Импортозамещение на марше

В этом году наша конференция прошла в самый разгар санкционного противостояния, когда иностранные производители, в том числе средств защиты и АСУ ТП, наперебой обещали уйти с российского рынка. Кроме того, отечественные компании подверглись массовой атаке, которая была направлена как на вывод инфраструктуры из строя, так и на замену сайтов компаний пропагандистскими сообщениями. Естественно, это стимулировало и стремление к замещению иностранных решений отечественными, и в целом интерес к вопросам информационной безопасности особенно значимых объектов критической информационной инфраструктуры. Конечно, не все ответившие были искренни в своих ответах, было несколько анкет, где выбирались только ответы-«заглушки» – «Другое» или «Затрудняюсь с ответом», что говорит о сильном брожении в умах. Тем не менее именно такой переходный срез может оказаться весьма полезным для понимания происходящих на рынке информационной безопасности процессов.

Вопрос 1.

Диаграмма 1. Какую организацию вы представляете? (2022 г.)

Общее количество ответов – 264.

Демография нашей конференции регулярно меняется – очевидные тенденции в ней заметить сложно. Скорее она отражает волны интереса к методам защиты промышленных объектов. Если в прошлом году на первое место вышла отрасль ОПК, а на втором были разработчики и интеграторы средств ИБ, то в этом году ситуация перевернулась – на первое место опять вышли разработчики средств защиты с долей 17,8%, вытеснив представителей ОПК на второе место с результатом 12,12%. На третье и четвертое места опять поднялись представители нефтегазовой и энергетической отраслей с долями 10,98 и 10,23% соответственно. В прошлом году их интерес к ИБ угас настолько, что на третье место вырвались вузы. Ситуация текущего года все-таки возвратила интерес промышленности к различным аспектам безопасности.

Следует отметить, что доля ответов «Прочее» неуклонно растет все шесть лет существования нашего рейтинга, что говорит о непрерывном увеличении интереса со стороны других секторов экономики, которые не относятся к КИИ. В текущем году «Прочее» вышло на пятое место с долей в 9,47%, вытеснив на шестое разработчиков и интеграторов АСУ ТП. Вот у этих компаний в 2022 г. отмечается кризис интереса к безопасности, что в общем-то объяснимо. Аутсайдером по посещаемости стала новая отрасль – горнодобывающая, ее впервые включили в опрос, и она закономерно заняла последнее место. Хотя понятно, что проблем с информационной безопасностью в горнодобывающей промышленности не меньше, чем во всех остальных.

И да – это самый популярный вопрос. На него ответило больше всего респондентов, что также достаточно предсказуемо – сложно не ответить на самый первый вопрос.

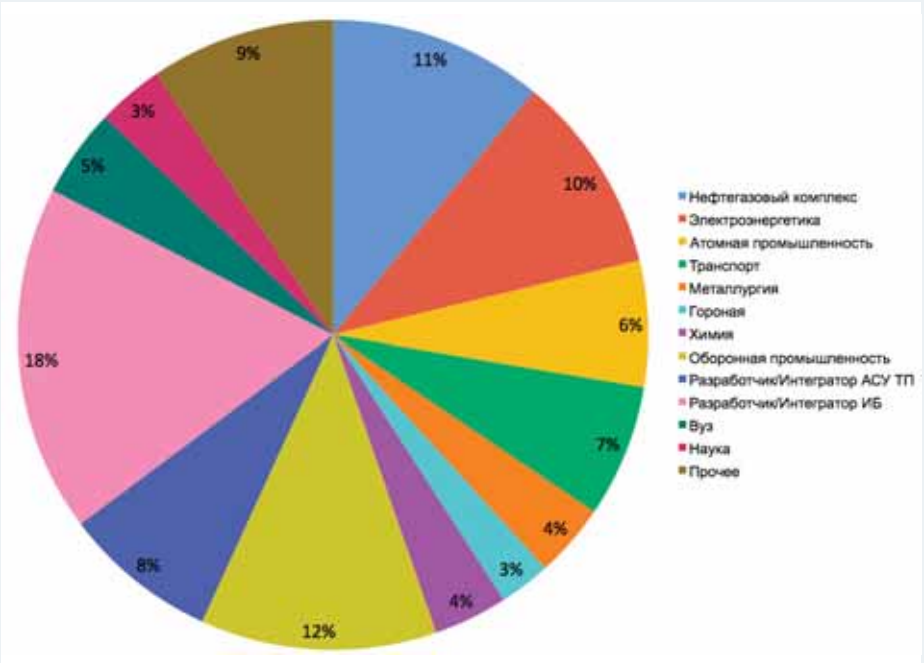
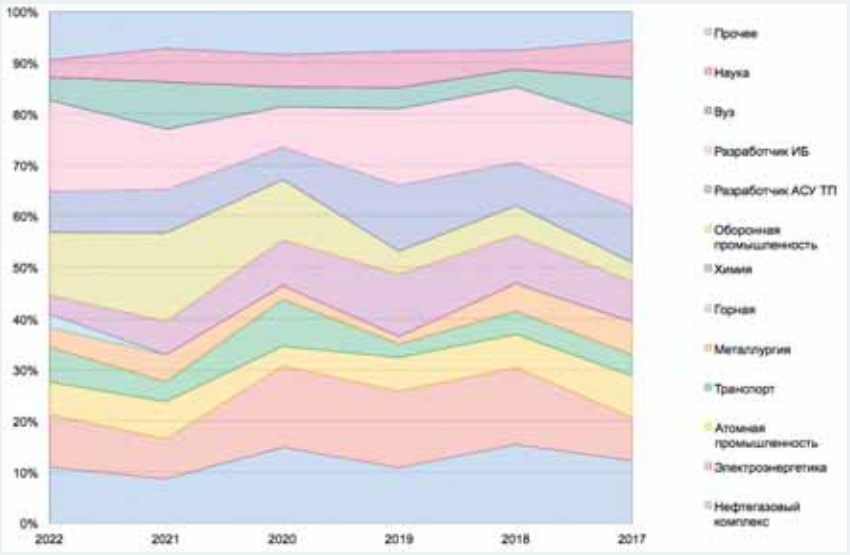


