ИТОГИ ОПРОСА

IX КОНФЕРЕНЦИИ

«Информационная безопасность АСУ ТП критически важных объектов»

Организатор конференции

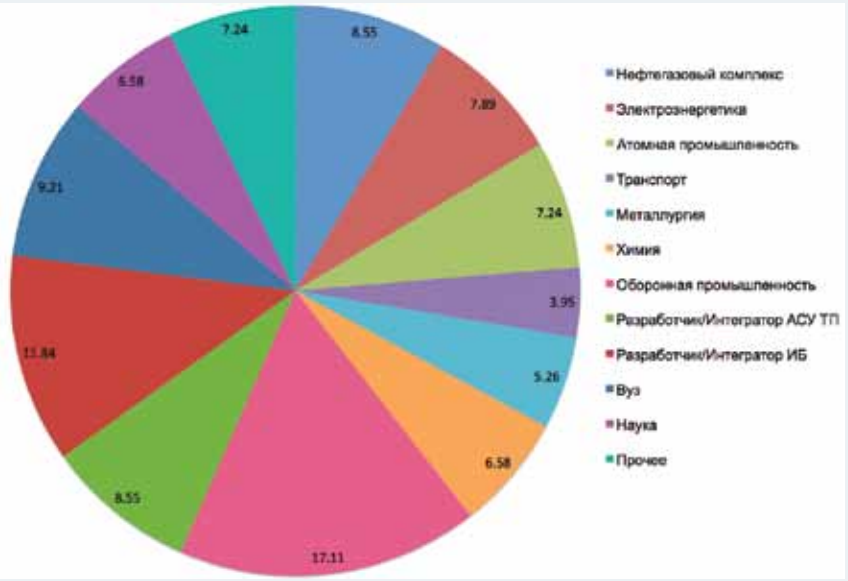
Connect!

Защита необходима всем

Предыдущий год прошел под знаком пандемии, перевода на удаленную работу и окончательного размытия периметра безопасности. За год многое изменилось, в том числе и тенденции развития рынка информационной безопасности. Ставший традиционным опрос участников конференции «Информационная безопасность АСУ ТП критически важных объектов», который мы проводим с 2017 г., показывает, что ситуация с защитой критически важных объектов за год существенно изменилась: если раньше ею интересовались специалисты отдельных отраслей – нефтегазовой и энергетической, то теперь все отрасли, которые отнесены Законом № 187-ФЗ «О безопасности КИИ РФ» к критической информационной инфраструктуре (КИИ), как минимум, приехали на нашу конференцию и ответили на вопросы по защите своих объектов автоматизации.

Вопрос 1. Какую организацию Вы представляете?

Вопрос социально-демографического состава традиционно очень важен для интерпретации результатов анкетирования. В нашем случае ответы на этот вопрос показывают степень заинтересованности специалистов из различных отраслей в информационной безопасности АСУ ТП – основной тематике конференции. В этом году ответы впервые показали равномерное распределение интереса по всем отраслям, в то время как раньше можно было четко выделить лидеров – нефтегазовый комплекс и электроэнергетику. Теперь на пальму первенства претендует оборонно-промышленный комплекс, который в прошлом году был на третьем месте. На третье место вышли вузы, хотя ранее доля их участия была минимальной. Второе место занимают разработчики ИБ-решений для АСУ ТП, их доля всегда была чуть больше 10%

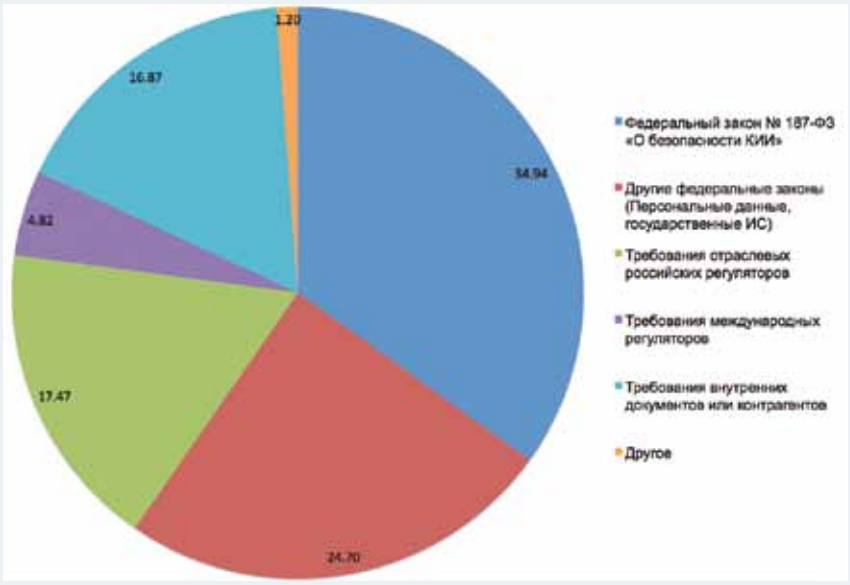


(за исключением прошлого года). Равномерное распределение долей участников различных индустрий подтверждается, в частности, близкими значениями долей нефтегазовый отрасли, электроэнергетики, атомной и химической промышленности, научных заведений. Среди отстающих – только транспорт и металлургия, вероятно, у них специфические требования по безопасности. Демографический состав респондентов позволяет распространить результаты на большинство других индустрий, связанных с КИИ.

