Круглый стол

Безопасность объектов КИИ:
нормы и правила

В круглом столе принимают участие

Сергей ЗОЛОТУХИН,
эксперт по информационной безопасности, Group-IB

Дмитрий КУЗНЕЦОВ,
директор по методологии и стандартизации, Positive Technologies

Дмитрий МИХЕЕВ,
технический директор, ООО «АйТи БАСТИОН»

Ян СУХИХ,
руководитель направления по информационной безопасности, R&D Центр Иннополис подразделения Industry компании Schneider Electric

Игорь ТАРВИ,
ведущий архитектор систем безопасности АСУ ТП, АО «ДиалогНаука»

Закон № 187-ФЗ «О безопасности КИИ РФ» установил базовый набор мер информационной защиты для российских компаний из ключевых отраслей. Мы решили обсудить с экспертами, насколько данные меры адекватны современным угрозам в сфере кибербезопасности и насколько они реализуемы.

Какова доля коммерческих компаний, которым придется соблюдать требования к ИБ, регламентированные законом № 187-ФЗ «О безопасности КИИ (критической информационной инфраструктуры)»?

Сергей ЗОЛОТУХИН

Среди субъектов КИИ, определенных в статье 2 Закона № 187-ФЗ есть не только государственные органы и государственные учреждения, но еще и юридические лица, и даже индивидуальные предприниматели. В банковской сфере, ТЭК, промышленности, транспорте, связи, энергетике, естественно, много коммерческих организаций, и часть из них является субъектами КИИ. На мой взгляд, делить организации – субъекты КИИ по принципу получения прибыли некорректно. Требования закона одинаковы для всех независимо от того, ведет организация коммерческую деятельность или нет. Если организации принадлежат информационные системы, отнесенные к КИИ, – выполнение требований закона для нее обязательно.

Игорь ТАРВИ

В определениях закона указываются сферы деятельности, на которые распространяются требования по обеспечению безопасности критической инфраструктуры, а именно: здравоохранение, наука, транспорт, связь, энергетика, банки, финансы, ТЭК, атомная энергетика, оборонная, ракетно-космическая, горнодобывающая, металлургическая

и химическая отрасли промышленности. Закон причисляет к критической информационной инфраструктуре все компании, информационные системы которых функционируют в указанных сферах деятельности.

В каждой из этих сфер деятельности задействовано немало коммерческих компаний. В частности, финансовая сфера полностью подпадает под действие закона, а это банки и страховые компании, которые являются коммерческими организациями, что уже может говорить о довольно большой доле коммерческих компаний, которым необходимо соблюдать требования Закона № 187-ФЗ.

Зафиксированные в приказах № 235 и № 239 ФСТЭК требования к ИБ КИИ являются, по вашему мнению, адекватными, избыточными или недостаточными?

Сергей ЗОЛОТУХИН

На мой взгляд, требования, установленные нормативными документами, в целом соответствуют текущей ситуации. Выполнение этих требований действительно обеспечит приемлемый уровень ИБ. Однако специфика киберугроз такова, что ситуация меняется очень быстро. В связи с этим важна поддержка требований в актуальном состоянии, чтобы обеспечить адекватный ответ на угрозы не только сегодняшнего дня, но и ближайшего будущего.

Дмитрий КУЗНЕЦОВ

Если посмотреть требования ФСТЭК России к разным видам информационных систем в порядке их утверждения (приказы № 17 и № 21, приказ № 31, затем приказы № 235 и № 239), то видно их эволюционное развитие. В каждом новом документе учитываются недостатки предыдущих, при этом ведомство прислушивается к мнению профессионального сообщества. Сами требования сформулированы таким образом, что фактически обязывают владельца каждой информационной системы самостоятельно формировать индивидуальные требования безопасности, учитывающие специфику защищаемой системы и актуальные для нее угрозы. Поэтому мнения об избыточности или недостаточности требований часто оказываются результатом нежелания владельцев ИС самостоятельно анализировать угрозы или признавать их наличие, если защита от них требует существенных затрат.

Ян СУХИХ

Требования к ИБ КИИ, зафиксированные в приказах № 235 и № 239 ФСТЭК, на мой взгляд, являются достаточно адекватными. Они закрывают как техническую, так и организационную части, что в совокупности и при должном исполнении позволяет существенно снизить риски инцидентов, связанных с информационной безопасностью. Разделение по категориям значимости также получилось достаточно логичным, требования не выглядят чрезмерными.