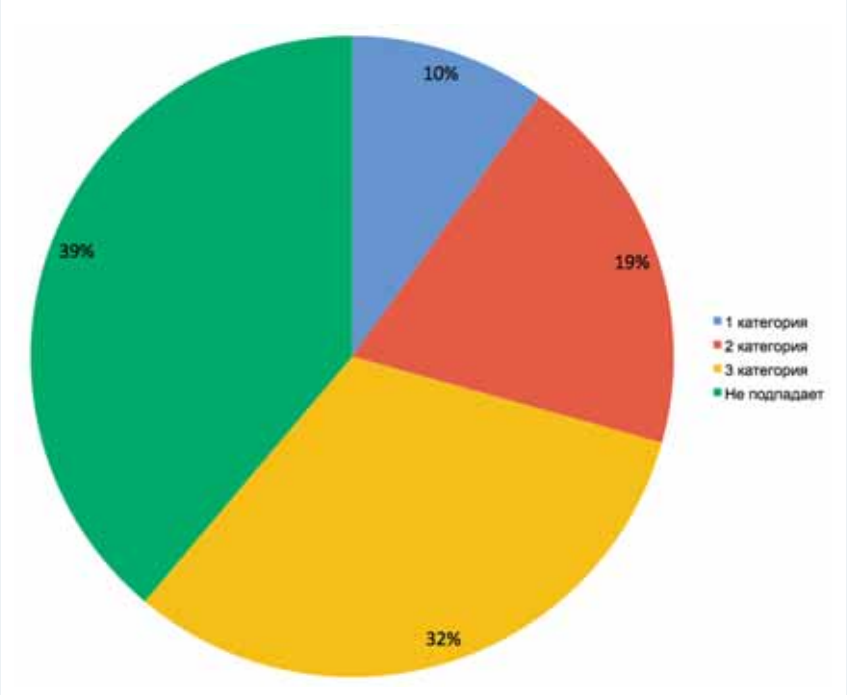
Диаграмма 2. Какую организацию вы представляете? (2017–2022 гг.)



Уже шесть лет мы проводим опросы посетителей нашей конференции «Информационная безопасность автоматизированных систем управления технологическими процессами критически важных объектов». По каждому опросу ежегодно публиковались подробные отчеты. Чтобы максимально соответствовать современным тенденциям, вопросы регулярно меняются, поэтому сквозных вопросов, которые были с самого начала, немного – всего четыре. Было бы интересно проанализировать и сделать общие выводы по замеченным тенденциям.

