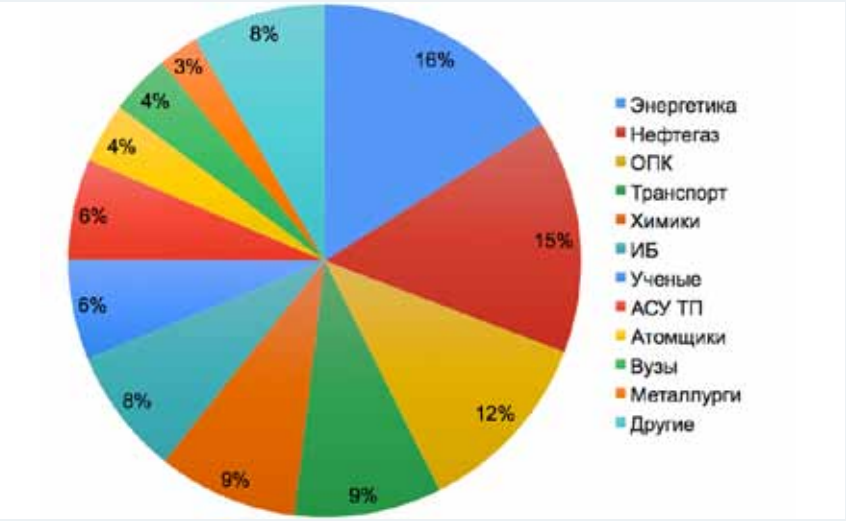
На пути к промышленной защите

Прошедший год в сфере информационной безопасности промышленных объектов был посвящен в основном категорированию объектов КИИ. Этот процесс, похоже, в массе своей подходит к концу – большинство промышленных предприятий уже определились с категориями своих объектов, оценили все перечисленные в процедуре категорирования типы ущерба и зарегистрировали соответствующие акты во ФСТЭК. Поэтому в текущем году наш опрос в рамках восьмой конференции «Информационная безопасность АСУ ТП критически важных объектов» был немного изменен с целью оценить состояние рынка информационной безопасности после завершения процесса категорирования. Были добавлены вопросы по методическим материалам Закона № 187-ФЗ, по типу ущерба, по импортозамещению и аутсорсингу – современным показателям рынка. Наиболее общие вопросы не подверглись коррекции, чтобы иметь возможность оценить динамику изменения ответов со временем.

Вопрос 1. Какую организацию Вы представляете?

Общее количество ответов – 211.

Демография опроса важна для понимания остальной части опроса. Если в опросе прошлого года доля производителей ИБ и АСУ ТП была достаточно большой – 14,9 и 12,9%, т. е. на уровне лидирующих индустрий, то в 2020 г. их доля существенно уменьшилась – до 8,0 и 6,3% соответственно. Это при том, что представители лидирующих индустрий увеличили свою долю в опросе: электроэнергетики – до 16,0% (было 14,9%), нефтегаза – до 14,8% (было 10,8%). Неожиданно на третье и четвертое место в опросе попали оборонная промышленность и транспорт, доля которых в прошлых обзорах была минимальной – 4,6 и 2,6%, а в 2020 г. резко увеличилась до показателей в 11,8 и 9,3%.



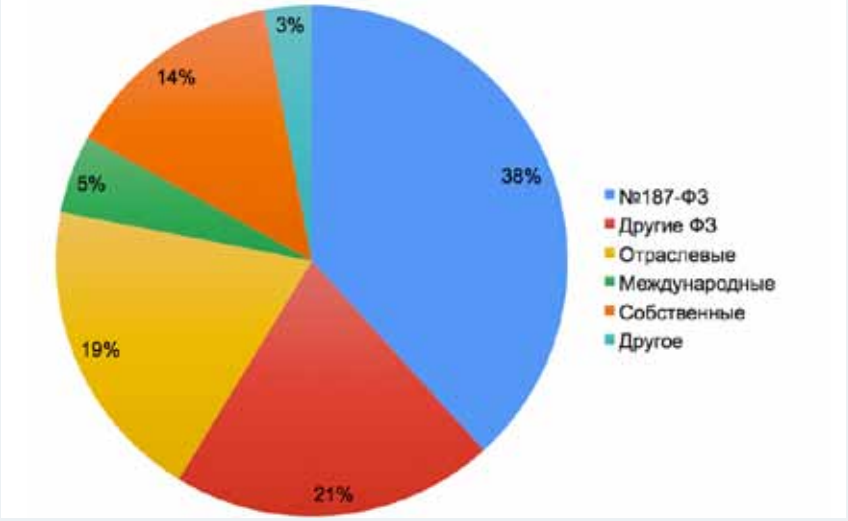
На пятом месте оказались химики, которые в прошлом году вырвались даже на четвертое с долей в 11,9%, но сейчас количество их ответов сократилось до 8,9%. В результате оказалось, что на пяти первых местах по ответам оказались представители промышленных отраслей. В этом году также продолжился рост доли ответов «Другое», где вполне могут быть представители индустрий, не связанных с промышленностью, но отнесенных к критическим – банки, государственные компании и операторы связи. В прошлом году их доля составляла 7,7%, а в текущем увеличилась до 8,4%.