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

Ключевым для всех отраслей является Федеральный закон № 187-ФЗ

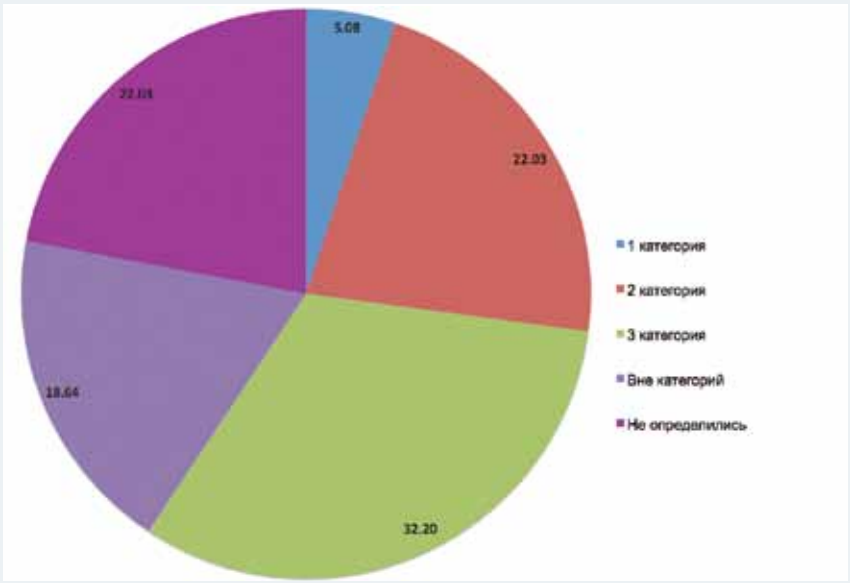
«О безопасности КИИ» – более трети всех ответов связано именно с ним, хотя и другие российские законодательные акты также учитываются при формировании требований к защите промышленных систем – на них приходится почти четверть ответов. Если сравнить эти данные с ответами за предыдущие годы, то заметна тенденция снижения важности требований по КИИ в пользу других законодательных актов. Доля первого минимальна за прошедшие три года, в то время как доля последних уже в течение трех лет неуклонно растет. Плохо, что доля отраслевых актов колеблется в диапазоне 15–20%, что говорит о пассивности отраслевых регуляторов в вопросах обеспечения информационной безопасности. Некоторые из них выпустили свои требования по



ИБ, но остальные ведомства не торопятся следовать примеру лидеров. Доля международных стандартов составляет 5%, что, скорее всего, связано с малой интеграцией российских производственных компаний в международные цепочки кооперации.

Вопрос 3. К какой максимальной категории, по Вашим оценкам, относятся принадлежащие вашей компании объекты КИИ?

Постепенное проведение процедуры категорирования уточняет картину по количеству объектов различных категорий. Последние три года неуклонно снижается доля не определившихся в вопросах категорирования, как и доля объектов вне категорий, – специалисты понимают, что прятаться за вывеской незначимых объектов невыгодно им самим. Естественно, что доля объектов минимальной, третьей категории значимости растет – она составляет почти треть всех ответов. Доля объектов первой и второй категорий остается примерно на одном уровне – 5 и 20%

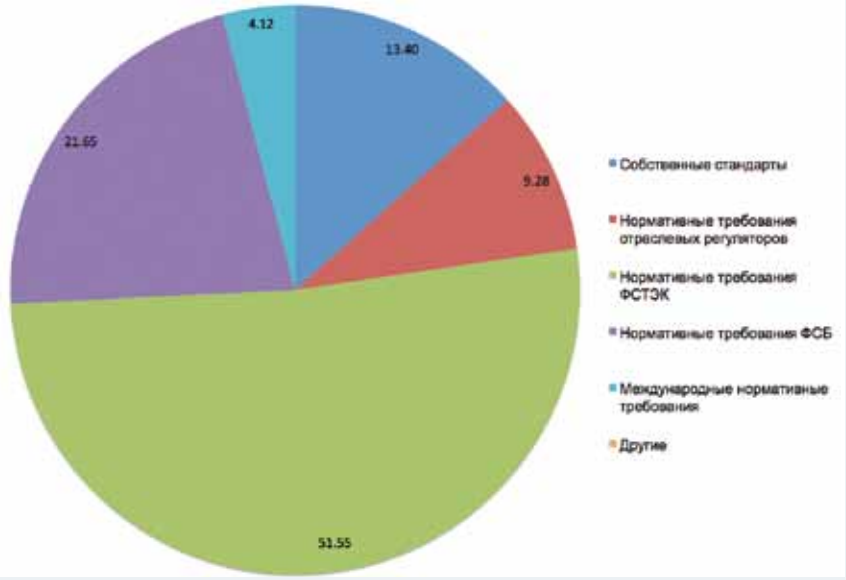


соответственно, что подтверждает гипотезу об отказе субъектов КИИ от «незначимости» в пользу третьей категории – возможно, им так «спокойнее».