Первый общий для всех вопрос о демографии самого опроса: «Какую организацию вы представляете?» В самом начале в качестве лидера по количеству ответов были разработчики ИБ, поскольку это сообщество хорошо консолидировано и активно ведет себя на рынке. Менее инициативные разработчики АСУ ТП оказались на третьем месте, уступив второе представителям нефтегаза. Однако уже на следующей конференции ситуация резко поменялась – в лидеры вышли энергетики и нефтегазовый комплекс, а интеграторы ИБ с первого места сместились на третье. На третий год ситуация опять развернулась в сторону разработчиков АСУ ТП и ИБ, но только теперь энергетики стали третьей отраслью, попавшей в лидеры. Однако уже в 2020 г. в лидеры вновь вышли прикладные отрасли – нефтянка, энергетика и ОПК. Причем в 2021 г. ОПК стала лидером по количеству заполненных анкет, а на третье место вышли вузы. В 2022 г. маятник опять качнулся в сторону ИБ-компаний – они вышли на первое место, потеснив и ОПК, и энергетиков, и нефтяников.

Следует отметить, что именно нефтегазовая и энергетическая отрасли всегда были лидерами по категорированию своих объектов и построению средств защиты, что неоднократно отмечалось регуляторами, поэтому можно сказать, что результаты наших опросов адекватно отражают интерес, который представители различных отраслей проявляют к тематике защиты промышленных объектов. Внимание к отрасли средств защиты со стороны ОПК особенно показательно: вопросами ИБ заинтересовались те отрасли, которые являются основой обороноспособности страны, для них защита своих информационных ресурсов принципиально важна. И теперь именно эта отрасль стала лидером среди клиентских, уступив пальму первенства только разработчикам ИБ.



Вопрос 2

Диаграмма 3. К какой максимальной категории, по вашим

оценкам, относятся принадлежащие вашей компании объекты КИИ? (2022 г.)

Общее количество ответов – 242.

Здесь самым популярным ответом оказался «Не подпадает» – так ответили 38,8% участников опроса. Таким образом, практически две трети респондентов относят себя к той или иной категории КИИ. Предсказуемо, что еще почти треть (31,8%) относят свои объекты к минимальной третьей категории объектов. Доля первой категории – всего 9,9%, что говорит о том, что даже не все представители ОПК относят свои информационные системы к данной категории. Это хорошее дополнение к демографической картине конференции, которая в целом отображена предыдущим вопросом. Однако если в конференции участвует 61,2% владельцев ЗОКИИ, то и обсуждение вопросов, связанных с реализацией Закона № 187-ФЗ «О безопасности КИИ РФ», будет более предметным и насыщенным.

Можно отметить, что распределение по категориям стремится фактически к идеальному – 10, 20, 30, 40. Из тенденции в большую сторону выделяется только третья категория, которой, видимо, присваивают чуть больше, чем следовало. Это логично: с одной стороны, наличие ЗОКИИ является поводом финансировать службы ИБ, специалисты которой обычно участвуют в процессе категорирования объектов, с другой – это минимальная категория, требующая минимального внедрения различных средств защиты. Она хороша для начала, если компания не готова тратить больше средств на обеспечение безопасности.