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

Общее количество ответов – 211.

Нормативные акты сейчас являются одним из важнейших движущих факторов формирования культуры защиты базовых

функций АСУ ТП, потому было интересно исследовать, какие именно документы влияют на это развитие. В прошлом году мы впервые задали данный вопрос, поэтому уже можно определить динамику влияния законотворчества. Оказалось, что растет доля влияния Закона № 187-ФЗ (с 36,2 до 38,3%), других федеральных законов (с 19,5% до 20,4%) и отраслевых документов (с 16,7 до 19,4%), а вот международные и собственные документы теряют влияние с 7,7 до 4,9% и с 16,4 до 14,0% соответственно. Больше всего выросло именно отраслевое регулирование – ведомства наконец разобрались в структуре Закона № 187-ФЗ и начали выпускать свои отраслевые стандарты

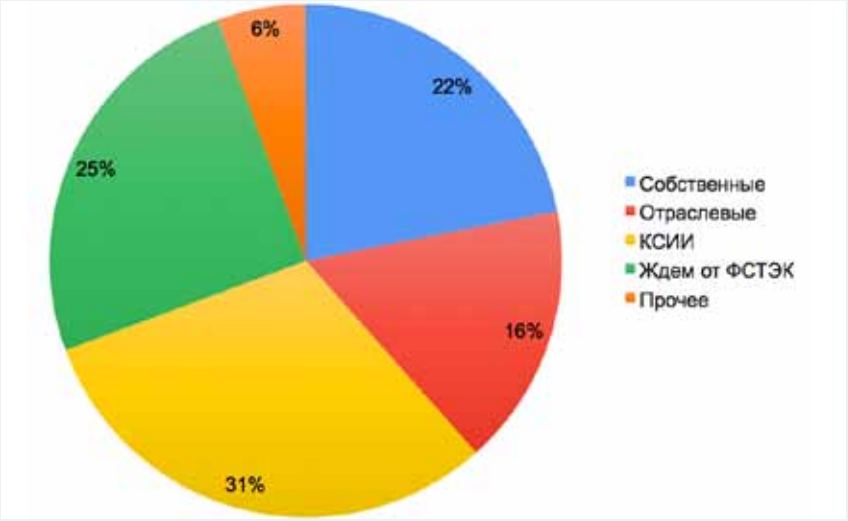


и рекомендации по категорированию и обеспечению защиты. Собственно, именно к такому распределению ответственности и стремился ФСТЭК с самого начала.

Вопрос 3. Какие методические материалы вы используете для исполнения требований Закона № 187-ФЗ?

Общее количество ответов – 211.

В прошлом году мы выясняли, насколько понятны требования законодательства. Оказалось, что большинство респондентов разобрались с ними. В текущем году было решено уточнить, какие именно материалы использовались. Значительная часть ответивших (30,9%) пользуются старыми документами по защите ключевых систем информационной инфраструктуры (КСИИ). Но поскольку эти рекомендации являются старыми, то довольно часто отвечающие выбирали дополнительно пункт «Ждем рекомендаций от ФСТЭК» (25,1%). На третьем месте находятся собственные разработки



