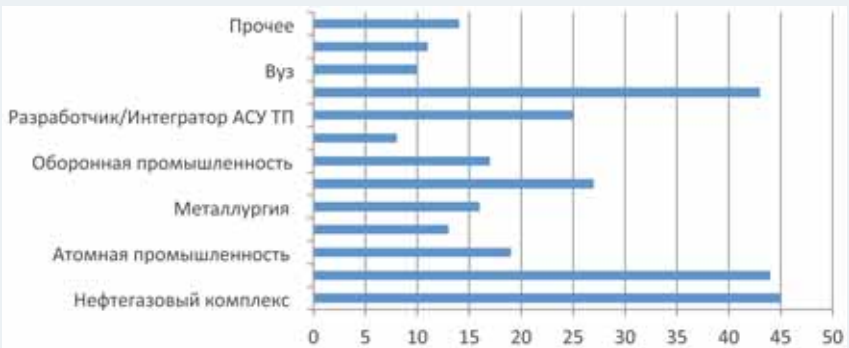
Отраслевая безопасность.
Начало

Флагманская тема на рынке информационной безопасности в 2018 г. – вступление в силу Федерального закона № 187 «О безопасности КИИ», который требует от компаний в критических сферах деятельности обеспечить информационную безопасность своих информационных ресурсов. Вопросам обеспечения защиты наиболее критических систем промышленных предприятий – АСУ ТП и была посвящена шестая конференция «Информационная безопасность автоматизированных систем управления технологическими процессами критически важных объектов». В рамках конференции был проведен опрос, в котором приняло участие 258 человек. Речь в нем шла о готовности предприятий к соблюдению законодательных норм по КИИ.

1. Какую организацию вы представляете?
Количество ответов: 258.
Допускались альтернативные варианты ответа.



Конечно, демографический состав специализированной конференции не может быть репрезентативным, поскольку он представляет мнение только тех людей, которые уже интересуются безопасностью АСУ ТП. Из перечисленных в Федеральном законе № 187-ФЗ сфер деятельности безопасностью АСУ ТП заинтересованы в основном представители нефтегазовой отрасли (45 ответов), энергетики (44 ответа) и химики (27 ответов). Данная тема привлекает внимание и представителей рынка ИБ (43 ответа). Разработчики АСУ ТП и интеграторы заняли бы в общем зачете пятое место с 25 заполненными анкетами. Таким образом, безопасностью АСУ ТП интересуются специалисты, работающие в сферах государственного контроля или имеющие конкретные бизнес-интересы.

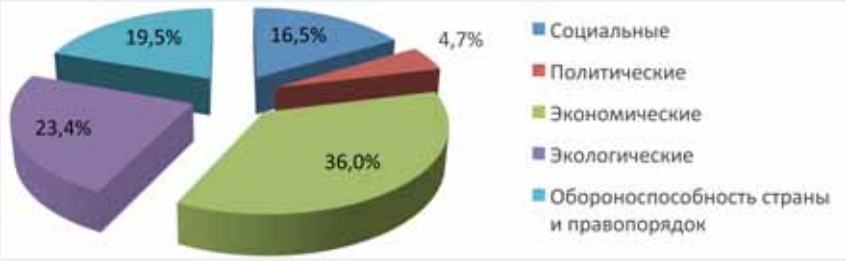
2. Как вы оцениваете четкость и прозрачность требований Федерального закона № 187-ФЗ и подзаконных актов с точки зрения их практического применения?
Количество ответов: 255.
Альтернативные ответы не допускались.

Уровень исполнения требований регуляторов зависит от понимания специалистов на местах. Для этого законы должны быть сформулированы максимально четко и конкретно. Однако российские законодатели идут по пути создания целой экосистемы законодательных актов, где сам закон – лишь вершина айсберга, а соблюдать нужно требования всевозможных подзаконных актов различных регуляторов. В результате у специалистов не складывается целостная картина требований. Сейчас требования этого закона непонятны многим представителям отраслей (47,8%). Еще почти треть (29,8%) отмечают в законе «нюансы», вызывающие вопросы. Всего десять ответивших (3,9%) считают, что им все ясно. Возможно, со временем особенности законодательства в части КИИ станут более понятными для специалистов – именно ради этого и проводятся различные конференции.

3. Есть ли на вашем предприятии план работ по выполнению требований Федерального закона № 187-ФЗ и подзаконных актов?
Количество ответов: 262.
Альтернативные ответы не допускаются.

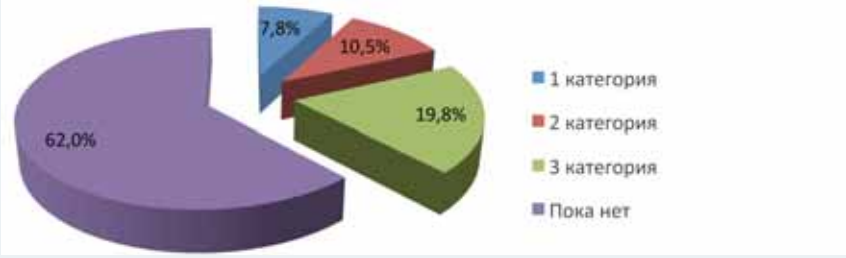
Любую работу нужно начинать с плана, тем более приведение в соответствие с требованиями законодательства. Вначале следует разобраться с положениями закона и выбрать стратегию реализации требований. Те, кто имеет план по выполнению работ, уже, как минимум, знают о наличии законодательных требований и даже приступили к их реализации, однако таких всего 6,5%. Большинство (49,6%) знает о наличии законодательных требований, но пока только формируют план действий. Почти каждый десятый (10,6%) считает, что его компания не подпадает под действие закона. Тут, конечно, стоит отметить, что речь идет о специалистах по информационной безопасности АСУ ТП, где доля причастных достаточно велика. Скорее всего, доля владельцев объектов КИИ по российским компаниям в целом значительно ниже 90%.

4. Какие группы негативных последствий, учет которых предусмотрен в Постановлении Правительства № 127-ПП при категорировании объектов КИИ, наиболее значимы для вашего предприятия?
Возможны альтернативные варианты.



Закон № 187-ФЗ определяет пять групп критериев значимости объектов по категориям угроз: для людей (социальный ущерб), для государственных органов (политический), для финансового климата (экономический), для среды обитания (экологический) и для безопасности страны (обороноспособность и правопорядок). Вывод объекта из строя может нанести ущерб в нескольких категориях сразу, поэтому в опросе допускался альтернативный выбор ответа. Наиболее часто встречаются критические объекты для экономики (131 ответ), экологии (85 ответов) и обороноспособности (71 ответ). Реже всего указывается политический ущерб – всего 17 ответов. Таким образом, ключевыми показателями являются стабильность финансовой системы и высокое качество окружающий среды: их безопасность и создает комфортные условия для жизни граждан. Влияние хакерских атак на социальную и политическую обстановку в стране оценивается, видимо, не очень высоко.

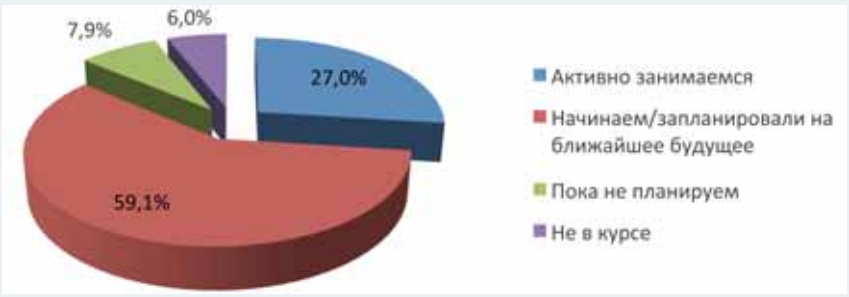
5. Есть ли у вас предварительное понимание, к какой категории преимущественно относятся ваши объекты КИИ?
Количество ответов: 258.
Альтернативные ответы не допускаются.



В законе предусмотрены три категории значимости объектов: самая слабая, минимальный ущерб – первая, максимальная – третья. Предусмотрено также отсутствие категории, когда ущерб от вывода из строя информационной системы ниже указанных в постановлении рамок. Естественно, что сейчас, менее чем через месяц после опубликования постановления, которое устанавливает критерии оценки ущерба, большая часть (62,0%) ответивших еще не успела определить категорию значимости. Остальные, скорее всего, также не сделали этого официально, но уже поняли масштабы предстоящей работы. Оказалось, что больше всего компаний отнесли себя к высшей третьей категории (19,8%), но из определившихся (без учета последнего варианта ответа) их доля составляет 52,0%.

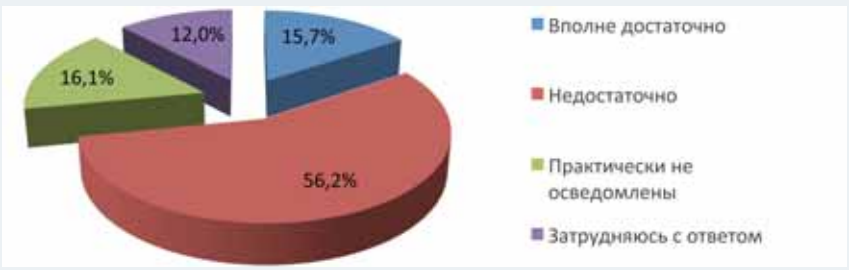
Меньше всего рассчитывают присвоить своим объектам первую категорию 7,8% общего числа и 20,5% определившихся. Возможно, критерии ущерба для различных объектов в постановлении завышены. Впрочем, подобная ситуация может означать и тот факт, что наиболее опасные производства и компании быстрее могут оценить ущерб от собственных проблем для окружающих.

6. Приступили ли на вашем предприятии к реализации мер по защите АСУ ТП как объекта КИИ?
Количество ответов: 252.
Альтернативные ответы не допускаются.



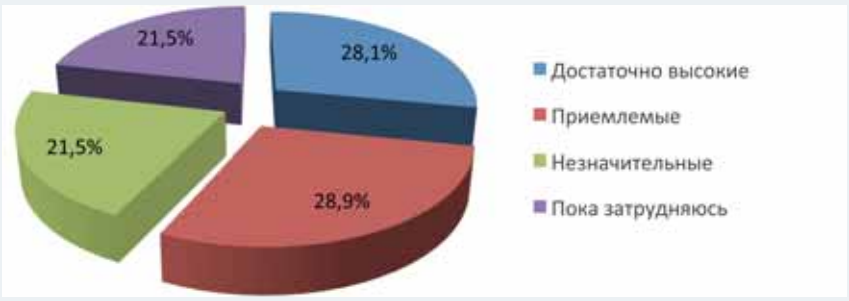
Федеральный закон № 187-ФЗ был принят еще летом прошлого года, но только после его вступления в силу и разработки подзаконных актов компании приступили к реализации набора мер – таких компаний 27,0%. Большинство специалистов (59%) ответили, что запланировали мероприятия на ближайшее будущее. И только 6,0% респондентов не имеют представления о том, что делает их предприятие по обеспечению безопасности ключевой информационной инфраструктуры.

7. Как вы оцениваете уровень осведомленности персонала вашего предприятия в области защиты АСУ ТП как части КИИ?
Количество ответов: 249.
Альтернативные ответы не допускаются.



Человеческий фактор является одним из ключевых в любой защите и обороне, и информационная инфраструктура не исключение. Поэтому компетенции компании в вопросах обеспечения безопасности КИИ крайне важны. Однако многие респонденты (56,2%) ответили, что считают уровень осведомленности и подготовки персонала в вопросах ИБ недостаточным для обеспечения безопасности объектов КИИ. Впрочем, значительна и доля специалистов (12,0%), которые вообще не задумываются над этим вопросом и потому затруднились с ответом. Приемлемый уровень осведомленности персонала у 15,7% респондентов, что явно недостаточно для обеспечения безопасности критической инфраструктуры.

8. Как вы оцениваете затраты на выполнение требований по защите АСУ ТП как части КИИ предприятия? Например, как долю от всего ИБ-бюджета предприятия?
Количество ответов: 228.
Альтернативные ответы не допускаются.



Экономический вопрос любого законодательства является важным показателем его исполнимости. Большинство респондентов (28,7%) считают, что для выполнения требований закона № 187-ФЗ эти затраты приемлемы. Примерно столько же (28,1%) предполагают, что им придется раскошелиться для реализации предписанных законодательством мер защиты. Возможно, что для тех компаний, которые уже ранее построили собственную систему информационной безопасности, затраты вполне приемлемы – достаточно подкорректировать деятельность соответствующих отделов и привести в порядок бумаги. Если же придется строить систему защиты с нуля, то расходы действительно могут показаться весьма существенными. Практически каждый пятый (21,5%) еще не оценивал объемы предстоящих работ.

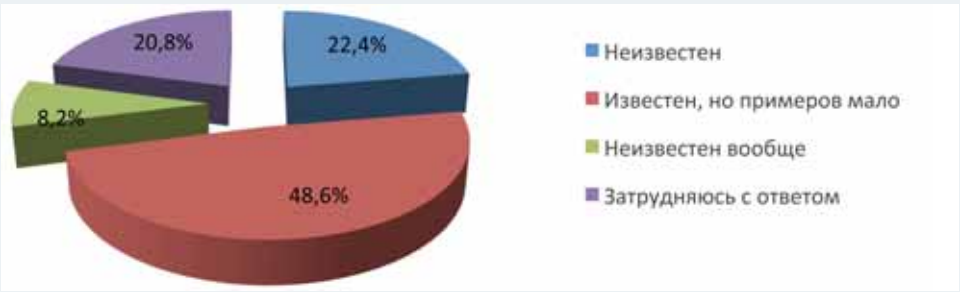
9. Как вы оцениваете ассортимент представленных на рынке продуктов и услуг по безопасности АСУ ТП?
Количество ответов: 244.
Альтернативные ответы не допускаются.

Вопрос защиты часто связывается с технологическими решениями. Однако сейчас, судя по ответам, большинство (38,9%) считает, что продукты вроде есть, но опыта их использования пока мало. По мнению 20,5% специалистов, отдельных видов средств защиты еще недостаточно. Доля удовлетворенных ассортиментом продукции, доступной на российском рынке, минимальна – 12,7%. Вполне возможно, что для массового удовлетворения требований законодательства в части защиты КИИ придется разработать специализированные продукты, которые позволят компаниям быстро отчитаться о соответствии законодательству. Впрочем, альтернативой является аутсорсинг систем защиты, услуги которого, при удовлетворении оператором законодательных норм, в ближайшее время, похоже, будут особенно востребованы.

10. Есть ли на вашем предприятии расхождения в понимании службами АСУ ТП и ИБ проблем защиты АСУ ТП?
Количество ответов: 246.
Альтернативные ответы не допускаются.

Проблемы в обеспечении безопасности АСУ ТП связаны, в частности, с тем, что эксплуатацией промышленных систем занимаются одни отделы, а их защитой – другие. Понятно, что для предприятия важнее выпустить товар, чем соблюсти во время производства требования законодательства. Поэтому иногда отдел АСУ ТП саботирует исполнение требований по информационной безопасности. Большинство респондентов (47,6%) отметили, что некоторые расхождения в понимании есть, но они не принципиальны. Доля принципиальных расхождений минимальна (12,6%). Это говорит о том, что в целом компании научились разрешать конфликты между службами АСУ ТП и ИБ. Возможно, принятый закон стимулировал этот процесс.

11. Насколько хорошо вам знаком опыт предприятий, подобных вашему, в области защиты АС ТП?
Количество ответов: 245.
Альтернативные ответы не допускаются.



Обмен опытом позволяет компаниям учиться на чужих ошибках и быстрее реализовать проекты в любой сфере. В информационной безопасности проектов по защите АСУ ТП уже достаточно много, поэтому обмен опытом вполне возможен. Сообщество специалистов по ИБ АСУ ТП оказалось достаточно открытым – 48,6% специалистов знакомы с опытом коллег, хотя и считают, что публичных проектов в этой сфере пока мало. При этом новых участников рынка, которым опыт коллег вообще неизвестен, всего 8,2%. Правда, еще 22,5% также получали мало информации о реализации проектов в сфере ИБ на аналогичных предприятиях, что подчеркивает важность проводимых Издательским домом «КОННЕКТ» конференций.

Выводы

Опрос, проведенный Издательским домом «КОННЕКТ», является достаточно представительным, поскольку удалось получить ответы специалистов практически из всех критических сфер деятельности, указанных в Законе № 187-ФЗ, где есть АСУ ТП, за исключением банков, государственных органов и телеком-операторов. Проблемы обеспечения безопасности именно АСУ ТП наиболее сложные, что повышает ценность настоящего опроса.

Следует отметить, что крупные компании из наиболее критичных для России отраслей, таких как нефтегазовая, энергетическая, химическая и др., уже активно занимаются реализацией требований закона: посещают тематические конференции, готовят соответствующие планы, оценивают значимость собственных объектов и изучают рынок средств защиты, необходимых для удовлетворения требований регуляторов. В этом году их количество даже превысило число представителей разработчиков средств ИБ – лидеров прошлого года. Кроме того, увеличилась доля разработчиков и интеграторов АСУ ТП. Таким образом, сегодня тема безопасности АСУ ТП интересует не только разработчиков средств защиты, но и владельцев и разработчиков АСУ ТП.

> Сегодня тема безопасности АСУ ТП интересует не только разработчиков средств защиты, но и владельцев и разработчиков АСУ ТП.

Опрос показал, что основным риском владельцы АСУ ТП называют экономический, т. е. ущерб для самого предприятия в случае выхода систем из строя.

> Основным риском владельцы АСУ ТП называют экономический, т. е. ущерб для самого предприятия в случае выхода систем из строя.

Может быть, и не нужно было принимать отдельный закон, а следовало просто подождать, пока «невидимая рука рынка» не убедила бы российские компании в необходимости обеспечивать собственную безопасность? К тому же политические риски от нарушения работы информационных систем АСУ ТП, судя по всему, минимальны. Впрочем, закон продолжает деятельность ФСТЭК по защите АСУ ТП, начатую с подготовки приказа № 31, подчеркивая важность промышленной кибербезопасности.

При этом сами владельцы АСУ ТП, судя по всему, склонны завышать ценность своих объектов. Хотя со времени публикации Постановления Правительства № 127 прошло всего две недели, большинство объектов, по предварительным оценкам, рассматриваются как наиболее значимые, что, естественно, потребует и значительных финансовых вложений в средства защиты, поскольку к третьей категории требования будут максимально жесткими. Одни владельцы планируют честно выполнять все требования регуляторов и вкладывать значительные средства, другие рассчитывают найти приемлемые по деньгам методы исполнения закона, причем доли обеих категорий примерно равны (с точностью до третьего знака).

В этом году по сравнению с прошлым снизилось число тех специалистов, которые были недовольны ассортиментом средств защиты, – с 29% до 18,4%. Правда, выделился сегмент респондентов, которые удовлетворены набором продуктов, но не качеством услуг, – таких оказалось 38,9%, Видимо как следствие, уменьшилась доля полностью удовлетворенных потребителей – с 16,4% до 12,7%. Таким образом, технологически ассортимент средств защиты достаточен, но возникает потребность в качественных услугах на их основе.

Стоит отметить, что за прошедший год стало меньше разногласий между отделами АСУ ТП и ИБ. Доля компаний, где разногласия были принципиальными, сократилась с 15,9% до 12,6%, в то время как доля компаний, где таких разногласий нет, увеличилась – с 17,6% до 22,8%. Вполне возможно, что здесь сказалось влияние законодательных требований по защите АСУ ТП от киберрисков, эпидемии шифровальщиков, а также проводимых нами конференций, которые снижают уровень недопонимания между этими группами специалистов. ■