В то же время все меры, прописанные в приказе № 239, имеют очень общий характер и могут трактоваться в широчайших пределах. К сожалению, общий характер рекомендаций очень сильно снижает полезность приказа. Ответственные компании, которые понимают цену потери информации и/или простоя производства по вине киберпреступников, обладающие необходимыми кадрами, могут должным образом трактовать требования приказа или даже шагнуть гораздо дальше, чем того требует приказ № 239 ФСТЭК. Они будут принимать к сведению требования этого приказа, но ориентироваться скорее на западную модель: отталкиваться от модели угроз и оценки рисков и внедрять средства защиты информации, которые не только необходимы, но и целесообразны в каждом конкретном случае. Такие компании при оценке необходимости защиты той или иной системы и при выборе необходимых мер будут руководствоваться не только Постановлением № 127-ПП, но и оценкой бизнес-рисков – таким образом перечень защищаемых систем станет гораздо шире.

Другие компании, субъекты КИИ, которые не обладают достаточными компетенциями в области ИБ, хотят найти в приказе № 239 конкретные рекомендации о том, как им защитить свои системы. Таких компаний сейчас большинство, но в этом приказе нет ответа, есть лишь общие правила и требования, и когда собственники КИИ начинают прорабатывать их, возникает лавина вопросов, ответы на которые найти не так просто.

Есть еще одна группа компаний собственников КИИ – те, кто не хочет инвестировать в ИБ, и их цель свести издержки на реализацию мер по Закону № 187-ФЗ к минимуму. Для таких компаний есть лазейка – формальное соответствие нормативным актам. Это означает, что таким компаниям будет достаточно установить антивирусное программное обеспечение, закупить самые дешевые межсетевые экраны, а большинство остальных требований закрыть организационными мерами, исполнение которых будет крайне сложно, если вообще возможно, проверить. В этом случае реальная ситуация с информационной безопасностью предприятия не улучшится, но формальное соответствие требованиям закона у заказчика будет.

От такой работы не будет толку ни самой организации, ни государству.

В заключение хотелось бы сказать, что ФСТЭК выпустил хорошие документы, но нужно двигаться дальше и прорабатывать детали. Без этого вся огромная работа, которая была проделана в области повышения информационной безопасности КИИ, не принесет должного результата.

Игорь ТАРВИ

Зафиксированные в приказах № 235 и № 239 ФСТЭК России требования к обеспечению безопасности значимых объектов КИИ являются вполне адекватными и выполнимыми.

В приказе № 235 определяются общие требования к созданию и функционированию системы безопасности ЗОКИИ, определены силы и средства, с помощью которых должна обеспечиваться безопасность объектов КИИ, обязанности их владельцев по построению службы информационной безопасности. Также даны рекомендации для структуры и содержания организационно-распорядительной документации по безопасности ЗОКИИ. При этом ФСТЭК России не стала предлагать какой-то конкретный перечень ОРД, ограничившись лишь его содержанием, оставив за субъектами КИИ право выбирать форму и наименование документов, регламентирующих деятельность по защите ЗОКИИ, а также возможность включения определенных положений в состав уже имеющийся в компании нормативной документации по ИБ. ФСТЭК России не стала навязывать и применение сертифицированных средств защиты информации, отдав это на усмотрение субъектов КИИ, обязав применять такие средства лишь в случае, если этого требует законодательство РФ.

Что касается приказа № 239, то он устанавливает требования к самим системам защиты, которые обеспечивают безопасность объектов КИИ от целенаправленных атак. В данном приказе определен состав мер, которые необходимо выполнить для защиты объектов КИИ. Следует отметить, что состав мер не нов и по большей части совпадает с аналогичным из приказа ФСТЭК России № 31 (АСУ ТП) от 14 марта 2014 г. Также многие аналогичные меры присутствуют в приказах № 17 (ГИС) и № 21 (ПДн) – прослеживается желание ФСТЭК России прийти к единому, общему для всех приказов перечню мер защиты.

Представители каких из указанных в Законе № 187-ФЗ сфер деятельности, по вашему мнению, наиболее продвинулись в обеспечении ИБ значимых объектов КИИ (ЗОКИИ)? Что необходимо сделать, чтобы «отстающие» в кратчайшие сроки реализовали требования к ИБ для своих объектов?

