Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина
ФАКУЛЬТЕТ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ТЭК

ПРАВОВЫЕ АСПЕКТЫ СЕРТИФИКАЦИИ SCADA ТЕХНОЛОГИЙ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Жарова Анна Константиновна,
д.ю.н., доцент,
заведующий кафедрой правового обеспечения безопасности ТЭК, РГУ нефти и газа (Национальный исследовательский университет) им. И.М. Губкина

anna_jarova@mail.ru

SCADA

- SCADA - информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств; (ст. 2 ФЗ Об информации)

- SCADA - автоматизированная система управления - 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 (ст. 2 ФЗ О КИИ)

Система нормативного правового регулирования в области обеспечения информационной безопасности АСУ ТП

1. Информационная безопасность SCADA

- Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании. *(ч. 8. ст.14 ФЗ об информации)*

Действие закона не распространяется на «…. стандарты распространения, предоставления или раскрытия информации...»

Закон не регулирует отношения, «связанные с разработкой, принятием, применением и исполнением … **требований к безопасному использованию атомной энергии, в том числе требований безопасности объектов использования атомной энергии, требований безопасности деятельности в области использования атомной энергии, требований к осуществлению деятельности в области промышленной безопасности, безопасности технологических процессов на опасных производственных объектах, требований к обеспечению надежности и безопасности электроэнергетических систем и объектов электроэнергетики, требований к обеспечению безопасности космической деятельности….»**

(Федеральный закон от 27.12.2002 N 184-ФЗ (ред. от 22.12.2020) "О техническом регулировании« (с изм. и доп., вступ. в силу с 01.01.2021))

=>Возможность внедрения закладок в АСУ ТП (SCADA) иностранного производства

2. ЕСЛИ ВВЕСТИ ОБЯЗАТЕЛЬНУЮ СЕРТИФИКАЦИЮ

ФЗ О Техническом регулировании – **Обязательной сертификации подлежит продукция только определенная для этих целей. (ст. 25)**

Однако, из перечня обязательной сертификации выведены:

- Комплексы и машины вычислительные электромеханические и механические Исключен. - Постановление Правительства РФ от 20.10.2010 N 8484020
- Устройства центральные вычислительных сетей, систем, комплексов и машин электронных цифровых Исключен. - Постановление Правительства РФ от 04.03.2013 N 1824030
- Устройства периферийные вычислительных комплексов и машин электронных цифровых Исключен. - Постановление Правительства РФ от 04.03.2013 N 1824040
- Устройства межсистемной связи сетей, систем, комплексов и машин вычислительных электронных Исключен. - Постановление Правительства РФ от 04.03.2013 N 182

3. Контроль и надзор в области АСУ ТП (ФЗ об информации)

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, **обязаны обеспечить**:

- 1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- 2) своевременное обнаружение фактов несанкционированного доступа к информации;
- 3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- 4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- 5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- 6) постоянный контроль за обеспечением уровня защищенности информации;
- 7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

(ч.4. ст. 16. Защита информации)

3. Контроль и надзор в области АСУ ТП (ФЗ об информации)

- Статья 10.4. Особенности распространения информации новостным агрегатором
- Статья 10.5. Обязанности владельца аудиовизуального сервиса
- Статья 10.6. Особенности распространения информации в социальных сетях
- Статья 14.1. Применение информационных технологий в целях идентификации физических лиц
- Статья 14.2. Обеспечение устойчивого и безопасного использования на территории Российской Федерации доменных имен
- Статья 15.1. Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено
- => *ГДЕ КОНТРОЛЬ И НАДЗОР ЗА АСУ ТП ?*

ФЗ Об информации

- **Статья 14.1. Применение информационных технологий в целях идентификации физических лиц**
- *Ч. 10. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных…*
- *Ч.10.1. Контроль и надзор за обработкой персональных данных в единой биометрической системе, а также в информационных системах государственных органов…*
- *Ч.11. Контроль и надзор за выполнением организациями финансового рынка организационных и технических мер по обеспечению безопасности биометрических персональных данных осуществляются Центральным банком Российской Федерации.*

4. Федеральный закон N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

- Определены виды нарушений
- Определена ответственность за нарушение требований закона и принятых в соответствии с ним иных нормативных правовых актов (ст.14)

ОДНАКО

Ответственность за несоблюдение требований, создающее предпосылки к нанесению ущерба критической информационной инфраструктуре в случае совершения компьютерной атаки, но не повлекшее причинение вреда критической информационной инфраструктуре, не установлена.

4.

- КоАП РФ не предусматривает составов правонарушений в отношении субъектов КИИ.
- УК РФ устанавливает, в частности, наказание за несоблюдение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ. Уголовная ответственность наступает, только если нарушение причинило вред КИИ.

4. Гражданско-правовая ответственность

- Гражданско-правовая ответственность - это меры, которые применяются к лицу, нарушившему нормы гражданского законодательства или требование договора.

Например, поставка ПО не соответствующего качества или содержащее закладку и тд.

В настоящее время:

Обязанность лицензиара возмещать вред в полном объеме (ст. 15 ГК РФ) возникает только в том случае, если будет установлено, что этот вред причинен по его вине.