Вопрос 4. Какие нормативные акты для вашей организации являются ключевыми при построении системы управления информационной безопасностью?

Такой вопрос мы задали впервые, предполагая, что у большинства субъектов КИИ процедура

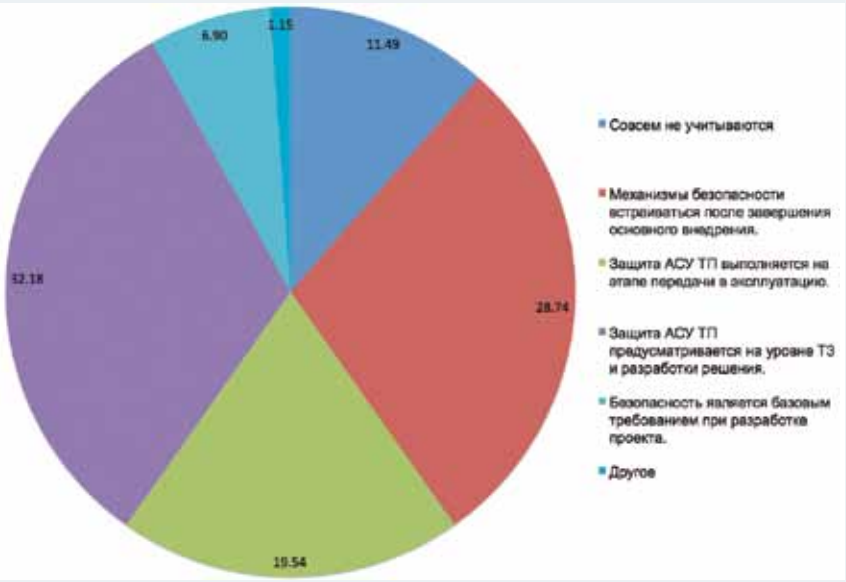
категорирования уже завершена и они должны переходить к следующему этапу – обеспечению защиты. В этом случае ключевым требованием является создание службы управления информационной безопасностью (СУИБ). Нас интересовало, в соответствии с какими требованиями создаются подобные службы. В основном респонденты опираются на требования ФСТЭК к СУИБ. Еще 21,1% соблюдают требования ФСБ – скорее всего, речь идет о взаимодействии с ГосСОПКА и криптографической защите информации. В целом к сфере действия Закона № 187-ФЗ относятся свыше 70% требований. Причем отраслевые регуляторы, такие как Минэнерго и Центробанк, не оказывают существенного влияния на действия ИБ-специалистов промышленных предприятий. Получается, что сами компании лучше разбираются



в отраслевой специфике защиты своих решений, чем отраслевые регуляторы. Показательна также нулевая доля ответов для пункта «Другие» – это означает, что СУИБ строят все-таки по стандартам, а не спонтанно и не на коленке.

Вопрос 5. Насколько, по Вашим оценкам, вопросы информационной безопасности учитываются в проектах цифровизации современных производств?

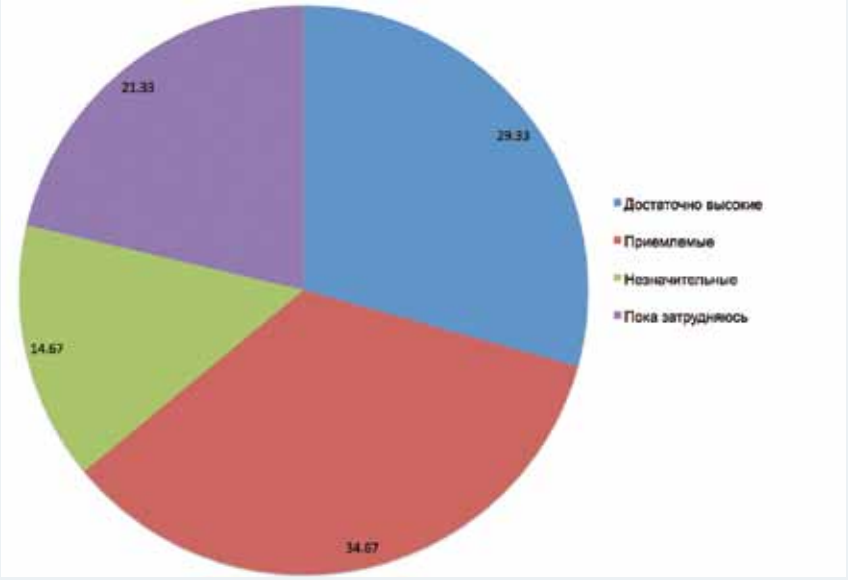
Достаточно часто (практически в одном из трех проектов) требования по информационной безопасности закладываются на уровне ТЗ, что является следствием принятия Закона № 187-ФЗ, поскольку, скорее всего, пункт ТЗ в данном случае звучит так: «Полностью соответствовать требованиям федеральных законов». Второй по популярности ответ – «Механизмы безопасности встраиваются после завершения основного внедрения» – показывает, что так было не всегда. Проекты, которые стартовали раньше, подобного требования на уровне ТЗ не имели, и теперь компаниям приходится доделывать уже работающие системы. При этом