Сергей ЗОЛОТУХИН

Наиболее подготовлены, на мой взгляд, организации финансовой сферы. Банки были и остаются одной из первых целей атакующих, поэтому в финансовой индустрии накоплен большой опыт обеспечения ИБ – как в части практического противостояния, так и с точки зрения регулирования. Что касается «отстающих», как вы их назвали, то здесь основную роль играют два фактора: первый – желание и готовность организации решать задачи по обеспечению безопасности; второй – финансирование работы по обеспечению соответствия законодательству. К сожалению, зачастую работы откладываются именно из-за неготовности организаций, которые ссылаются на недостаточно четкие требования или методические указания, отсутствие опыта подобных работ и т. д. На наш взгляд, таким организациям нужно не отсиживаться в ожидании указа сверху, а начинать пошаговую реализацию требований и в процессе проведения работ получать необходимый опыт.

Дмитрий КУЗНЕЦОВ

Требования приказа ФСТЭК России № 239 фактически систематизируют опыт создания систем безопасности информации, наработанный федеральными органами власти и коммерческими компаниями. Поэтому в наибольшей степени ему соответствуют организации, которые давно сталкиваются с инцидентами: например, когда кибератаки используются как инструмент для хищения денежных средств из банков или продукции у промышленных предприятий. Такие организации реализовали большую часть мер защиты приказа № 239 задолго до того, как был принят соответствующий Федеральный закон. Так, к лидерам по защищенности можно отнести отдельные организации и холдинги банковской сферы, энергетики, ТЭК, металлургической и химической промышленности.

Дмитрий МИХЕЕВ

За II и III кварталs 2018 г. мы провели более 60 пилотных проектов у представителей самых различных отраслей экономики. К III кварталу сложилась такая картина: если заходит речь про соответствие требованиям регулятора, то оказывается, что так или иначе работы по категоризации в терминах закона № 187-ФЗ идут. Задачи поставлены, ответственные назначены. Это большой поворотный момент, и представители промышленности шли к нему долго.

Не уверены, что наша статистика в чем-то показательна: как правило, учитывая активность и позицию регулятора, существуют две полярные ситуации. Либо есть четкая уверенность, что указанные требования не касаются данного предприятия, либо в каком-то виде процессы,

связанные с подготовкой к категоризации, уже запущены. И конкретная позиция предприятия не слишком завязана на сферу деятельности. Торопить этот процесс, наверное, возможно, но стоит вопрос: нужно ли еще сильнее нагнетать ситуацию? Регулятор делает очень правильные и понятные ответственным людям шаги в части поддержания процесса, а скорость здесь – не показатель. Мы говорим о том, что необходимо подготовить, часто с нуля, определенный набор документов, разработать регламенты и реализовать их, хотя бы вчерне, на весьма немаленьких предприятиях.

Нам кажется, по опыту похожих предыдущих кампаний, разумным сроком будет конец 2019 г., когда установятся определенные стандарты, будут набраны и включены в работу люди, а регламенты – освоены и уточнены. Все-таки порядок прохождения и приемки документов еще не отработан до конца, опыта мало, многое делается по аналогии, в несколько итераций. Для этого требуются и время, и средства. Компании, которые могли бы стать помощниками в этом непростом деле – предоставлять экспертизу, есть, но их пока не так много, а работы у них предостаточно, как вы понимаете.

Как следствие, трудно ожидать от любой индустрии каких-то успехов, значительно отличающихся от средних показателей. Это непрофильная активность для предприятий. Несмотря на это, необходимость подобной инициативы понятна специалистам, и если и не приветствуется, то, как минимум, не вызывает жесткого противодействия. Дело это государственного масштаба, требования будут выполнены так или иначе.

Нам, как производителю средств, связанных с выполнением требований в соответствии с этими законами, также необходимо провести собственные работы. В настоящий момент мы активно используем наше решение для реализации мер защиты, реализуя приличный набор функционала для соответствия требованиям регуляторов. Тем не менее у нас тоже есть необходимость доработать наше ПО для соблюдения уточненных мер защиты по нашей тематике, отработать практику применения, довести обновленное ПО до необходимого уровня сертификации на уровень доверия. Это все не получится реализовать мгновенно, но, как и наши уважаемые заказчики, мы эти задачи себе поставили и работаем по плану.