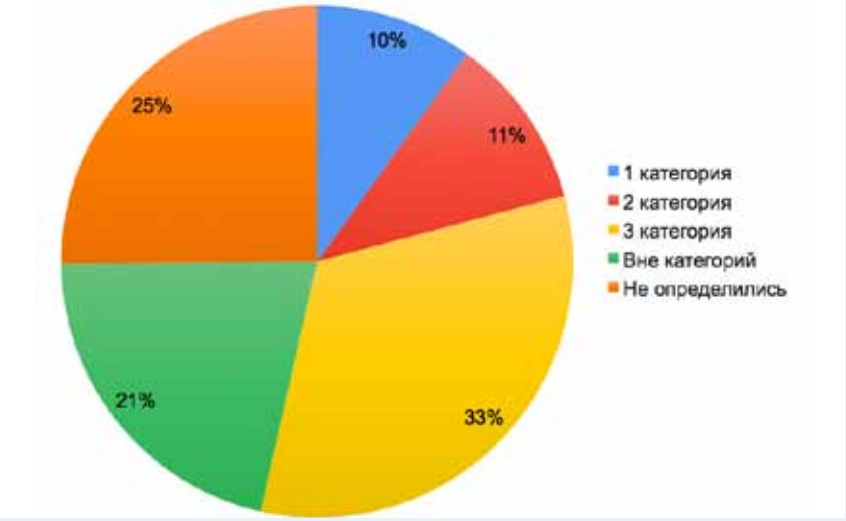
компаний (21,9%). То есть компаниям приходится самостоятельно разрабатывать процедуры для проведения категорирования, оценки соответствия и проектирования систем управления ИБ. К сожалению, меньше всего пользуются отраслевыми рекомендациями – 16,5%, хотя именно по такому пути предполагалось развитие всей регуляторики, связанной с КИИ: ФСТЭК дает лишь общие рекомендации, а отраслевые регуляторы уточняют особенности для подконтрольных организаций.

Вопрос 4. К какой максимальной категории, по вашим оценкам, относятся принадлежащие вашей компании объекты КИИ?

Общее количество ответов – 211.

В предыдущих опросах задавался другой вопрос: «Есть ли у вас предварительное понимание, к какой категории преимущественно относятся ваши объекты КИИ?». Это было связано с тем,

что большинство компаний год назад еще не прошли процедуру категорирования и не могли точно сообщить о присвоенной категории. Предварительные оценки распределились так: практически три четверти заняли ответы: «Третья категория», «Вне категорий» и «Не определились», а последняя четверть была поделена между первой и второй категориями в пропорции примерно один к четырем. Реальность оказалась несколько другой. Как показал опрос, между первой и второй категориями наблюдается примерный паритет: 10,0 против 10,9% соответственно. Третья категория была присвоена почти трети всех компаний (точнее 32,7%), а пятая часть (21,3%) оказалась вне категорий. При этом доля неопределившихся осталась примерно на прежнем

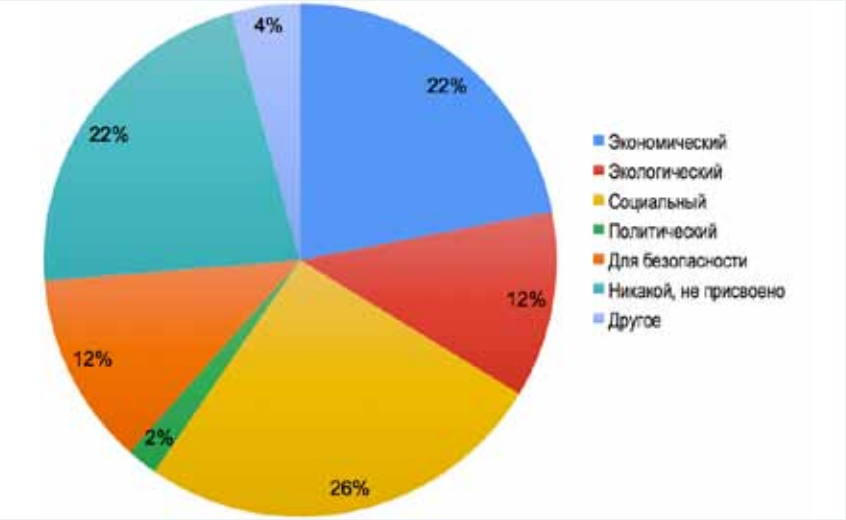


уровне – 25,1%. Такое резкое изменение результатов можно объяснить изменением демографии опроса: в этом году на вопросы отвечали в основном представители промышленности, а в прошлом доля производителей АСУ ТП и ИБ была достаточно высокой, что и вносило искажения в представления о категориях промышленных объектов.