доля проектов по цифровизации, в которых безопасность совсем не учитывается, незначительная – чуть больше 10%. Менее популярным оказался только ответ, что именно безопасность стала базовым элементом проекта по цифровизации.

Вопрос 6. Как Вы оцениваете затраты на выполнение требований по защите АСУ ТП как части КИИ предприятия? Например, как долю от всего ИБ-бюджета предприятия?

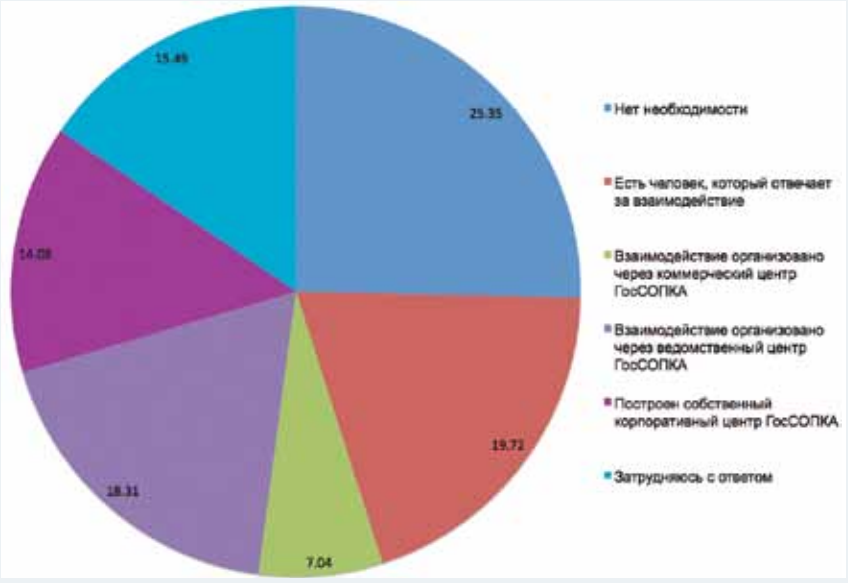
Этот вопрос мы задаем в опросе с 2018 г., и до 2020-го тенденция была очевидна: доля ответов «достаточно высокие» неуклонно росла, «незначительные» – падала, а «приемлемые» – составляла примерно 27%. Однако 2021 г. продемонстрировал неожиданную тенденцию. Доля «приемлемых» ответов неожиданно увеличилась – до 34,7%, а пункты «достаточно высокие» и «незначительные» вернулись на уровень 2018 г. Видимо, данные за 2018 г. относились к тому случаю, когда об обеспечении безопасности еще не думали, поэтому и расходы на информационную безопасность были незначительными. Когда же требования Закона № 187-ФЗ начали вступать в силу, компаниям пришлось раскошелиться на построение защиты.



Теперь же, когда защита уже построена, расходы возвращаются в привычное русло. Впрочем, возможна и другая причина: про безопасность во время пандемии немного забыли, поэтому оценка расходов на нее снизилась. При этом доля затрудняющихся с ответом оставалась стабильной – на уровне 21%.

Вопрос 7. Как у вашей компании организовано взаимодействие с ГосСОПКА?

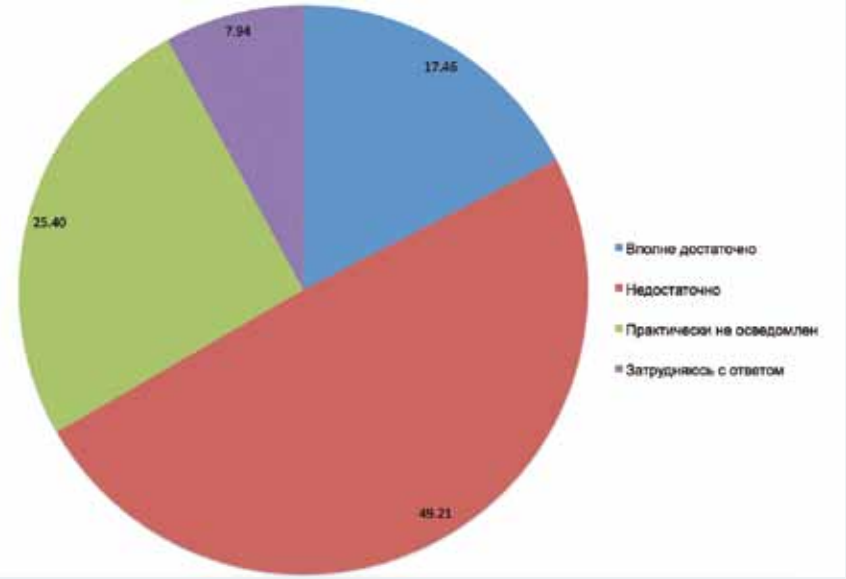
ГосСОПКА – часть инфраструктуры контроля за соблюдением законодательства в части защиты КИИ. Все значимые объекты КИИ должны взаимодействовать с этой инфраструктурой, хотя и остальным такое подключение не запрещено. Фактически ГосСОПКА – это государственный источник фидов, требующий передачи собственных сообщений об инцидентах. Однако то, что он находится под контролем ФСБ России, видимо, многих отпугивает – около четверти респондентов не хотят иметь с ней дела. В то же время 19,7% опрошенных организаций, как минимум, имеют человека, который взаимодействует с указанной инфраструктурой. Наиболее популярными



