Химия, КИИ и ФСТЭК

К 2020 году химические предприятия обязаны сертифицировать свои программно-аппаратные комплексы

Андрей Помешкин, директор ООО «Системы информационной безопасности»

29 июля 2018 года принята новая редакция Федерального закона от 21.07.1997 N 116-ФЗ «О промышленной безопасности опасных производственных объектов», которая уточнила классификацию опасных производственных объектов и отнесла химпредприятия к субъектам критической информационной инфраструктуры (КИИ). Что вводит обязанность для всех химических заводов Российской Федерации в соответствии со вновь установленными нормами использовать только сертифицированные программно-аппаратные комплексы.

Федеральный закон о безопасности критической информационной инфраструктуры № 187 принят 26 июля 2017 года. В новой редакции статьей 2.3 к субъектам критической информационной инфраструктуры отнесены предприятия химической промышленности.

В соответствии со статьей 9.3 «Права и обязанности субъектов КИИ» — предприятия обязаны соблюдать требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленные ФСТЭК РФ — федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Химические предприятия относятся к субъектам критической информационной инфраструктуры и должны выполнять нормативные предписания ФСТЭК.

Со своей стороны, ФСТЭК выпустил ряд приказов.

Приказ ФСТЭК РФ от 14 марта 2014 г. № 31 утвердил требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

В нем записано, что «Обеспечение безопасности автоматизированных систем управления, являющихся значимыми объектами критической информационной инфраструктуры Российской Федерации, осуществляется в соответствии с Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом Федеральной службы по

техническому и экспортному контролю от 25 декабря 2017 г. N 239, а также Требованиями к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденными приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. N 235 (зарегистрирован Минюстом России 22 февраля 2018 г., регистрационный N 50118).»

Приказ ФСТЭК РФ от 25 декабря 2017 г. № 239 в п.28 предписывает: в случае признания субъектом КИИ необходимо применять средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации.

Итак, химические предприятия относятся к субъектам критической информационной структуры и поэтому должны выполнять нормативные документы ФСТЭК, которые обязывают применять средства защиты информации, в том числе СУБД, программы «сервер — клиент — сервер» и аппаратные комплексы, прошедшие обязательную сертификацию.

Текущее положение

Уровень зависимости процессов современного предприятия от бесперебойной работы его информационных систем сегодня как никогда высок.

Эпидемия вируса WannaCry, затронувшего более 500 тысяч компьютеров и парализовавшего работу сотен организаций по всему миру, атака на иранские ядерные объекты с использованием вредоносного ПО Stuxnet, атака на украинские электростанции (BlackEnergy) — показали это особенно ярко.

Паралич информационных систем социально значимого предприятия может оставить город/регион без воды, газа и электроэнергии, а остановка таких систем на химическом предприятии чревата серьезными экологическими последствиями.

Теперь, если объект КИИ не был защищен должным образом и ему был нанесен вред, должностные лица могут понести ответственность в соответствии с Уголовным кодексом.

Текущая ситуация с КИИ в целом по стране (по материалам Доклада заместителя руководителя ФСТЭК России С.В.Лютикова на «Инфофоруме» в феврале 2019 года) характеризуется следующим образом.

- Нормативная база по КИИ в целом сформирована.
- Субъекты КИИ стремятся занизить категорию значимости своих объектов, пользуются всевозможными юридическими лазейками.
- 1800 субъектов КИИ подали Перечни объектов и приступили к категорированию.
- Сейчас в Перечне ФСТЭК находится 27 000 объектов КИИ.
- 700 субъектов КИИ завершили категорирование.
- По оценке ФСТЭК, озвученные выше цифры — 15% от прогнозируемого итогового количества. В целом по стране ожидается 12 000 субъектов КИИ и 180 000 объектов КИИ.
- ФСТЭК видит проблему в несовершенстве методологии определения субъектов и объектов КИИ.
- Лидеры по категорированию — здравоохранение, ТЭК, ВПК, металлургия.
- Аутсайдеры категорирования — операторы связи (перечни подали только 40 операторов).