Ян СУХИХ

Думаю, лидерство однозначно стоит отдать организациям, относящимся к финансовому сектору. Это лидерство легко объяснимо: финансовые организации являются основной мишенью киберпреступников, поэтому чаще других сталкиваются с кибератаками и вынуждены принимать меры по защите инфраструктуры. Выделить какие-либо другие отрасли я не могу, в каждой есть предприятия, которые довольно далеко продвинулись в защите ЗОКИИ, но есть и отстающие. В целом рынок постепенно раскачивается, но медленно.

Сейчас есть довольно много объективных причин для такой замедленной реакции организаций:

- отсутствие явно прописанных сроков прохождения этапов реализации требований Закона № 187-ФЗ, а точнее, срока утверждения перечня объектов КИИ, от которого и начинается обратный отсчет;
- отсутствие конкретики в требованиях к защите ЗОКИИ;
- отсутствие на рынке достаточного количества специалистов в области информационной безопасности;
- сложные взаимоотношения между службами ИТ, АСУ ТП (большинство ЗОКИИ в промышленности – это автоматизированные системы управления) и службой безопасности, что существенно затрудняет процесс.

С моей точки зрения, для ускорения реализации требований закона о КИИ нужны прозрачные «правила игры»: понятные, разумные сроки; необходимо выпустить разъяснения к приказу № 239 ФСТЭК, где будет гораздо больше конкретики; определиться по взаимодействию с ГосСОПКА.

С точки зрения реализации далеко не все компании располагают достаточным количеством ресурсов для внедрения комплексных систем информационной безопасности. Было бы отличным подспорьем, если бы для предприятий была возможность привлекать дешевые кредиты на реализацию мер по приведению ИС, АСУ, АСУТП в соответствие с требованиями Закона № 187-ФЗ.

Игорь ТАРВИ

В основном больше всего продвинулись те компании, которые связаны с энергетикой, и промышленные предприятия. Многие из них и до вступления в силу Закона № 187-ФЗ считались критически важными объектами и к ним применялись особые требования по обеспечению безопасности. На таких предприятиях на производстве для автоматизации управления технологическим оборудованием задействованы автоматизированные системы управления технологическими процессами (АСУ ТП), нарушение функционирования которых может привести не только к остановке производства, но и нанести серьезный ущерб для жизни и здоровья людей, для окружающей природной среды, экономики и обороноспособности страны и т. д. Руководство таких предприятий придает большое значение обеспечению безопасности своих автоматизированных систем от возможных кибератак. Для защиты автоматизированных систем на подобных предприятиях ранее ФСТЭК России был принят приказ № 31 от 14 марта 2014 г. «Об утверждении Требований к обеспечению защиты информации в АСУ ТП на КВО, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». Данный приказ можно считать преддверием Закона № 187-ФЗ, набор мер защиты из приказа № 31 по большей части перекочевал в приказ № 239, что облегчает реализацию требований закона о КИИ для тех компаний, где уже проводились работы по приведению защиты в соответствие с требованиями приказа № 31 ФСТЭК России.

Необходимо отметить, что многие банки также уже реализовали большой комплекс мероприятий, предусмотренный требованиями

Закона № 187-ФЗ. Это связано с тем, что кредитно-финансовые организации должны соответствовать целому ряду отраслевых стандартов по защите информации, таким как PCI DSS, СТО БР ИББС, положению № 382-П ЦБ РФ и др., которые предполагают реализацию мер, пересекающихся с требованиями Закона № 187-ФЗ.

Для реализации требований ИБ в минимальный срок необходимо запустить в компании процедуру категорирования объектов КИИ, определить критические процессы и состав систем, обеспечивающих их выполнение, направить перечень объектов КИИ, подлежащих категорированию в ФСТЭК России и, не откладывая в долгий ящик, заняться приведением в соответствие организационно-технических мер защиты. Для экономии времени эти процессы можно выполнять параллельно. Стоит отметить, что с момента направления перечня объектов КИИ, подлежащих категорированию, во ФСТЭК России владельцам объектов КИИ отводится на выполнение необходимых работ до одного года.

Возможно ли удовлетворить требования регулятора по созданию службы управления ИБ и построению системы защиты до конца этого года? Какие сроки завершения процедуры категорирования вам кажутся наиболее реалистичными?