каналами такого взаимодействия являются ведомственные центры реагирования – здесь существенна роль отраслевых регуляторов. Еще 14,1% построили собственный центр реагирования, который передает все необходимые данные в ГосСОПКА. И только 7,0% пользуются услугами коммерческих центров реагирования. Таким образом, коммерческие центры ГосСОПКА имеют большие перспективы развития.

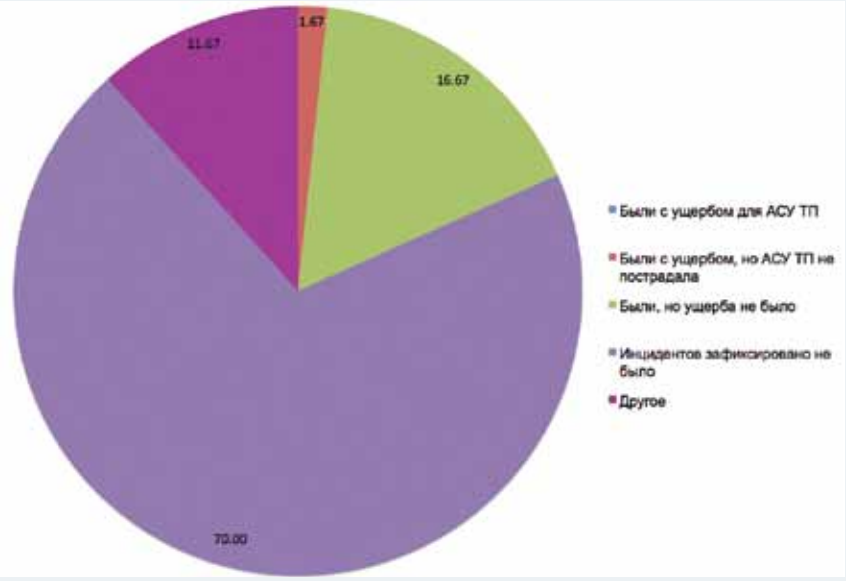
Вопрос 8. Как Вы оцениваете уровень осведомленности персонала вашего предприятия в области защиты АСУ ТП как части КИИ?

Однозначную тенденцию по ответам обнаружить сложно. Доля ответа «недостаточно» составляет около 50%, а количество тех, кто считает свой персонал практически неосведомленным в вопросах безопасности КИИ, неуклонно растет, и в этом году она достигла 25,4%. Доля удовлетворенных осведомленностью своего персонала в вопросах защиты ключевых промышленных систем колеблется от 15 до 33%. Текущее значение показателя в 17,5% из этого диапазона не выходит, хотя и приближается к нижнему пределу. В прошлом году неудовлетворенных было 27,5%. Видимо, за несколько лет внедрения Закона № 187-ФЗ персонал все-таки сумел доказать свою компетенцию в вопросах защиты АСУ ТП.



Вопрос 9. Были ли у вашего предприятия или холдинга инциденты информационной безопасности?