Вопрос 5. Какой тип ущерба для вас определил категорию объекта (был максимальным)? Допустим альтернативный ответ.

Общее количество ответов – 211.

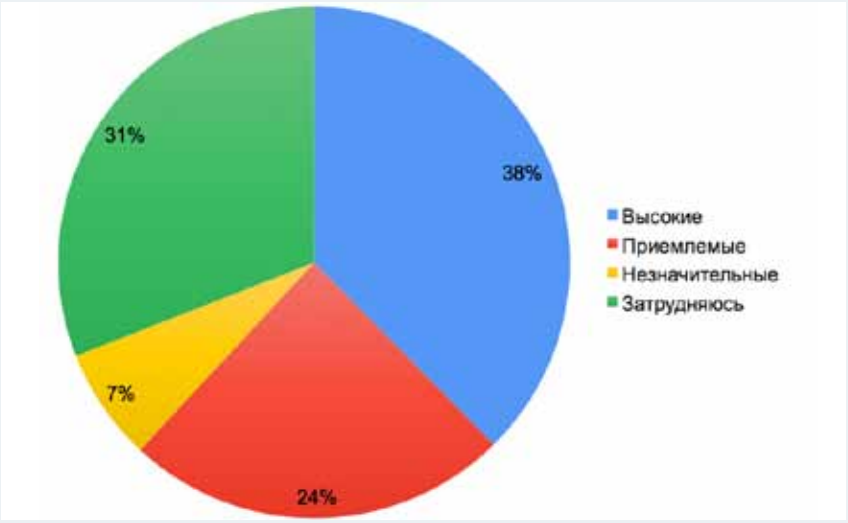
Ранее данного вопроса не было, поскольку моделирования угроз как часть категорирования у большинства проведено не было. Но в этом году было решено его ввести. В результате оказалось, что для промышленности наиболее популярным является ущерб социальный, который привязан к территориальным образованиям, – его назвали 25,9% опрошенных. Чуть менее значимый показатель экономический – его назвали 22,0%. Еще два менее значимых показателя – ущерб для безопасности и экологическая опасность, которые определили категорию для 12,2 и 11,8% соответственно.



Естественно, на последнем месте располагается политический ущерб, который назвали всего 2% ответивших. При этом чуть больше четверти тех, кто не определился с категориями и, естественно, не может определить максимального ущерба ни по одной категории, что примерно соответствует результатам ответов на предыдущий вопрос. По полученным результатам можно сделать вывод, что взлом промышленных систем может иметь в основном социальные и экономические последствия, а не политические.

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?

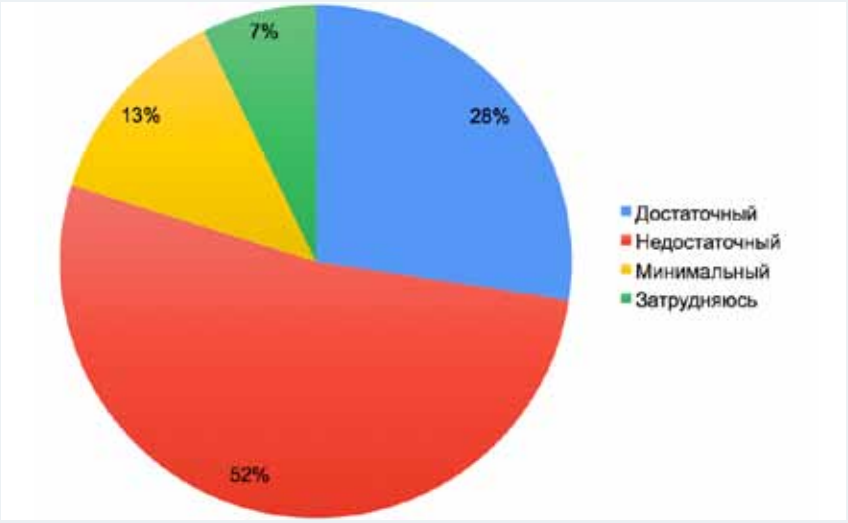
Общее количество ответов – 210.