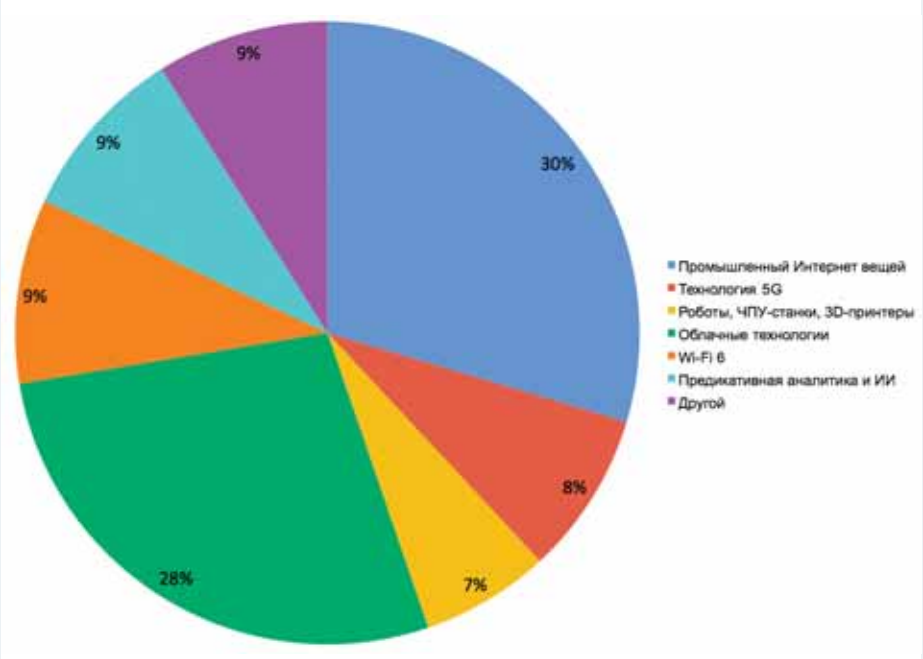
Вопрос 3

Диаграмма 4. Какие промышленные технологии, по вашему мнению, существенно увеличивают информационные риски для предприятий? (2022 г.)

Общее количество ответов – 449.

Этот вопрос мы задавали нашим респондентам впервые с целью выяснить отношение к различным технологиям у специалистов по информационной безопасности. Оказалось, что наиболее опасными считаются промышленный Интернет вещей (29,6%) и облачные технологии (27,6%), т. е. все, что связано с использованием Интернета в промышленности, считается потенциально опасным. Далее следуют технологии «ближней» связи и обработки информации: Wi-Fi 6 (9,6%), предиктивная аналитика и искусственный интеллект (9,1%), технология мобильной связи 5G (8,5%). Минимум беспокойства вызывают, казалось бы, совсем локальные устройства – роботы, станки с ЧПУ и 3D-принтеры. Их опасность отметили всего 6,7% опрошенных. Впрочем, доля «прочих» технологий достаточно велика – 8,9%, и в ней могут прятаться технологии не менее опасные, чем роботы и 5G. Видимо, в дальнейшем придется расширять спектр возможных рискованных для промышленных предприятий технологий.

Интересен тот факт, что кроме различных технологий связи – Интернет, Wi-Fi и 5G – обеспокоенность ИБ-специалистов вызывает искусственный интеллект, который призван помогать промышленным предприятиям решать свои оперативные задачи. Однако решения искусственного интеллекта воспринимаются многими как непрозрачные, т. е. неконтролируемые. Специалисты не очень доверяют «постороннему интеллекту». Хотя понятно, что используемые сейчас технологии ИИ – это в основном статистический анализ предварительно размеченных данных. Статистика вроде не должна ошибаться, но не все готовы ей доверять.

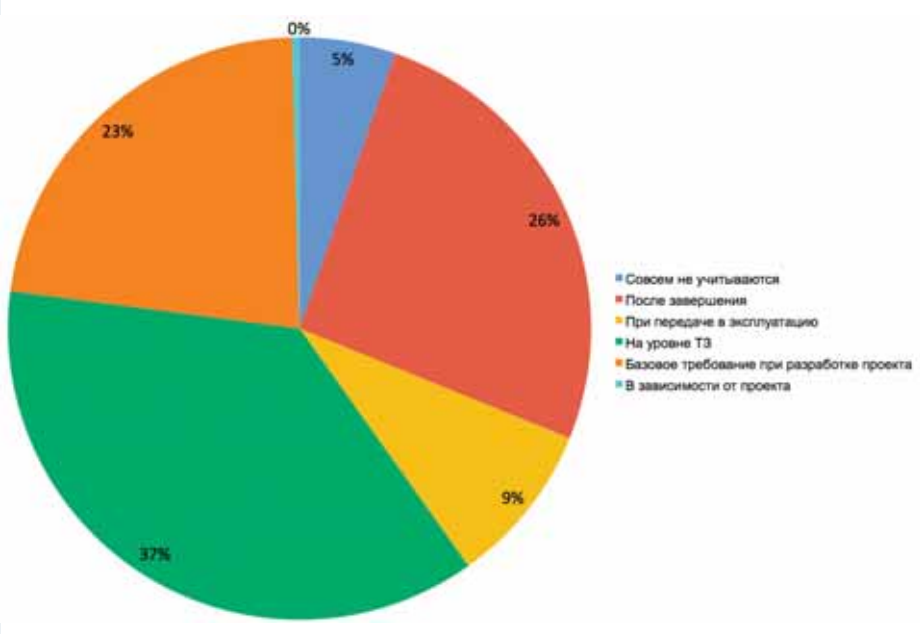


Вопрос 4

Диаграмма 5. Насколько, по вашим оценкам, вопросы информационной безопасности учитываются в проектах цифровизации современных производств? (2022 г.)

Общее количество ответов – 244.