В целом по стране ожидается появление 12 000 субъектов КИИ (предприятий) и 180 000 объектов КИИ (программ и систем).

Объекты КИИ

24 августа 2018 года ФСТЭК выпустила информационное сообщение N 240/25/3752, в котором ответила на вопрос — что на предприятии является объектом КИИ, подлежащим категорированию.

Вот полный перечень объектов: информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть. Все три объекта представлены на химическом предприятии.

До 1 января 2019 года каждое предприятие, имеющее класс опасности, должно было направить во ФСТЭК сведения о результатах присвоения названным объектам КИИ одной из категорий значимости или же указать, что в присвоении категории значимости данный объект не нуждается.

В связи с несоблюдением означенных сроков значимой частью субъектов КИИ срок категорирования был продлен до 1 сентября 2019 года.

Категорирование

Для выполнения требований законодательства организациям — субъектам КИИ необходимо сделать следующие шаги (кратко на схеме 1).

1. Руководитель организации — субъекта КИИ — создает комиссию по категорированию, в обязанности которой входит выявление критических процессов субъекта (управленческих, технологических, производственных и т.д.).

2. Комиссией определяются объекты КИИ — информационные системы, сети и автоматизированные системы, которые связаны с этими процессами.

3. Перечень объектов КИИ владелец (субъект КИИ) согласовывает с регулятором в установленной сфере (Минэнерго для НПЗ и ТЭК, Минпромторг для и химической промышленности, Министерство связи и массовых коммуникаций для телеком-операторов и т.д. по направлениям) и затем отправляет во ФСТЭК России.

4. В течение года с момента согласования субъект КИИ осуществляет категорирование объектов КИИ.
   - При выборе категории объект оценивается по уровню влияния на показатели значимости. Итоговая оценка ставится по максимальному значению среди критериев.
   - Объекту могут быть присвоены три категории значимости. Либо комиссия признает, что объект КИИ не является значимым.

5. Результаты категорирования фиксируются в акте, который утверждает руководитель субъекта КИИ, далее согласовываются с отраслевым регулятором (если он установлен) и направляются в ФСТЭК России.

6. Субъект КИИ должен создать систему безопасности значимых объектов КИИ. В нее входят:
   - Люди (руководитель субъекта КИИ, уполномоченное лицо по контролю функционирования системы, сотрудники профильных структурных подразделений, сотрудники подразделений, ответственных за обеспечение безопасности).
   - Средства защиты информации.
   - Организационная документация (общесистемные документы, правила безопасной работы сотрудников и регламенты действий при нештатных ситуациях).
   - Документы планирования (порядок приемки и проведения испытаний, порядок взаимодействия подразделений и т.д.).

7. Для каждого значимого объекта КИИ должны быть реализованы меры по обеспечению безопасности.

На каждом предприятии химического комплекса представлены три объекта критической информационной инфраструктуры (КИИ): информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть.

Аттестация

В ходе выполнения проекта инвентаризации объектов КИИ лицензированная компания производит следующие работы:

- Обследование потенциальных объектов КИИ заказчика.
- Идентификация процессов (управленческих, технологических, производственных, финансово-экономических и т.д.), выявление критических процессов, определение объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, оценка возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры Заказчика, описание идентифицированных объектов КИИ, включая их взаимодействие с другими объектами КИИ и сетями электросвязи, подготовка предложений и обоснований по категорированию объектов КИИ нфраструктуры организации с учетом положений федерального закона № 187 и «Правил категорирования объектов критической информационной инфраструктуры Российской Федерации», утвержденных постановлением Правительства РФ № 127 от 08.02.2018.

Проверку объектов КИИ ФСТЭК проводит 1 раз в 3 года. Пересмотр категории объекта осуществляется 1 раз в 5 лет.

В результате проведенной аттестации Заказчику передаются следующие документы.

