АСУ ТП как объект КИИ

Виктор СЕРДЮК,
генеральный директор АО «ДиалогНаука»

Летом прошлого года был принят Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», основные положения которого вступили в силу с 1 января 2018 г. Одной из характерных особенностей закона является наличие требования подключения к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА). Эта система предназначена, в частности, для обеспечения защиты критической информационной инфраструктуры РФ (КИИ). Следует отметить, что АСУ ТП многих предприятий могут попасть в область действия закона и будут рассматриваться как объект КИИ, по отношению к которому необходимо проводить комплекс мероприятий по защите информации. В предлагаемой статье сделан краткий обзор данного закона и подзаконных актов, которые разрабатываются на его основе.

Закон

Федеральный закон № 187-ФЗ «О безопасности КИИ» определяет два федеральных органа исполнительной власти, которые несут ответственность за обеспечение безопасности КИИ. Первый – ФОИВ – уполномоченный в области обеспечения безопасности КИИ, второй – уполномоченный в области обеспечения функционирования ГосСОПКА. Первый отвечает за формирование реестра объектов критической инфраструктуры, формирование требований к ним и обеспечение их безопасности. В роли ФОИВ выступает ФСТЭК России. Вторым ФОИВ является ФСБ, которая обеспечивает функционирование ГосСОПКА по сбору информации об инцидентах и рассылке предупреждений об атаках на объекты КИИ.

Собственно, ГосСОПКА была ранее сформирована в рамках Указа Президента РФ 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», который продолжает действовать как один из подзаконных актов в рамках № 187-ФЗ. Она предполагает наличие центрального узла системы – GovCERT (http://gov-cert.ru/), который в законе упомянут как «национальный координационный центр по компьютерным инцидентам» (НКЦКИ). GovCERT является центром всей распределенной иерархической системы ГосСОПКА, куда могут входить и отраслевые, и территориальные, и даже корпоративные центры реагирования на компьютерные инциденты путем обмена информацией с GovCERT. Теоретически все отрасли и территории, где есть предприятия, отнесенные к объектам КИИ, должны построить собственные центры мониторинга.

Основой для требований к защите объектов КИИ будет выбран приказ № 31 ФСТЭК, который уже успешно применяется для защиты АСУ ТП. В рамках «Росстандарта» ФСТЭК организовала свой технический комитет, поэтому велика вероятность подготовки в среднесрочной перспективе ГОСТов для обеспечения защиты АСУ ТП объектов КИИ.

Следует отметить, что Президент РФ 22 декабря 2017 г. уже подписал Указ № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», где назначил ФСБ в качестве ФОИВ, отвечающего за ГосСОПКА. В Указе определены задачи функционирования ГосСОПКА:

а) прогнозирование ситуации в области обеспечения информационной безопасности РФ;
б) обеспечение взаимодействия владельцев информационных ресурсов РФ, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении

задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности информационных ресурсов РФ от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

Таким образом, ФСБ получает возможность осуществлять контроль защищенности объектов КИИ, в том числе АСУ ТП, если таковые будут признаны КИИ.

Подзаконные акты

На основе Федерального закона № 187-ФЗ в настоящее время разрабатываются подзаконные акты, направленные на определение порядка защиты объектов КИИ. Согласно Указу Президента РФ № 569 от 25 ноября 2017 г. «О внесении изменений в Положение о ФСТЭК» с 1 января 2018 г. ФСТЭК становится ответственным ФОИВ в области обеспечения безопасности КИИ.

Кроме того, 8 февраля 2018 г. было выпущено Постановление Правительства РФ № 127 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений». В тот же день в Минюсте РФ был официально зарегистрирован приказ ФСТЭК России № 227 от 6 декабря 2017 г. «Об утверждении Порядка ведения реестра значимых объектов КИИ РФ».

В рамках этих подзаконных актов должен быть сформирован реестр значимых объектов КИИ, где, собственно, они все и должны быть перечислены. Когда компании, имеющие объекты КИИ в своем подчинении, будут определены, их предстоит категорировать в соответствии с уровнем значимости, который устанавливается исходя из следующих критериев:

1) социальная значимость, которая выражается в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также в максимальном времени отсутствия доступа к государственной услуге для ее получателей;

2) политическая значимость, выражающаяся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;

3) экономическая значимость, выражающаяся в оценке возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации;

4) экологическая значимость, выражающаяся в оценке уровня воздействия на окружающую среду;

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

Всего устанавливаются три категории значимости, самая высокая категория – первая, самая низкая – третья.

Практически во всех случаях есть собственные АСУ ТП, деятельность которых, таким образом, может попасть под действие № 187-ФЗ. Компаниям, которые попадут в реестр значимых объектов КИИ, придется, как минимум, создавать свой центр мониторинга и реагирования на компьютерные инциденты, чтобы иметь возможность сообщать о них в вышестоящий узел ГосСОПКА. Он должен не только собирать информацию об инцидентах, но и в случае получения предупреждения от системы суметь соответствующим образом отреагировать на атаку.

> Основой для требований к защите объектов КИИ будет выбран приказ № 31 ФСТЭК, который уже успешно применяется для защиты АСУ ТП.

Скорее всего, остальные технические требования к мерам по защите информации будут базироваться на видоизмененном приказе № 31 ФСТЭК. Тем не менее, пока уточняющие подзаконные акты не будут приняты, о полноценном введении закона в действие говорить не приходится.

Заключение

Федеральный закон № 187-ФЗ направлен на повышение уровня информационной безопасности объектов КИИ, к числу которых, вероятно, будут отнесены АСУ ТП многих предприятий. Соответствующие подзаконные акты предусматривают проведение комплекса мероприятий, начиная с категорирования объектов КИИ и заканчивая реализацией мер по защите информации, в том числе подключение в ГосСОПКА. С учетом вышесказанного предприятия должны заранее начинать работу в этом направлении, чтобы быть готовыми выполнить требования указанного закона. ■