Вопрос по оценке стоимости удовлетворения требований законодательства задавался уже несколько лет, и за все время доля ответа «Высокие» только увеличивалась – 28,0% в 2018 г., 35,4% в 2019 г. и 37,6% в 2020 г. Доля ответов «Приемлемо», два предыдущих года державшаяся на отметке около 29%, уменьшилась до 24,3%, а ответы «Незначительные» продолжили сокращение – 21,5% в 2018 г., 13,9% в 2019 г. и всего 7,1% в текущем году. В то же время два года подряд доля тех, кто затруднялся с ответом, была на уровне 21%, а в этом году существенно увеличилась – до 31,0%. Так что, по мере того как промышленность разбирается с требованиями по информационной безопасности, оценка ресурсоемкости принимаемых мер только увеличивается. С другой стороны, понятно, что расходы на информационную безопасность – это плата за экономию, которая достигается в результате цифровой трансформации и реализации концепции «Индустрия 4.0».

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

Общее количество ответов – 208.



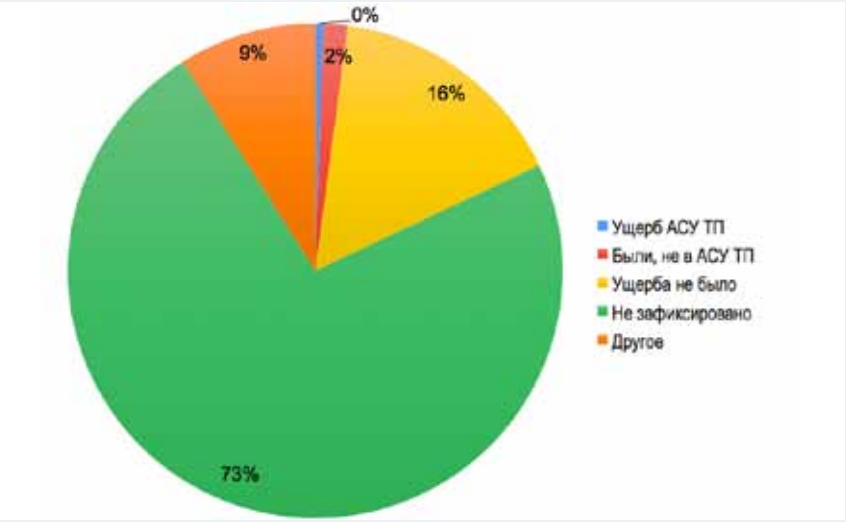
Этот вопрос также задается уже не первый год, и понятную динамику показывает только ответ «Достаточный» – его доля в 2018 г. была 15,7%, в 2019 г. – 23,5%, а в текущем увеличилась до 27,4%. Доля ответа «Недостаточный» составляет примерно 50%. В текущем году он зафиксировался на отметке в 52,4%, но его движения в предыдущие годы были разнонаправлены. Количество ответов «Минимальный» в 2020 г. уменьшилось до 13,0%, хотя еще в прошлом году их было 19,3%. Тенденцию к сокращению продолжила и доля тех, кто затруднился с ответом, – их стало 7,2%, хотя за год до этого названный показатель снизился до 9,7%. Фактически это означает, что уровень осведомленности постепенно повышается, поскольку сотрудники ИБ и персонал, обслуживающий АСУ ТП, понимают свои права и обязанности. Причем правила безопасности утверждаются на уровне организационно-распорядительной документации субъектов КИИ.

Вопрос 8. Были ли у вашего предприятия или холдинга в 2019 г. инциденты информационной безопасности в части АСУ ТП?

Общее количество ответов – 189.

Наиболее популярный ответ – «Инцидентов зафиксировано не было» (его выбрали в этом году 73,0% респондентов,

в прошлом – 54,5%) – фактически означает, что службы не видят инцидентов, т. е. мониторинг либо не работает, либо плохо настроен. Инциденты в реальных условиях есть всегда, но при правильной организации работы они не перетекают в атаки и не приносят ущерба. Поэтому более правильным ответом был бы такой: «Были, но ущерба не было». В прошлом году такой ответ был достаточно популярен – его выбрали 30,3% ответивших, но в текущем его доля значительно уменьшилась – до 15,9%. Подобная тенденция показывает, что специалисты больше заботятся о бумажной безопасности и формально «непробиваемой» защите, а не о выстраивании системы эффективной обработки инцидентов и совершенствования СУИБ. В то же время доля инцидентов с реальным ущербом пока не очень большая: без ущерба для АСУ ТП – 1,6%,