- Отчет по результатам идентификации объектов критической информационной инфраструктуры организации-заказчика.
- Отчет «Перечень объектов критической информационной инфраструктуры» организации-заказчика.

Реестр объектов КИИ

Реестр значимых объектов формируется и ведётся ФСТЭК России на основании данных, предоставляемых субъектами КИИ.

Реестр подлежит защите в соответствии законодательством РФ о гостайне на основании приказа ФСТЭК № 227 от 6.12.2017 г.

Данные об изменении категории также должны направляться во ФСТЭК.

Изменение категории значимости может произойти:

- По мотивированному решению ФСТЭК по результатам проверки, выполненной в рамках осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ.
- Объект перестал соответствовать критериям значимости и показателям их значений.
- Субъект КИИ был реорганизован, ликвидирован или произошли изменения в его организационно-правовой форме.

Проверки

После внесения в реестр объектов КИИ или после последней проверки ФСТЭК России 1 раз в 3 года проводит новую проверку объектов КИИ на соответствие требованиям законодательства.

Кроме того, субъект КИИ могут ожидать и внеплановые проверки по следующим основаниям:

- Истечение срока действия предписания об устранении нарушений требований безопасности.
- Инцидент на объекте КИИ.
- Поручение президента, правительства или прокуратуры.

По результатам проверки возможны санкции в соответствии с действующим законодательством.

Не реже 1 раза в 5 лет осуществляется пересмотр установленной категории объекта КИИ. Также пересмотр осуществляется при следующих ситуациях:

- Реорганизация субъекта КИИ.
- Изменение влияния объекта на показатели значимости.
- По результатам проверки ФСТЭК России.

Уровень задач и квалификация

Высокий уровень значимости защищаемых систем и различия в построении платформ требуют наличия в компании, осуществляющей сертификацию, специалистов различной квалификации с высоким уровнем подготовки.

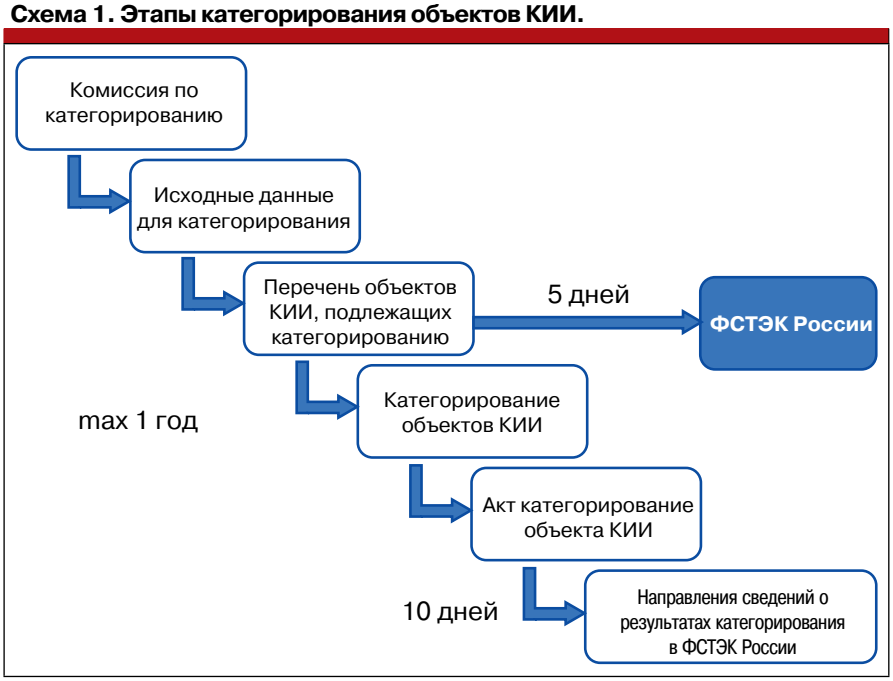
Как правило, для выполнения требований по защите КИИ приходится осуществлять модернизацию существующих на предприятиях систем.
В реализации проекта принимают участие специалисты по информационной безопасности сертифицирующей компании-подрядчика и работники подразделений, эксплуатирующих объекты КИИ.