Сергей ЗОЛОТУХИН

Если говорить о системах защиты, то в большинстве организаций они в той или иной степени уже работают. Да, они требуют модернизации и дополнения современными средствами в соответствии с требованиями, но в целом системы защиты в организациях уже построены. Сложнее с управлением ИБ. На бумаге создать такую службу просто, а вот так же быстро внедрить процессы управления ИБ невозможно. Для того чтобы выстроить системы управления безопасностью, в организациях должен быть достигнут определенный уровень зрелости ИБ: необходимо разделить процессы мониторинга и реагирования, сформировать службу аналитиков, обеспечить управление всеми процессами, связанными с обеспечением ИБ. Если всего этого в организации нет, то выполнить требования до конца года – это очень амбициозная, однако почти нереальная задача.

Категорирование – одна из самых обсуждаемых тем сегодня. Порядок проведения категорирования определен, процедуры описаны. Организации с высоким уровнем зрелости ИБ могут провести эти работы достаточно быстро. Если же требуется проведение масштабного аудита, оценка угроз безопасности, разработка моделей угроз и нарушителя, тогда работы действительно могут затянуться. Но в любом случае один год – это достаточный срок.

Дмитрий КУЗНЕЦОВ

Даже для значимых объектов КИИ регулятор не требует создать систему защиты к какому-либо определенному сроку. Вместо этого приказ № 235 нормативно закрепляет циклический подход к реализации мер защиты (цикл PDCA). Субъекту предписывается ежегодно планировать, в каком объеме и какими средствами он будет реализовывать те или иные меры защиты, и в дальнейшем, также на основе ежегодных планов, эти меры защиты можно совершенствовать. Поэтому субъект вправе к концу года реализовать меры защиты в минимально необходимом объеме, достаточном для формального соответствия приказам ФСТЭК, и в дальнейшем совершенствовать систему безопасности до того уровня, который владелец информационной системы сочтет достаточным для противодействия актуальным угрозам.

Регулятор добивается, чтобы субъекты в разумный срок предоставили перечни объектов, подлежащих категорированию. Ни в самом ФЗ, ни в Постановлении Правительства от 8 февраля 2018 г. № 127 этот срок не установлен. Поэтому регулятор называет рациональную с его точки зрения дату получения перечней, после наступления которой у него появится основание считать, что субъекты уклоняются от проведения категорирования. Само же категорирование должно быть проведено в течение года после направления во ФСТЭК перечня объектов.

Ян СУХИХ

Если ориентироваться на решение Коллегии ФСТЭК России от 24.04.2018 № 59, то категорирование необходимо закончить до 1 января 2019 г. Эта задача теоретически выполнима, но на практике едва ли. Еще есть организации, которые даже не создали комиссию по категорированию, да и сами работы по категорированию довольно трудоемки, что требует времени и серьезных ресурсов. Мне более реалистичным кажется срок до июля-августа 2019 г.

В соответствии с решением Коллегии ФСТЭК России от 24.04.2018 № 59 внедрение систем защиты ЗОКИИ необходимо закончить до 01.09.2019, что выглядит абсолютно нереалистичным. Даже если допустить, что 1 января 2019 г. все субъекты КИИ проведут категорирование, то внедрить системы защиты ЗОКИИ за 8 месяцев совершенно невозможно. За это время необходимо провести конкурсы на выбор проектных организаций, разработать проекты по защите ЗОКИИ, провести конкурсы на внедрение систем, внедрить системы защиты, провести обучение персонала и опытную эксплуатацию. Выполнить такую работу за 8 месяцев всем субъектам ЗОКИИ заведомо невыполнимо. Более реальным выглядит срок в 3–5 лет.

Надо понимать, что в стране сейчас не найти даже достаточного количества специалистов, чтобы в обозначенные сроки успели запроектировать и внедрить системы на всех объектах ЗОКИИ, и тем более их не хватит для обслуживания всех этих систем.

За 8 месяцев можно успеть внедрить какие-то базовые меры, например разработать политики

и процедуры, но не выполнить весь комплекс мер, включая интеграцию с ГосСОПКА.

Впрочем, всегда есть возможность формального подхода. В этом случае можно успеть до 01.09.2019 привести защиту объектов КИИ в соответствие с требованиями ФЗ, но это будет фиктивное исполнение требований, где основная доля мер будет носить организационный характер и на практике выполняться не будет.

Игорь ТАРВИ

На мой взгляд, создание службы ИБ и проведение процедуры категорирования не должно занять много времени, тем более что после направления первичного списка объектов КИИ в ФСТЭК России компаниям дается до одного года для проведения категорирования своих систем.

Что касается построения системы защиты, то для тех компаний, которые изначально уделяли должное внимание обеспечению безопасности своих систем, например в рамках выполнения требований по защите персональных данных или АСУ ТП, и реализовали комплекс технических мероприятий по построению системы защиты, это вполне реально. Тем компаниям, в которых вопросам безопасности критических систем уделялось гораздо меньше внимания, конечно, потребуется приложить больше усилий. Но даже если очевидно, что в такой компании не удастся завершить полный комплекс мероприятий до конца года, тем не менее очень важно как можно раньше начать построение системы защиты, что позволит существенно минимизировать потенциальные риски от возникновения угроз безопасности критических систем.

Насколько, на ваш взгляд, затратно будет соблюдение обнародованных требований регуляторов?

Сергей ЗОЛОТУХИН

Как я говорил выше, требования регуляторов к обеспечению безопасности вполне адекватные, они соответствуют актуальному уровню угроз. Если организация ранее уже задумывалась о своей безопасности и современная система ИБ в организации уже существует, дополнительные затраты будут невелики. Ну а если строить систему защиты с нуля – то да, в создание современной системы защиты придется вложить немало средств.

Ян СУХИХ

Если собственник КИИ относится к задаче ответственно, понимает риски и действительно хочет повысить защищенность своих активов, то внедрение защитных мер обойдется недешево. Впрочем, если речь идет о крупном бизнесе, то потери от возможного простоя/порчи оборудования будут гораздо выше и затраты в этом случае целесообразны.

Если цель организации – формальное соблюдение требований регуляторов, то затраты будут незначительные. Другое дело, что такие компании будут находиться в зоне повышенного риска с точки зрения ИБ. В то время как большинство компаний будут повышать свою защищенность и их взлом будет стоить слишком дорого для подавляющего числа злоумышленников, компании, которые решат пойти по формальному пути, станут лакомым кусочком для киберпреступников.

Игорь ТАРВИ

Построение адекватной защиты требует определенных затрат, но, на мой взгляд, требования Закона № 187-ФЗ выглядят вполне корректно, в них отсутствует избыточность. В целом перечень необходимых работ для выполнения требований № 187-ФЗ сравним с тем, что проводится для выполнения требований, например, к защите персональных данных или защите АСУ ТП, при этом во многом эти требования перекрывают друг друга. Потому если в компании уже выполнялись подобные работы, то это может существенно снизить затраты на выполнение требований № 187-ФЗ.

Насколько сложна, по вашему мнению, реализация требований регуляторов для небольших владельцев ЗОКИИ? Возможно ли появление рынка аутсорсинга услуг по защите ИБ для таких владельцев?

Сергей ЗОЛОТУХИН

Небольшие компании, действительно, могут не иметь ресурсов, достаточных для самостоятельного выполнения требований. В такой ситуации единственным выходом является аутсорсинг ресурсов. Хорошо зарекомендовала себя практика, когда базовые средства защиты организация внедряет самостоятельно, а вот внедрение решений, обеспечивающих защиту от самых современных атак, проводится с помощью внешней компании. Также очень эффективно работает передача на аутсорсинг функций мониторинга. В этом случае владелец объекта КИИ не тратит свои ресурсы на рутинный мониторинг событий ИБ, а фокусируется на реагировании и минимизации ущерба.

Дмитрий КУЗНЕЦОВ

Основная сложность заключается не в формальном соответствии требованиям нормативных документов, а в реальном обнаружении атак и реагировании на инциденты. Для этого нужны специалисты-практики, а подобных практиков не так много не только в РФ, но и в мире. Поэтому параллельно с созданием систем защиты значимых объектов КИИ идет процесс создания центров ГосСОПКА – системы центров кибербезопасности, которые будут оказывать услуги субъектам КИИ, выполняя для них те функции по

противодействию компьютерным атакам, которые эти организации не в состоянии исполнять самостоятельно.

