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;

2) *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.

3) *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.

Задачи

Задачами государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности являются:

1) Укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;

2) Совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);

3) Совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

4) Повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

Кибератаки на объекты критичной информационной инфраструктуры

Закон о критической инфраструктуре – один из этапов, необходимых для создания защиты этой самой инфраструктуры. Интересно посмотреть разбивку кибератак на объекты критичной информационной инфраструктуры по их отраслевой направленности. На графике ниже видно, что основной целью являются предприятия топливно-энергетического комплекса.

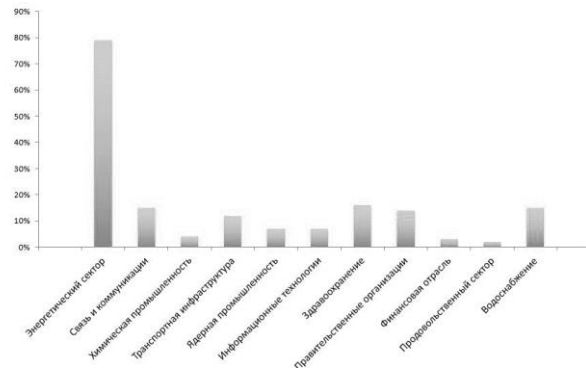

Рис. 1. График кибератак на объекты критической инфраструктуры

За последние несколько лет были зарегистрированы несколько кибератак на объекты энергетики, в частности на атомных электростанциях (АЭС).

1) 2016 – на АЭС «Гундреминген» в Германии. Заражение не представляло угрозы безопасности атомной электростанции, поскольку управляющие системами АЭС компьютеры не подключены к интернету. Использованы вирусы W32.Ramnit и Conficker.

2) 2016 – на 3 областных энергетический компании Украины, подача энергии была прервана на несколько часов. Использован вирус BlackEnergy.

3) 2010 – на строящуюся АЭС «Бушер» в Иране. Кибератака отбросила ядерную программу страны на два года. Использован вирус Stuxnet.

4) 2003 – на АЭС в штате Огайо, США. На восстановление работоспособности систем ушло 6 часов. Использован вирус Slammer.

Уязвимые места

В ходе анализа энергетической отрасли были выделены следующие уязвимые места и предложены решения.

1) Несанкционированные воздействия на оборудование, отдающее команды и нарушение связи между подстанциями.

2) Терминалы релейной защиты и автоматики (РЗА), контроллеры присоединения, измерительные преобразователи, серверы SCADA, автоматизированные рабочие места (АРМы).

3) Современные автоматизированные системы управления технологическими процессами (АСУ ТП) предприятия объединены в промышленные сети и в большинстве своем связаны с офисными сетями, а в некоторых случаях и с интернетом.

4) Отсутствие ответственных за обеспечение информационной безопасности (ИБ) АСУ ТП.

Решения

1) Анализаторы сетевого трафика, подключенные черед дата-диод.

2) Комплексные решения по защите компонентов АСУ ТП, в том числе на базе продуктов ведущих российских разработчиков средств защиты.

3) Однонаправленные шлюзы.

4) Необходимо проведение аудиторских обследований систем информационной безопасности предприятий, генерирующих и транспортирующих электроэнергию.

5) Договор на поставку электроэнергии должен предусматривать для предприятий 1 категории особые условия по аварийно-техническому бронированию неотключаемых линий.

6) Организация доступа к оборудованию инженерной инфраструктуры, обеспечивающую безотказную работу центров автоматизации и информатизации, требует регламентирования на отраслевом уровне.

7) Проектирование и реализация автоматизирования и информатизации АО «Саровская генерирующая компания» и АО «Саровская электросетевая компания» должны обеспечивать требования Федерального закона.

Так же в качестве защиты на определенном этапе можно предложить версию антивируса Касперского разработанного специально для автоматизированных систем управления. Антивирус обеспечивает:

1) пассивный анализ трафика;

2) контроль целостности сети;

3) контроль целостности индустриального процесса;

4) контроль запуска приложений;

5) контроль подключения внешних устройств;

6) контроль целостности проектов ПЛК.

Список литературы

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ».