



ИТОГИ ОПРОСА

VII КОНФЕРЕНЦИИ

**«Информационная безопасность АСУ ТП
критически важных объектов»**

Организатор конференции

Connect.
МЕДИАСЕРВИСНЫЙ ЦЕНТР

27–28 февраля 2019, г. Москва

Категорирование.

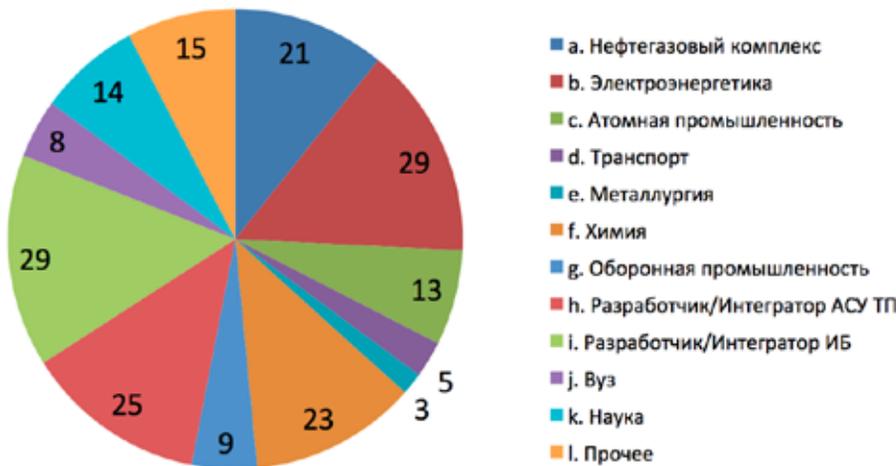
Первые результаты

Год 2018-й прошел у компаний из 13 ключевых отраслей под знаком процедуры категорирования, определенной в Постановлении Правительства № 127-ПП. Это только первый этап выполнения требований Федерального закона № 187-ФЗ «О безопасности КИИ», но и его прошли далеко не все. Первым результатам категорирования была посвящена седьмая конференция «Информационная безопасность автоматизированных систем управления технологическими процессами критически важных объектов». Поэтому в традиционный опрос участников конференции были добавлены вопросы, связанные с процедурой категорирования. Часть вопросов была взята из предыдущих анкет, что позволяет проследить изменение ответов на вопросы во времени. В этом году общее количество ответивших составило 194 человека.

Вопрос 1. Какую организацию вы представляете?

Общее количество ответов – 194.

Из 13 ключевых сфер деятельности, перечисленных в Федеральном законе № 187-ФЗ, семь находятся в нашем списке.



Из компаний, имеющих АСУ ТП, в раздел «Другие» попадают предприятия космической отрасли и операторы связи, и доля эта с каждым годом растет: в 2017 г. – 5,3%, в 2018 г. – 7,5%, в 2019 г. – 7,7%. Традиционно велика доля разработчиков и интеграторов ИБ – около 15%, но если в прошлом году они

уступили лидерство нефтегазовому комплексу и электроэнергетике, то в текущем нефтегаз уже насытился информацией и показал долю посещения конференции в 10,8%, хотя в электроэнергетике по-прежнему остается паритет с разработчиками и интеграторами ИБ – у обоих доля по 14,9%. В этом году на третье место вырвались разработчики и интеграторы АСУ ТП – их доля составила 12,9% (в прошлом – 8,6%). Неуклонно растет интерес к информационной безопасности у химиков: их доля в 2017 г. была 7,2%, в 2018 г. – 9,2%, в 2019 г. – 11,9%, и в результате они вышли на четвертое место, обогнав нефтегаз. В то же время металлургия теряет интерес к ИБ: в 2017 г. их доля составляла 6,1%, в 2018 г. – 5,5%, а в 2019 г. – всего 1,6%, и они вышли в абсолютные аутсайдеры, уступив даже транспорту с традиционно малой долей в несколько процентов.

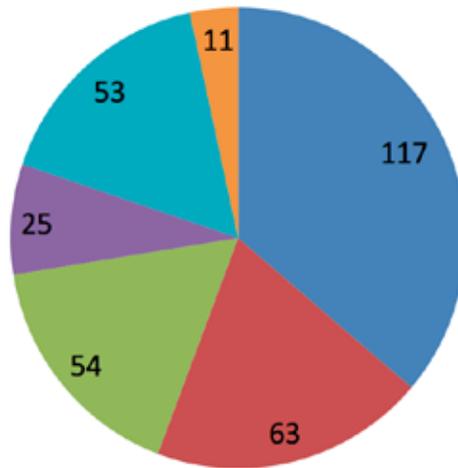
2. Какие нормативные акты для вашей организации или холдинга являются определяющими при формировании требований к информационной безопасности?

Общее количество ответов – 323.

Этот вопрос был задан в исследовании впервые, чтобы выяснить важность различных источников нормативных требований в сфере информационной безопасности. Оказалось, что в среднем две трети респондентов указали два источника, т. е. большинству

специалистов в процессе принятия решений приходится учитывать требования нескольких нормативных актов. Поскольку в опросе участвовало свыше 60% представителей отраслей, перечисленных в Законе № 187-ФЗ, то логично, что на первое место вышел

именно этот нормативный акт, хотя второе место – «Другие ФЗ» – вполне оправданно, поскольку федеральные законы должны соблюдать все компании, работающие на территории РФ. В то же время отраслевые регуляторы и обычаи делового оборота (требования внутренних документов и контрагентов) определяют примерно одинаковое количество требований ИБ. Меньше всего российских участников рынка заботят требования международных регуляторов.

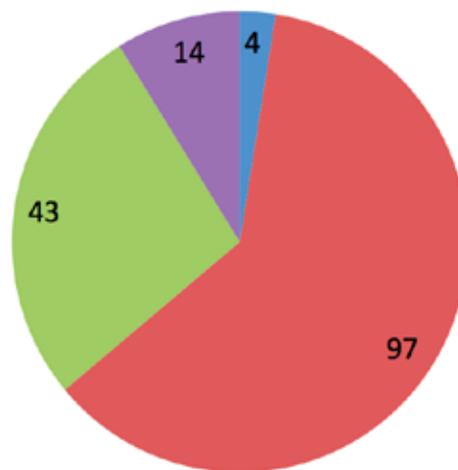


- а. Федеральный закон № 187-ФЗ «О безопасности КИИ»
- б. Другие федеральные законы (Персональные данные, государственные ИС)
- в. Требования отраслевых российских регуляторов
- г. Требования международных регуляторов
- д. Требования внутренних документов или контрагентов
- е. Другое

3. Как вы оцениваете четкость и прозрачность требований Федерального закона № 187-ФЗ и подзаконных актов с точки зрения их практического применения?

Общее количество ответов – 158.

Данный вопрос мы уже задавали в прошлом году, и тогда лидером среди ответов стал «Недостаточно четко, размыто» с долей ответов 47,8%. В этом году такой ответ оказался на втором месте с долей 27,2%, уступив первенство ответу «Все ясно, но есть нюансы», который выбрали 61,4% отвечавших. Доля тех, кто затрудняется ответить, также снизилась с 18,4% до 8,9%. Можно было бы констатировать, что просветительская



- а. Все четко и ясно
- б. Все ясно, но есть нюансы
- в. Недостаточно четко, размыто
- г. Затрудняюсь ответить

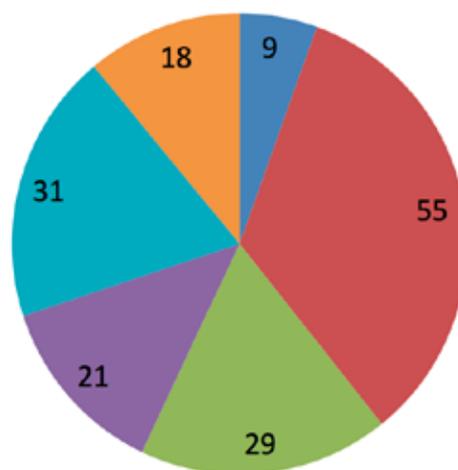
деятельность регуляторов возымела свое действие, если бы не первый вариант ответа «Все четко и ясно», доля которого за год также уменьшилась с 3,9% до 2,5%.

А это уже означает, что компании постепенно разбираются с требованиями Закона № 187-ФЗ и у них появляются дополнительные вопросы о его нюансах.

4. Сформирована ли на вашем предприятии комиссия по категорированию принадлежащих вам объектов КИИ?

Общее количество ответов – 163.

Этот вопрос новый – он пришел на смену задававшемуся в прошлом году «Есть ли на вашем предприятии план работ по выполнению требований Федерального закона № 187-ФЗ и подзаконных актов?». Понятно, что сейчас необходимо не просто иметь план, а выполнять предписания постановления № 127-ПП по категорированию. И если в прошлом году



- а. Сформирована, категорирование проведено, акт зарегистрирован во ФСТЭК
- б. Сформирована, перечень объектов передан во ФСТЭК
- в. Формируется
- г. Пока нет, наблюдаем
- д. Не подпадаем под действие закона
- е. Прочее

лидером по ответам был «Формируется» (49,6%), то сейчас этот же

ответ показывает скорее нераспоротность – таких ответивших

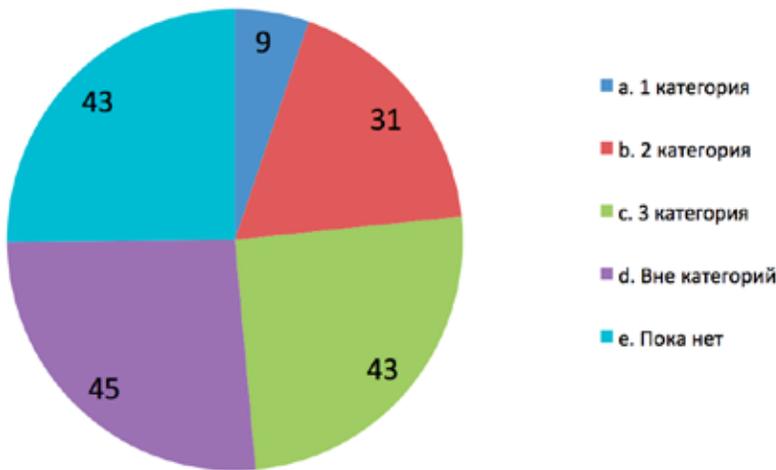
17,8% (второе место). Лидером стал ответ «Сформирована, перечень объектов передан во ФСТЭК» с долей в 33,7%. Это означает, что еще треть респондентов к следующей конференции должна будет завершить процедуру категорирования. Завершили данную

процедуру и готовы приступить к построению систем защиты своих значимых объектов 5,5% респондентов. Конечно, есть ответы «Не попадаем под действие закона» и «Прочее», сумма которых составляет 30,6%, однако если посмотреть на ответы на первый

вопрос, то окажется, что примерно столько отвечавших действительно не подпадают под действие закона – разработчики, интеграторы и др. Важнее, что доля наблюдающих оказалась достаточно большой – 12,9%, т. е. практически каждый восьмой отвечающий.

5. Есть ли у вас предварительное понимание, к какой категории преимущественно относятся ваши объекты КИИ?

Общее количество ответов – 171.

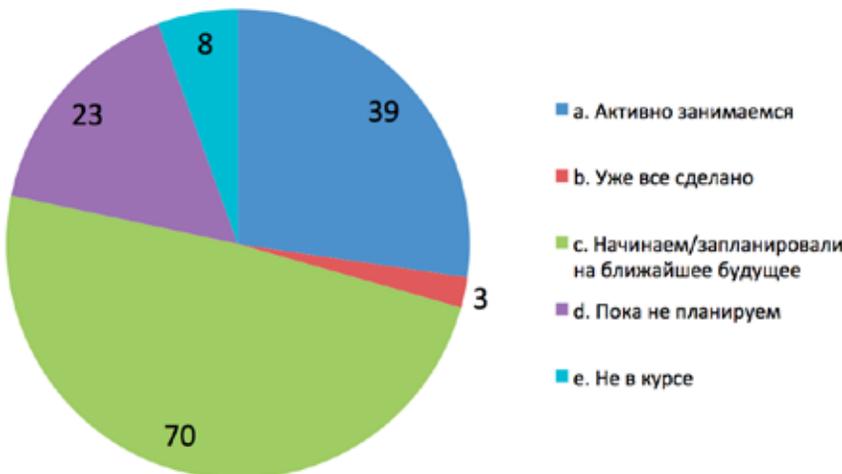


Этот вопрос был и в прошлом году, хотя в нем отсутствовал вариант ответа «Вне категорий», но именно такой результат категорирования, скорее всего, будет наиболее популярным. В 2019 г. мы разделили две ситуации: нет необходимости присваивания категории значимости;

нет предварительного представления о том, какая категория значимости должна быть присвоена. Оказалось, что доля ответов очень близка – 26,3 и 25,1% соответственно. В сумме они составили чуть больше половины ответов (51,5%), что меньше прошлогодних 62,0%, т. е. понимание, какие категории объектам необходимо присваивать, постепенно формируется. В то же время доля первой категории уменьшилась – с 7,8 до 5,3%. Доля второй категории увеличилась с 10,5 до 18,1%, еще больше – третьей категории (с 19,8 до 25,2%), практически достигнув (с точностью погрешности измерения) доли объектов вне категорий. Получается, что примерно у четверти объектов категория не определена, четверть являются незначимыми, четверть имеют третью категорию, в оставшиеся попадают объекты первой и второй категории.

6. Приступили ли на вашем предприятии к реализации мер по защите АСУ ТП как объекта КИИ?

Общее количество ответов – 143.



Данный вопрос задавался и в прошлом году, но сейчас был добавлен новый вариант ответа – «Уже все сделано», который выбрали 2,1% респондентов. При этом доля тех, кто активно занимается

реализацией мер защиты, увеличилась незначительно – с 27,0 до 27,3%. В то же время существенно увеличилась доля тех, кто пока не планирует, – с 7,9 до 16,1%. Видимо, разобрались с законом и поняли, что реализовывать меры защиты «не обязательно». Также уменьшилась доля тех, кто запланировал активность на ближайшее будущее, – с 59,1 в прошлом году до 49,0% в текущем. Похоже, что изначально Федеральный закон № 187-ФЗ представлялся как инструмент для навязывания новых средств защиты, однако уже через год он воспринимается уже как требование наведения порядка в документах и организационных мерах, а средства защиты можно при этом и не внедрять. Доля тех, кто «не в курсе», практически не изменилась – в этом году она составила 5,6%.

7. Как вы оцениваете уровень осведомленности персонала вашего предприятия в области защиты АСУ ТП как части КИИ?

Общее количество ответов – 145.

Этот же вопрос был задан и в прошлом году. За год доля оптимистов, которые ответили, что осведомленности персонала вполне достаточно, увеличилась с 15,7 до 23,5%. Впрочем, доля реалистов, которые отвечали «Недостаточно», уменьшилась с 56,2 до 47,6%. Однако пессимистов, которые считают, что персонал практически не осведомлен, также стало больше – 19,3%. В то же



время уменьшилось количество тех, кто затрудняется с ответом, – до 9,7%. Таким образом, можно констатировать, что специалисты

постепенно убеждаются в необходимости осведомленности сотрудников в вопросах информационной безопасности.

8. Были ли у вашего предприятия или холдинга инциденты информационной безопасности?

Общее количество ответов – 132.

Данный вопрос был задан впервые и сразу получил приз за минимальное количество ответов, что объяснимо – специалистам не особенно приятно отвечать на подобные вопросы. Да к тому же в нем был определенный подвох. Дело в том, что самый популярный ответ «Инцидентов зафиксировано не было» означает, что система мониторинга на предприятии работает не очень хорошо – служба безопасности просто не фиксирует инциденты. И таких ответов оказалось больше половины – 54,5%. Если же система



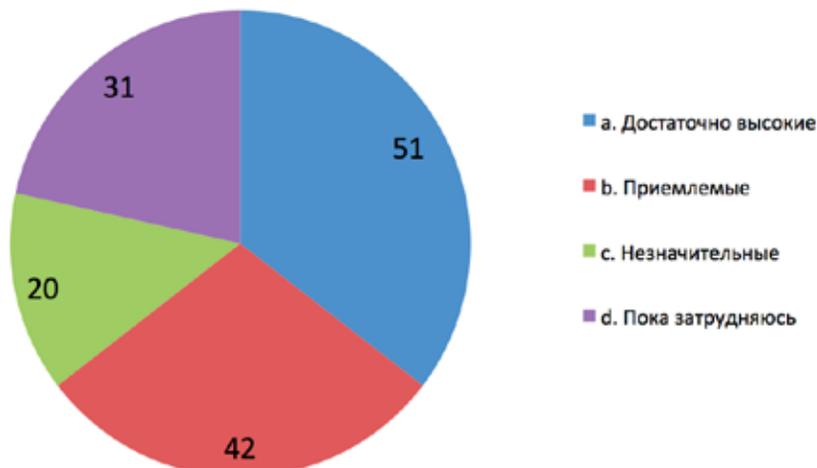
безопасности есть и работает, то в этом случае необходимо было отвечать «Были, но ущерба не было». До этого «додумались» 30,3% отвечавших, что является достаточно хорошим результатом. В наличии реального ущерба признались

единицы процентов: 1,5% с ущербом для АСУ ТП и 3,0% – без ущерба. Здесь достаточно высоким оказался процент выбравших пункт «Другое» – 10,6%. Возможно, речь идет о компаниях, которые просто не имеют АСУ ТП.

9. Как вы оцениваете затраты на выполнение требований по защите АСУ ТП как части КИИ предприятия? Например, как долю от всего ИБ-бюджета предприятия?

Общее число ответов – 144.

Этот вопрос задавался и на прошлой конференции. Тогда к нему отнеслись более оптимистично – лидером, хотя и с точностью до погрешности,



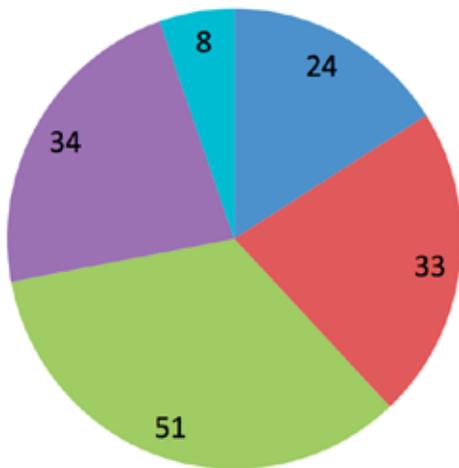
стал ответ «Приемлемые» с долей в 29,0%, «высокими» затраты назвали 28,0% респондентов. Чуть больше пятой части (21,5%) посчитали затраты на выполнение требований регуляторов к защите объектов КИИ

незначительными. В этом году ситуация изменилась. В лидеры выбился ответ, подразумевающий достаточно высокие затраты, – 35,4% респондентов, хотя и доля ответов «Приемлемые» немного увеличилась – до 29,2%. В то же

время существенно сократилось количество тех, кто посчитал затраты незначительными, – до 13,9%. Это при том, что доля тех, кто затруднялся с ответом, осталась практически на прежнем уровне – 21,5%.

10. Как вы оцениваете ассортимент представленных на рынке продуктов и услуг по безопасности АСУ ТП?

Общее количество ответов – 150.