(ст.15 Лицо, право которого нарушено, может требовать полного возмещения причиненных ему убытков, если законом или договором не предусмотрено возмещение убытков в меньшем размере.

2. Под убытками понимаются расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение его имущества (реальный ущерб), а также неполученные доходы, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода).

Если лицо, нарушившее право, получило вследствие этого доходы, лицо, право которого нарушено, вправе требовать возмещения наряду с другими убытками упущенной выгоды в размере не меньшем, чем такие доходы.)

4.

При отсутствии обязательных стандартов регулирование использования программного обеспечения возможно только путем заключения гражданско-правового договора, в котором будут зафиксированы:

все существенные условия использования программного обеспечения, его функциональность и ответственность разработчика (лицензиара).

- Сегодня практика такова, что правообладателю и разработчику программного обеспечения не может быть поставлено в вину возникновение в нем ошибки.
- Представляется, что в лицензионный договор об использовании программного обеспечения, которое предусмотрено для устройства в объекте КИИ, должно быть включено существенное условие об ответственности разработчика и о возмещении им вреда.

- Иностранный поставщик часто требует наличия удаленного дистанционного доступа и управления «своими» средствами.

- 5. С 1 января 2020 г. программное обеспечение должно быть зарегистрировано в едином реестре российских программ для электронных вычислительных машин и баз данных или едином реестре программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации.
- Программное обеспечение должно исключать несанкционированный удаленный доступ к системам автоматического управления и несанкционированное дистанционное вмешательство в функционирование турбин.

(Постановление Правительства РФ от 17.07.2015 N 719 (ред. от 19.01.2021) "О подтверждении производства промышленной продукции на территории Российской Федерации" (начало действия редакции - 21.01.2021 (за исключением отдельных положений) // СЗ РФ 2015, N 30, ст. 4597).

5. Устанавливаются требования к обеспечению защиты информации, обработка которой осуществляется автоматизированными системами управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (далее - автоматизированные системы управления), от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации, в том числе от деструктивных информационных воздействий (компьютерных атак), следствием которых может стать нарушение функционирования автоматизированной системы управления.

- **«Настоящие Требования применяются в случае принятия владельцем автоматизированной системы управления решения об обеспечении защиты информации, обработка которой осуществляется этой системой и нарушение безопасности которой может привести к нарушению функционирования автоматизированной системы управления».**

(ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ ПРИКАЗ от 14 марта 2014 г. N 31 ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХСИСТЕМАХ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ И ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ НА КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТАХ, ПОТЕНЦИАЛЬНО ОПАСНЫХ ОБЪЕКТАХ, А ТАКЖЕ ОБЪЕКТАХ, ПРЕДСТАВЛЯЮЩИХ ПОВЫШЕННУЮ ОПАСНОСТЬ ДЛЯ ЖИЗНИ И ЗДОРОВЬЯ ЛЮДЕЙ И ДЛЯ ОКРУЖАЮЩЕЙ ПРИРОДНОЙ СРЕДЫ)

6. Принцип технологической нейтральности

- «недопустимо установление нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами».

(ст.3 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ 2006. № 31 (1 ч.), Ст. 3448.)

ФЗ о КИИ

Принципами обеспечения безопасности критической информационной инфраструктуры являются:

- 1) законность;
- 2) непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры;
- 3) приоритет предотвращения компьютерных атак.

(Ст. 4. Принципы обеспечения безопасности критической информационной инфраструктуры)

? обязательность применения определенных информационных технологий

Принцип технологической нейтральности

- В условиях обеспечения информационной безопасности Российской Федерации приоритет принципа технологической нейтральности **для национальных технологий** должен быть закреплен на уровне федеральных законов.
- Необходимо поставить вопрос о распространении данного принципа для области отношений, связанной с созданием и использованием российских информационных технологий внутри страны.
- Речь должна идти не об обеспечении равных условий для использования всех информационных технологий на территории Российской Федерации, а о приоритете использования российских информационных технологий.
- Принцип технологической нейтральности должен распространиться на российские информационные технологии, поскольку нейтральность по отношению к зарубежным информационным технологиям может привести к нарушению информационного, цифрового суверенитета Российской Федерации.

ВЫВОД

- Анализ норм федеральных конституционных законов, федеральных законов и подзаконных актов Российской Федерации свидетельствует о том, **необходимо разрабатывать** систему взаимодействующих норм, определяющих порядок разработки компьютерных технологий, осуществляющих сбор, распространение и использование информации в АСУ ТП.
- В настоящий период развития информационной сферы государства в первую очередь должны поддерживать свои информационные интересы и безопасность.
- ИКТ являются основным фактором, определяющим уровень социально-экономического развития и состояние национальной безопасности. Обеспечение информационной безопасности должно определяться системой организационно-правовых средств, связанной с использованием информационных технологий.

Спасибо за внимание

Жарова Анна Константиновна,
Д.ю.н., доцент,
Заведующий кафедрой правового обеспечения безопасности ТЭК, РГУ нефти и газа (Национальный исследовательский университет) им. И.М. Губкина

anna_jarova@mail.ru