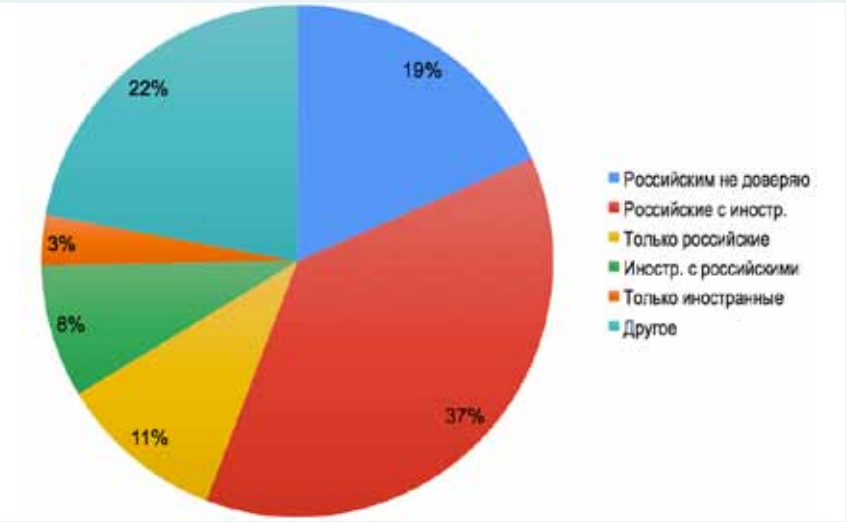


а с ущербом для промышленной сети – всего один случай (доля около 0,5%, т. е. на уровне погрешности опроса). Конечно, в опросах этот показатель обычно занижают и просто не отвечают на вопрос, но все равно можно говорить о довольно низком уровне реальной угрозы для АСУ ТП, но только с учетом того, что далеко не все качественно мониторят ситуацию с реальной безопасностью промышленной сети. Правда, реагирование на реальную атаку, которая привела к последствиям, не заметить для специалистов по ИБ предприятия довольно сложно.

Вопрос 9. Как Вы оцениваете возможности российских средств защиты информации в части обеспечения безопасности АСУ ТП?

Общее количество ответов – 190.

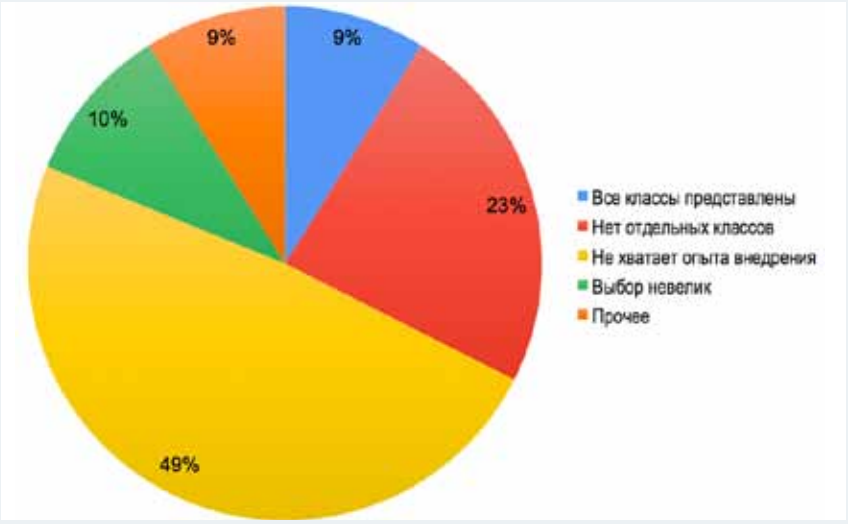
Данный вопрос был добавлен для оценки процесса импортозамещения в информационной безопасности промышленных систем. Наиболее популярным ответом является приоритет российских продуктов, но с сохранением иностранных продуктов – 37,4%. На втором месте оказался подход, при котором российским продуктам не доверяют защиту АСУ ТП. На третьем месте подход, при котором используются только российские продукты, – 10,5%. Доля представителей ОПК чуть больше – 11,8%. Поскольку для предприятий указанной отрасли действуют особые условия использования



иностранных продуктов, эта доля покажется даже маленькой. Подход, при котором для защиты АСУ ТП используют в основном иностранные продукты, но присматриваются к российским, не очень популярен – его доля составляет 8,4%. Минимум ответов получил подход, при котором применяются только иностранные продукты, – 3,2%. Если сложить доли тех, кто предпочитает российские средства защиты, то их окажется 47,9%, в то время как приверженцев иностранной продукции 30,0%, таким образом, плоды стратегии импортозамещения налицо.

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

Общее количество ответов – 191.

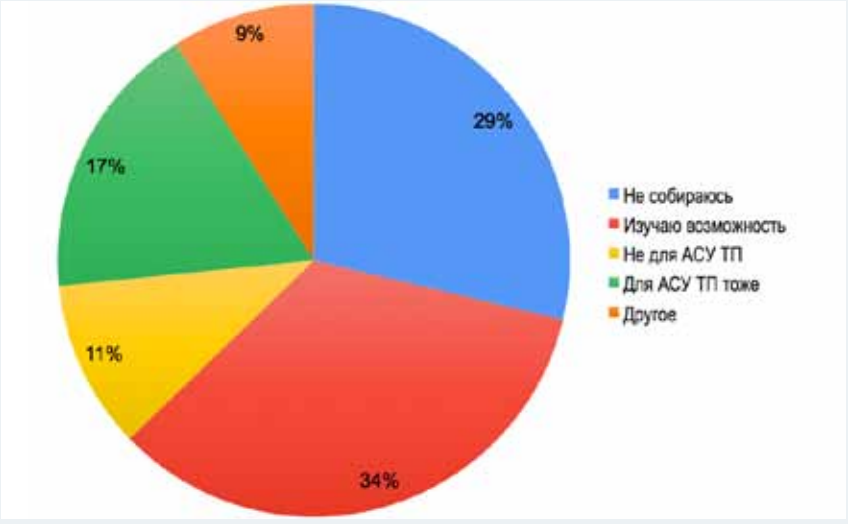


Оценку ассортимента продуктов и услуг мы проводим уже не первый год, и за все время доля тех, кто удовлетворен выбором средств защиты, неуклонно сокращается. В этом году она достигла отметки в 8,9%, хотя еще в прошлом была значительно больше – 16,0%. Однако и доля тех, кто не удовлетворен ассортиментом (ответ «Недостаточный, выбор невелик»), сократилась с 22,7% в прошлом году до 9,9%, т. е. примерно так же, как и доля удовлетворенных. Наиболее популярным ответом, как и в прошлом году, стал «Продукты есть, не хватает опыта внедрения и эксплуатации» с долей в рекордные 48,7%. В прошлом году этот показатель составлял 34,0%.

Доля тех специалистов, которым недостает отдельных классов продуктов, остается практически на уровне прошлого года: в текущем – 23,6%, в прошлом – 22,0%. Фактически это означает, что на рынке информационной безопасности появилось большое количество работников, которые имеют не очень богатый опыт внедрения и эксплуатации средств защиты, поэтому они не могут сориентироваться, достаточен ассортимент или нет, – доли обоих ответов значительно уменьшились. Это говорит о том, что средства защиты АСУ ТП нужно делать не только более специализированными по функциональности, но и более удобными для освоения начинающими кадрами.

Вопрос 11. Пользуетесь ли вы услугами аутсорсинга в области ИБ?

Общее количество ответов – 188.