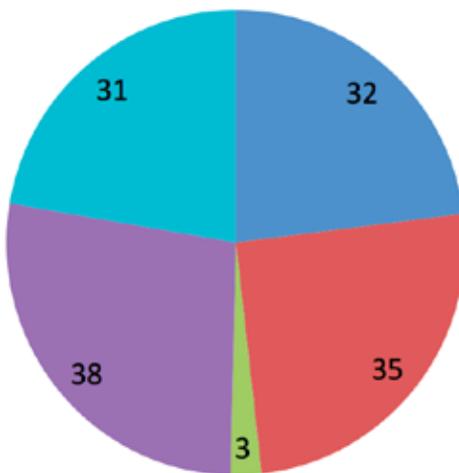


- а. Вполне достаточно, все классы представлены
- б. Недостает отдельных классов продуктов
- в. Продукты есть, не хватает опыта внедрения и эксплуатации
- г. Недостаточный, выбор невелик
- д. Прочее

неудовлетворенных предлагаемым выбором продуктов сокращается. Сейчас она составляет 22,7%, хотя в прошлом была меньше – 18,4%. Однако в прошлом году появился вариант «Продукты есть, не хватает опыта оказания услуг», который стал лидером с долей в 38,9%. В этом году он был сформулирован в другой форме – «Продукты есть, не хватает опыта внедрения и эксплуатации», который также стал лидером, но с меньшей долей – 34,0%. Серьезная проблема 2017 г. – нехватка отдельных классов продуктов – была купирована еще в прошлом году (до 20,5%), но в 2019 г. увеличилась до 22,0%. Видимо потому, что появились новые классы продуктов, например для автоматизации процесса категорирования, и именно их-то и не хватает специалистам.

11. Сформирована ли на вашем предприятии служба обеспечения ИБ АСУ ТП?

Общее количество ответов – 139.



- а. Да, в соответствии с приказом ФСТЭК
- б. Да, но нужно доработать часть требований приказа ФСТЭК
- в. Нет, отдана на аутсорсинг
- г. Нет, формируется
- д. Не знаю, другое

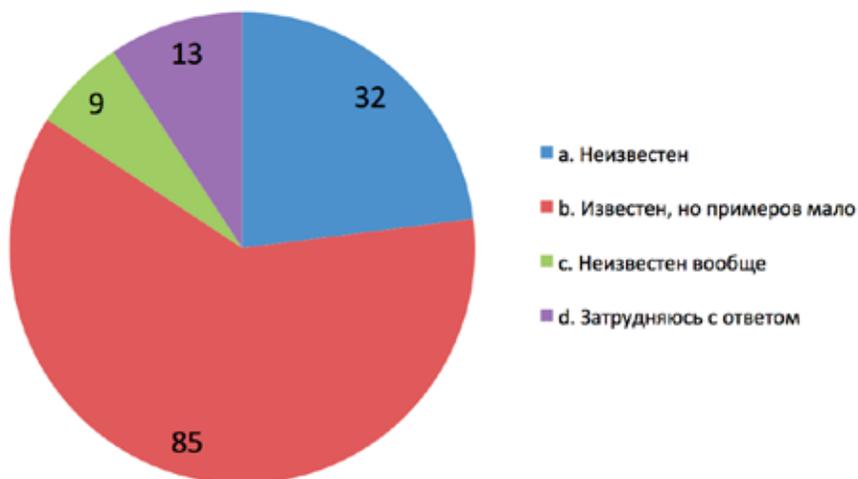
Этот вопрос связан с появившимися требованиями ФСТЭК по формированию службы управления информационной безопасностью на предприятии. И если раньше ее могло и не быть, то теперь такие службы формировать придется,

хотя можно подождать до завершения процедуры категорирования. Тем не менее уже сейчас 23,0% ответивших утверждают, что у них есть служба обеспечения безопасности АСУ ТП, которая соответствует требованиям приказов ФСТЭК, а еще 25,2% опрошенных уверяют, что служба есть, но ее нужно привести в соответствие этим требованиям. А доля тех, кто запланировал создание службы информационной защиты АСУ ТП на ближайшее будущее, составляет 27,3%, что является хорошим показателем. Правда, жалко, что услугами аутсорсинга пользуются не много компаний – всего 2,2%, однако если вспомнить, что речь идет о безопасности именно АСУ ТП, т. е. ключевых систем предприятия, то и этот результат будет вполне предсказуемым.