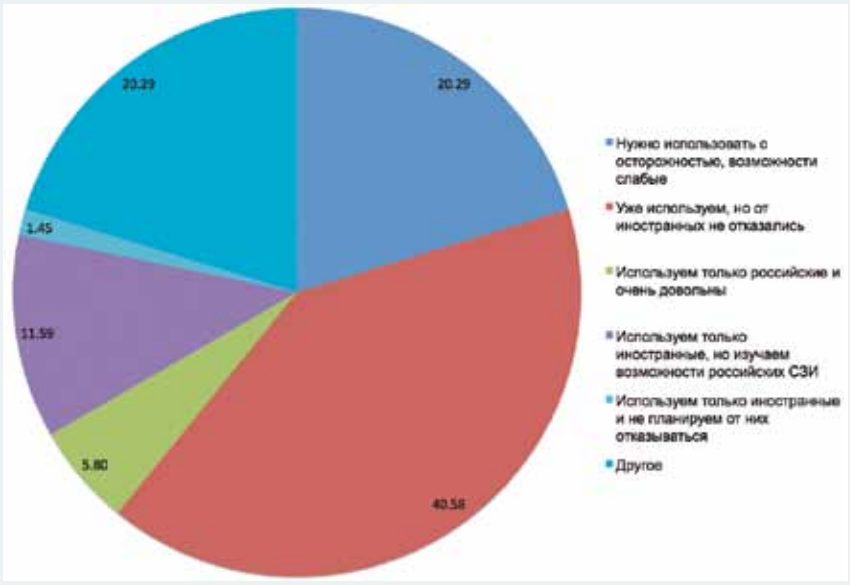
Служба безопасности призвана защищать предприятие от нападений. Поэтому если у ее специалиста спросить: «Были ли у тебя проблемы?», он, разумеется, ответит «нет». Самый близкий к такому варианту ответ – «инцидентов зафиксировано не было». Так ответили 70% респондентов. Скорее всего, это говорит о том, что служба ИБ не фиксирует мелкие инциденты, которые в дальнейшем можно было бы использовать для расследования сложных сценариев атаки. Чтобы продемонстрировать отсутствие проблем, лучше подходит другой ответ: «были, но ущерба не было» – его выбрали всего 16,7% опрашиваемых. Он означает, что служба ИБ в курсе всех нарушений, но реальных проблем не допускает. Естественно, признаваться в проблемах никто не хочет, хотя опрос анонимный и никаких данных по конкретному предприятию мы не собираем. Тем не менее в этом году доля заявивших о реальных проблемах была минимальной за все время проведения опросов. Впрочем, можно предположить, что отсутствие инцидентов является следствием реализации требований закона «О безопасности КИИ».



Вопрос 10. Как Вы оцениваете возможности российских средств защиты информации в части обеспечения безопасности АСУ ТП с учетом возможного вступления

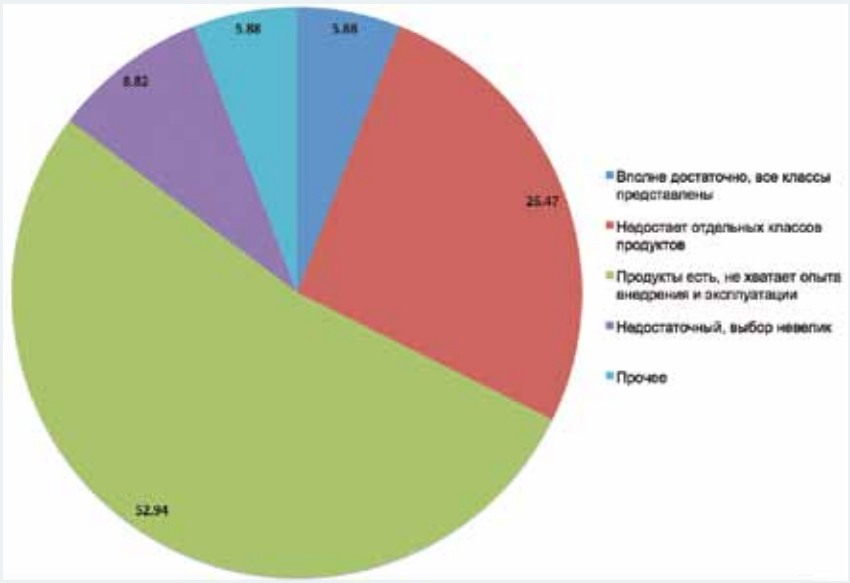
законодательных ограничений в 2022 г.?

Аналогичный вопрос задавали и в прошлом году, хотя и без ссылок на давление по импортозамещению со стороны регулятора. Доля тех, кто считает, что российским продуктам доверять не стоит, немного увеличилась – с 18,4 до 20,3%. Вариант, предполагающий приоритет российского, но без отказа от иностранного, в этом году выбрали 40,6% ответивших. При этом доля довольных российскими решениями сократилась практически вдвое, впрочем, как и ярых сторонников иностранного, – с 3,2 до 1,5%. В то же время увеличилась доля тех, кто рассматривает российские решения как возможную альтернативу, – с 8,4 до 11,6%. Таким образом, политика импортозамещения дает свои плоды, хотя этот процесс идет довольно медленно. Приходится преодолевать одну из самых прочных преград – психологическую.



Вопрос 11. Как Вы оцениваете ассортимент представленных на рынке продуктов и услуг по безопасности АСУ ТП?