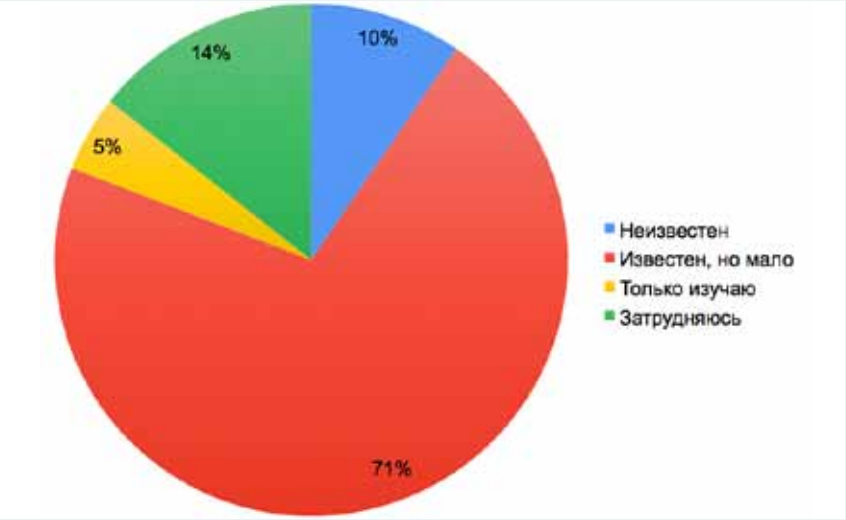


Аутсорсинг – относительно новая тема для защиты, особенно в области АСУ ТП, поэтому было решено оценить популярность таких услуг у российских промышленных предприятий. Интерес к этому рынку связан с тем, что сейчас завершился этап категорирования и компании должны приступать к построению эффективных систем защиты. Самый быстрый и менее затратный способ – отдать обслуживание ИБ на аутсорсинг. Те, кто пошел по этому пути (17,6%), сообщили, что пользуются аутсорсингом ИБ, в частности, для защиты АСУ ТП. Еще 10,6% пользуются, но не для АСУ ТП. Таким образом, уже сейчас чуть больше четверти промышленных компаний пользуются услугами аутсорсинга ИБ. Еще 34,0% респондентов сказали, что изучают возможность использования аутсорсинга управлением средств защиты. Это достаточно большое количество будущих клиентов коммерческих SOC. Впрочем, и пессимистов использования аутсорсинговых услуг по информационной безопасности довольно много – 28,7%. Таким образом, количество специалистов, у которых аутсорсинг ИБ

не вызывает отторжения, больше половины – 62,2%. Это позволит в ближайшем будущем расширить рынок коммерческих SOC, правда, при условии, что они предоставят удобные услуги по дистанционному управлению защитой промышленных информационных систем.

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

Общее количество ответов – 188.



Среди профессионалов в области защиты информационной безопасности сформировалось устойчивое сообщество: подавляющее большинство (71,3%) ответили, что опыт коллег им известен. В прошлом году их было меньше – 61,1%. При этом резко уменьшилась доля тех, кому опыт коллег не очень известен, – в прошлом году она составляла 23,0%, а в текущем сократилась до 9,6%. Специалистов, которые только начинают изучать рынок, не очень много – 4,8 в этом году против 6,5% в прошлом. Однако увеличилась доля тех, кто затрудняется с ответом, – 14,4%, хотя в прошлом году их было 9,4%. Таким образом, можно констатировать, что обмен опытом обеспечения безопасности объектов АСУ ТП налаживается, большинство специалистов устанавливают горизонтальные каналы взаимодействия со своими коллегами.

Заключение

По результатам опроса можно сделать вывод о том, что промышленные предприятия наконец заинтересовались задачей обеспечения информационной безопасности промышленных сегментов сетей. Об этом говорит и внимание к самой конференции ИБКВО, в рамках которой проводился опрос, со стороны представителей промышленности, и значимость законодательства по КИИ при проектировании систем защиты, и возрастающая популярность российских средств защиты АСУ ТП, и достаточно высокий уровень доверия клиентов к аутсорсингу защиты своих промышленных сетей. Категорирование не прошло даром: операторы КИИ провели инвентаризацию своих активов, оценили потенциальный ущерб взлома ключевых информационных активов и приступили к повышению осведомленности как своих СУИБ, так и рядовых сотрудников.

Хотя реальная оценка стоимости обеспечения защиты АСУ ТП со временем только возрастает, а бюджетов не хватает, тем не менее работа по обеспечению защиты все-таки проводится. К тому же и сам российский рынок средств защиты постепенно развивается – на нем появляются новые специализированные на защите именно АСУ ТП продукты. Завоевывают свое место и поставщики услуг в области аутсорсинга управления средствами защиты АСУ ТП.

Однако результаты опроса показывают, что сейчас превалирует «теоретическая» безопасность – категорирование, моделирование угроз и различные лучшие практики, а практическая часть мониторинга инцидентов, их расследование и анализ попрежнему не очень популярны, что и понятно. Часть Закона № 187-ФЗ, которая относится к практическим аспектам реагирования и за которую отвечает НКЦКИ, работает пока не очень хорошо. Связано это с тем, что отрасль новая и в ней еще не очень много профессиональных и компетентных кадров. Еще одной причиной является временный приоритет процедуры категорирования, т. е. анализа информационных активов, потенциальной их опасности и оценки риска атаки на них. Построение систем мониторинга, выявление реальной статистики по инцидентам и практика реагирования на инциденты только начинают нарабатываться. Скорее всего, эта деятельность будет активизироваться в этом и следующих годах. ■