12. Насколько хорошо вам знаком опыт предприятий, подобных вашему, в области защиты АСУ ТП?

Общее количество ответов – 139.

Данный вопрос задавался в течение трех лет в неизменном виде, и лидером всегда был ответ, подтверждающий существование сформированного сообщества специалистов в сфере информационной безопасности. Примерно 61,1% специалистов (с точностью до погрешности измерений) обмениваются опытом друг с другом. «Выброс» наблюдался в прошлом году, когда эта доля уменьшилась до 48,9%, но заметно увеличилась доля тех, кто затруднился с ответом (до 20,8%). Видимо, в прошлом году еще не все



поняли, насколько слухи о проектах у соседей соответствуют действительности. В 2019 г. и затруднившихся с ответом стало меньше (9,4%), и осведомленных больше. Тут важно, что затрудняющихся с ответом всегда было больше, чем тех,

кому опыт соседей неизвестен. К счастью, регуляторы ведут активную просветительскую работу с организациями, на которые налагаются требования по информационной безопасности в части АСУ ТП, что постепенно улучшает ситуацию.

Заключение

Хотелось бы рассмотреть данный опрос с точки зрения внимания участников конференции по информационной безопасности в АСУ ТП к различным темам. В частности, обращает на себя внимание то, что разработчики АСУ ТП заинтересовались темой обеспечения безопасности собственных решений и даже стали участвовать в опросах. Это подтверждает тенденцию на разработку встроенных механизмов защиты в АСУ ТП, которая в конце концов приведет к созданию безопасных решений. Однако для этого нужно модернизировать саму АСУ. Впрочем, интерес к теме защиты АСУ ТП не пропадает и у разработчиков средств защиты, которые стараются создавать специализированные промышленные решения, которые позволят защитить уже работающие АСУ ТП без их модернизации. Качество такой защиты может оказаться хуже, чем встроенной, тем не менее в некоторых случаях такой подход

приемлем. Да к тому же и над повышением качества сейчас работают специализирующиеся на этом компании.

Следует отметить и отраслевые тенденции: постоянный интерес к теме безопасности АСУ ТП у электроэнергетиков и химиков, но снижение интереса к этой теме у нефтегазовых компаний и металлургов. Последних, поскольку они ориентируются на международные рынки, больше заботят не российские нормативные акты, а международные, а также обычаи делового оборота. Суммарное количество анкет из этих отраслей примерно соответствует самому непопулярному ответу на второй вопрос о приоритете международных стандартов. Видимо, для них важнее международные отраслевые конференции, чем общение с российскими регуляторами на конференциях.

В то же время компаниям приходится учитывать не только Федеральный закон № 187-ФЗ в формировании своих требований к системам защиты,

но и другие нормативные акты. В результате возникает необходимость в определенной гармонизации подходов и требований в различных отраслях, по различным законодательным актам и с международными стандартами. Задача эта сложная, и хорошо, что ФСТЭК регулярно пересматривает свои нормы и правила, чтобы максимально соответствовать потребностям тех, кто эти нормы будет реализовывать.

Стоит также отметить достаточно высокий процент тех, кто уже отправил перечень своих объектов КИИ во ФСТЭК. Если в октябре Виталий Лютиков, заместитель директора ФСТЭК, отмечал, что передали свои перечни объектов в ведомство 15% компаний, подпадающих под действие закона, то сейчас таких 33,7%, при том что 5,5% уже завершили процедуру категорирования. Процесс идет, причем достаточно активно, что позволяет надеяться на хороший результат уже к следующему году. ■