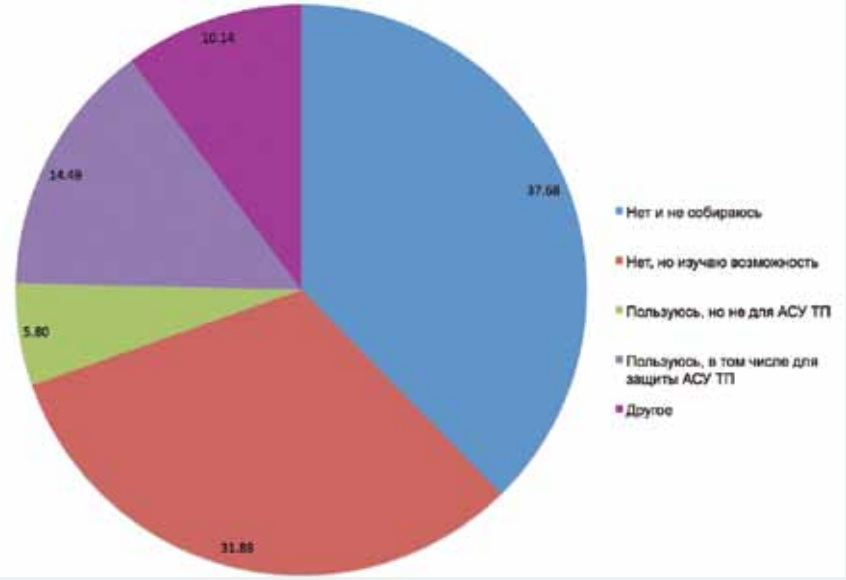
Данный вопрос связан с доступностью для российских пользователей современных технологий защиты. Следует отметить, что импортозамещение эту доступность несколько снижает. Однако более половины (52,9%) считают, что продуктов-то достаточно, но опыта их использования маловато. Чуть более четверти респондентов все-таки не очень довольны существующим в России выбором средств защиты. Доли ответов «вполне достаточно, все классы представлены» и «недостаточный, выбор невелик» в последние три года синхронно снижаются. Похоже, специалисты начинают понимать, что им реально нужно для работы, и осознают основную свою проблему – отсутствие опыта. Во всяком случае, доля респондентов, которым недостаточно какого-то одного класса продуктов, увеличивается.



Вопрос 12. Пользуетесь ли вы услугами аутсорсинга в области ИБ?

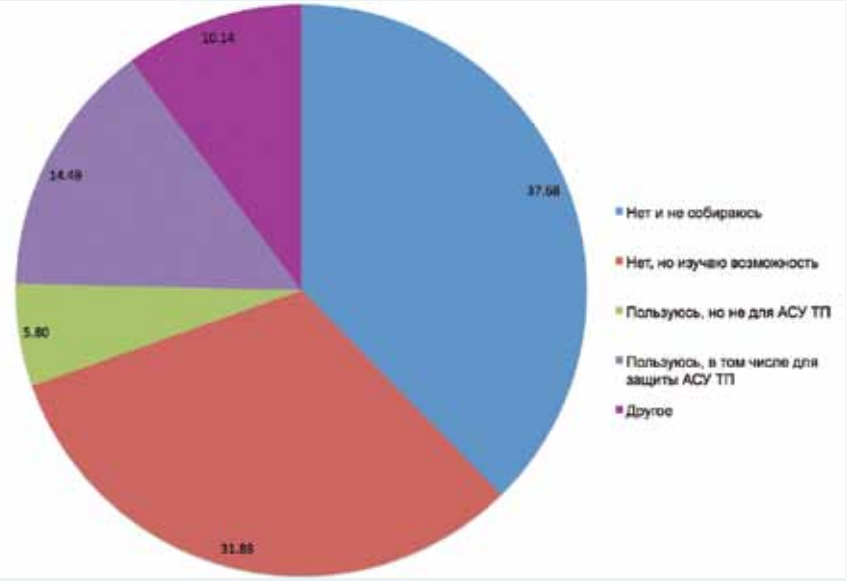
В прошлом году лидером стал ответ «нет, но изучаю возможность». В 2021-м на первом месте оказался ответ «нет и не собираюсь». При этом в целом аутсорсингом безопасности

пользуется практически пятая часть респондентов, однако данный показатель снижается – в прошлом году доля пользователей аутсорсинга составляла 28,1%. Показательны в связи с этим ответы на предыдущий вопрос: «Собственных компетенций по использованию средств защиты не хватает, но аутсорсингом качественных специалистов мы пользоваться все равно не будем». В обсуждении седьмого вопроса мы говорили, что коммерческие центры реагирования имеют большие перспективы, повторим это еще раз. Если компании, предоставляющие услуги аутсорсинга ИБ, не убедят потенциальных клиентов в своей компетентности, надежности и безопасности, то они так и останутся нишевыми игроками на рынке ИБ.



Вопрос 13. Насколько хорошо Вам знаком опыт предприятий, подобных вашему, в области защиты АСУ ТП?