Ян СУХИХ

Для небольших компаний, владельцев ЗОКИИ, соблюдение требований № 187-ФЗ может стать непомерным бременем. Серьезные капитальные затраты вкупе с необходимостью найма высококвалифицированных специалистов зачастую могут стать неподъемными для ограниченных бюджетов небольших компаний. В этом случае возможным выходом является использование облачных сервисов, куда субъекты КИИ могут выносить свои сервисы, а их защиту будет обеспечивать провайдер.

Другой вариант – использование внешних SOC (security operation center). Данный сегмент рынка сейчас активно развивается, расширяется список предоставляемых сервисов. Сложно дать оценку, будут ли подобные сервисы популярны среди небольших компаний: все будет зависеть от стоимости подобных услуг и уровня доверия между покупателем и продавцом. Тема информационной безопасности весьма щепетильная, и доверие здесь играет очень важную роль.

Игорь ТАРВИ

В целом принципиально новых требований № 187-ФЗ не добавил, в том или ином виде они уже встречались в других документах ФСТЭК России, и велика вероятность, что часть требований в компании уже выполняется, если ранее проводились мероприятия по построению системы защиты. Говоря о сложности реализации, стоит акцентировать внимание именно на технической составляющей – внедрении средств защиты. В этом плане небольшим владельцам ЗОКИИ может быть даже в какой-то степени проще выполнить требования – за счет либо меньшего количества ЗОКИИ, чем у крупных компаний, либо за счет их территориального распределения. Организовать защиту ЗОКИИ в рамках одной территориальной площадки проще и менее затратно. ■

Ростех создаст киберзащищенные станки

Госкорпорация «Ростех» создает станкостроительный кластер для разработки и серийного производства современных высокоточных станков и обрабатывающих центров. Кластер на базе Ковровского электромеханического завода (КЭМЗ) решит проблему технологической зависимости российской экономики от зарубежного промышленного оборудования.

Об этом заявил во время выездного совещания в городе Коврове Владимирской области генеральный директор «Ростеха» Сергей Чемезов. В совещании по вопросам снятия законодательных барьеров в области диверсификации предприятий оборонно-промышленного комплекса также приняли участие спикер Государственной Думы ФС РФ Вячеслав Володин, депутаты Государственной Думы, представители Министерства промышленности и торговли РФ, представители законодательной и исполнительной власти Владимирской области.

В настоящий момент для расширения производства станочного оборудования на КЭМЗ возводится новый корпус площадью 5 тыс. м². Ввод нового цеха в эксплуатацию состоится в 2019 г. С учетом новых производственных площадей кластер сможет производить суммарно до 650 современных станков в год.

«Пример Ковровского электромеханического завода показывает, что наш подход к переводу военных предприятий на гражданские рельсы может решать не только задачу загрузки мощностей предприятий ОПК в периоды снижения гособоронзаказа, но и способствовать ликвидации технологической зависимости в критически важных отраслях», – подчеркнул генеральный директор Госкорпорации «Ростех» Сергей Чемезов.

Главной задачей кластера является максимальная локализация производства токарных, токарно-фрезерных, вертикально-фрезерных, горизонтально-фрезерных станков самого современного уровня, которые станут основой для создания «цифровых фабрик». Основным преимуществом российских станков и обрабатывающих центров является отечественная система ЧПУ, которая обеспечит их киберзащищенность: станки нового поколения гарантируют высокий уровень информационной защиты и отсутствие скрытых возможностей для несанкционированного удаленного доступа к системам.

«В состав станкостроительного кластера войдут ведущие российские предприятия, способные создавать элементы станочного оборудования, а также исследовательские институты, готовые разработать всю необходимую документацию. Формирование такой кооперации позволит в кратчайшие сроки расширять линейку оборудования, которое будет производиться на КЭМЗ в интересах российской промышленности», – добавил Сергей Чемезов.

На данный момент на мощностях КЭМЗ в рамках кооперации с предприятиями, которые войдут в кластер, уже осуществляется сборка 10 моделей станков. Созданы первые образцы пяти осевых вертикально-фрезерных обрабатывающих центров с программным управлением, которые могут производить детали высших классов точности, например турбинные лопатки или сотовые компоненты в авиастроении. Доля российских компонентов в продукции КЭМЗ сегодня составляет от 50 до 60%. К 2026 г. долю зарубежных комплектующих планируется снизить – она будет составлять не более 10%.

https://rostec.ru