Важно понимать, что при реализации проекта нужно учитывать требования нескольких регуляторов в области информационной безопасности — ФСТЭК, ФСБ, отраслевых (ЦБ для банковского сектора, Минкомсвязи России для телеком-операторов, Минпромторга для химических предприятий, Минэнерго для предприятий ТЭК).

В ходе работ организуется постоянный мониторинг безопасности со своевременным извещением Национального координационного центра по компьютерным инцидентам (НКЦКИ) в случае обнаружения инцидентов.

Комплексная система защиты должна покрывать все элементы ИТ-инфраструктуры, обеспечивать высокий уровень надежности, а также иметь удобные механизмы управления и мониторинга, для чего введены критерии, общепризнанные в мире и известные специалистам IT.

Схема 1. Этапы категорирования объектов КИИ.



«Системы информационной безопасности»

Компания «Системы информационной безопасности» — команда с опытом работы и исследований в области информационной безопасности более 15 лет. Компания разрабатывает комплексные решения, совершенствует и сопровождает применяемые решения, постоянно повышает квалификацию участников команды со своей стороны и со стороны заказчика.

ООО «СИБ» обеспечивает выполнение следующих работ.

- Аудит защищенности информационных систем, безопасности web-приложений.
- Проектирование, внедрение и сопровождение защищенных информационных систем.
- Безопасность систем управления производством.
- Аттестация соответствия информационных систем требованиям информационной безопасности.
- Подготовка организационно-распорядительной документации.
- Создание корпоративных центров корреляции событий безопасности и прогнозирования инцидентов.
- Создание системы информационного обмена с Национальным координационным центром по компьютерным инцидентам (НКЦКИ).

В настоящее время компания акцентирует внимание на системе глобального ситуационного мониторинга, благодаря которому решаются задачи по комплексному контролю всей значимой инфраструктуры, детекции событий, приводящих к возникновению инцидентов и инициации протоколов действий, позволяющих минимизировать ущерб при наступлении инцидентов.

Срок категоризации промышленных объектов продлен до 1 сентября 2019 года, аттестация должна быть завершена в 2020 году.

Компания «СИБ» реализует проекты во всех федеральных округах РФ, в четырех округах и двух странах СНГ открыты представительства компании.

За последние годы в ООО «СИБ» обучено более 1500 специалистов в области информационной безопасности; проведены пентесты систем (penetration test) крупных государственных заказчиков; спроектировано и внедрено более 200 информационных систем в защищенном исполнении для государственных и коммерческих структур; в соответствии с новыми требованиями законодательства выполнены работы по безопасности систем управления производством на 10 промышленных предприятиях. ■

Средства защиты информации

Программно-аппаратные решения, которые позволяют защитить значимую информацию на предприятии и должны присутствовать на объекте КИИ, должны отвечать понятным требованиям.

Так, основные ресурсы должны быть внутренними (находиться под полным контролем корпорации) – свой почтовый сервер, свои файловые сервера и сервера приложений.

Все действия на них протоколируются, все почтовые сообщения сканируются антивирусом, несканируемые сообщения (зашифрованное сообщение или сообщение с защищенным вложением) отправляются в карантин, уведомление о таком сообщении отправляется адресату и администратору сети.

Создаются сквозные резервные копии для данных всех типов, и это предоставляет возможность не только восстанавливать систему при сбоях, но и проводить расследования в случае утечек, либо использования в личных целях.

Доступ к внешним ресурсам осуществляется через корпоративный прокси-сервер, где также выполняется сканирование на вредоносные и несанкционированные вложения, а все действия записываются в протокол.

Доступ через прокси-сервер возможен только с аутентификацией, анонимного доступа ни к каким ресурсам нет вообще.

Наличие данных решений прописывается в политиках безопасности компании.