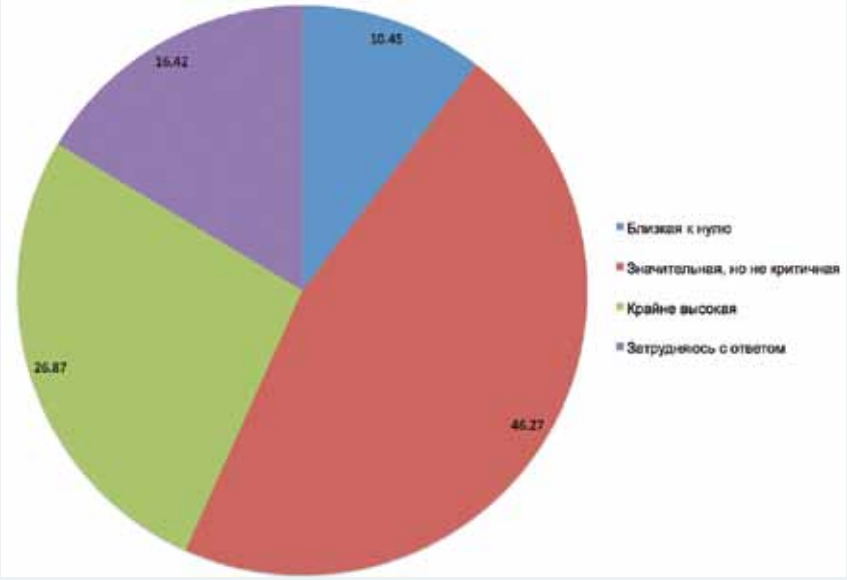
Этот вопрос мы задаем с самого первого опроса с целью показать необходимость нашей конференции, где как раз и происходит обмен опытом внедрения и эксплуатации различных инструментов защиты. Ответ «известен, но примеров мало» всегда был лидером – в этом году его доля чуть более половины. Следует отметить, что анкетирование проводится до начала конференции, таким образом, примеры, которые разбираются в рамках мероприятия, в отчет не попадают. Доля ответов «неизвестен вообще» традиционно не превышает 10%. В этом году она оказалась самой большой за все время проведения опроса.



Вопрос 14. Как Вы оцениваете в свете последних событий вероятность возрастания риска безопасности КИИ со стороны иностранных государств?

Этот вопрос был задан впервые, чтобы выяснить, насколько специалисты по информационной безопасности промышленных предприятий готовы участвовать в международных конфликтах. Минимальной оказалась доля тех, кто считает незначительной вероятность иностранного вмешательства в российскую критическую инфраструктуру, – всего 10,5%. Лидером стал ответ «значительная, но не критичная», который показывает, что российские

ИБ-специалисты не сбрасывают со счетов наиболее опасных противников – разведки иностранных государств, но при этом надеются от них защититься. Достаточно велика и доля тех, кто концентрирует свое внимание на защите именно от этих угроз, – таких чуть больше четверти. Однако при управлении защитой предприятия стоит соблюдать баланс между защитой от наиболее массовых атак и целенаправленного вмешательства иностранных спецслужб. Важно не забывать об этой угрозе, но искать иностранное вмешательство нужно без фанатизма.



Заключение

В целом по результатам опроса можно отметить переход от поголовного категорирования к построению комплексной защиты промышленных предприятий. Если раньше наблюдался интерес конкретных отраслей промышленности к решению вопросов информационной безопасности, то сейчас безопасность является одним из ключевых требований дальнейшего развития практически всех отраслей – она становится частью стратегии цифровизации. Во всяком случае, достаточно большая доля проектов дигитализации включает требования по защите в техническое задание еще при разработке. Кроме того, налаживается взаимодействие промышленных предприятий с выстроенной государством системой реагирования на инциденты – ГосСОПКой. Большинство участвующих в опросе предприятий так или иначе уже наладили обмен информацией с этой инфраструктурой, что говорит о достаточно высоком уровне зрелости служб информационной безопасности.

Среди проблем можно отметить слабое развитие аутсорсинга при недостаточной осведомленности персонала в вопросах информационной безопасности. Хотя коммерческие центры реагирования на инциденты сейчас активно продвигают свои услуги, специалисты по защите промышленных информационных систем почему-то не очень им доверяют: доля тех, кто не собирается пользоваться услугами аутсорсинга, растет, при том что во время прошедшей пандемии большинство компаний оценили удобство и гибкость облачных услуг. Кроме того, потребность в квалифицированных кадрах по защите промышленных систем сегодня достаточно высока, и именно их сейчас аккумулируют аутсорсинговые компании. На рынке аутсорсинга услуг по защите промышленных объектов наступает удачный момент для активного развития.

Следует отметить, что специалисты по ИБ промышленных предприятий считают достаточно высоким риск атак со стороны иностранных государств, что в целом подогревает интерес к процессам импортозамещения и безопасной разработки. Судя по всему, российскими средствами защиты уже научились пользоваться, хотя некоторых функций в них все-таки не хватает. Можно предположить, что это функции автоматизации, удобства и интеграции, поскольку по этим критериям иностранные продукты по-прежнему опережают российские. Однако именно автоматизация и интеграция, особенно с иностранными облачными сервисами, и вызывают все большую озабоченность со стороны служб ИБ. Если российским производителям удастся предложить промышленным компаниям контролируемые, эффективные и в то же время удобные в эксплуатации решения для построения комплексной системы защиты предприятия, то они имеют шанс вытеснить с рынка иностранные продукты. ■