Цифровизация производства – одна из ключевых тем развития промышленных предприятий. Однако чем больше предприятие цифровизовано, тем важнее в нем организовать защиту от кибератак. Поэтому мы решили спросить респондентов, на каком уровне принимаются решения по организации защиты предприятия в процессе его цифровизации. Оказалось, что больше трети проектов (36,9%) по цифровизации уже содержат требования по организации защиты в техническом задании, и это самый популярный ответ. Впрочем, четверть проектов (25,8%) реализуется без требований по безопасности, а потом вдогонку стартуют проекты по обеспечению их защиты. В 22,5% случаев безопасность является базовой функциональностью проекта, т. е. именно для усиления информационной защиты проект и реализуется. Совсем не учитывать требования по безопасности сейчас практически невозможно – это отметили 5,3% респондентов.



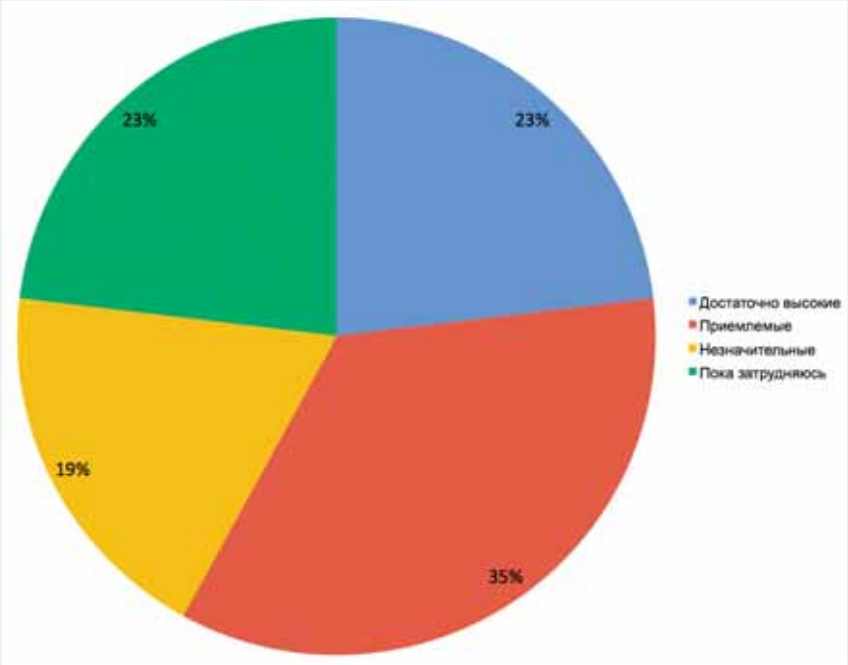
Аналогичный вопрос был задан и в прошлом году, и уже тогда доля проектов по цифровизации с прописанными в ТЗ требованиями по безопасности была на первом месте – 32,18%, что близко к значениям текущего опроса, однако доля проектов, где безопасность является базовой функциональностью проекта, резко увеличилась за год – с 6,9 до 22,5%. В то же время уменьшается доля проектов, в которых безопасность реализуется как в процессе ввода в эксплуатацию (с 19,5 до 9,0%), так и после завершения (с 28,7 до 25,8%). Таким образом, можно констатировать, что значимость вопросов информационной безопасности при реализации проектов по цифровизации предприятий возрастает.

Вопрос 5

Диаграмма 6. Как вы оцениваете затраты на выполнение требований по защите АСУ как части КИИ предприятия? Например, как долю от всего ИБ-бюджета предприятия? (2022 г.)

Общее количество ответов – 238.

Этот экономический вопрос по реализации требований законодательства отражает в основном то, умеет ли служба ИБ считать деньги. Конечно, реализовать законодательные требования можно и с помощью организационных мер, которые, как правило, не требуют больших расходов,



однако, чтобы это понять, как раз и нужно адекватно оценить свои финансовые возможности. В этом году, как и в прошлом, наиболее популярным ответом является «Приемлемые» – так ответили 34,9%. Это самое большое значение за все время существование данного пункта в опросе, т. е. за последние пять лет. При этом доля ответов «Достаточно высокие» оказалась минимальной за тот же период – 23,1%. Именно за этой долей скрываются те, кто так и не научился считать стоимость оперативной работы службы, считая ее «сверхценной». Впрочем, и затрудняющихся с ответом было немного больше, чем обычно: в течение нескольких лет этот показатель колебался около 21,5%, а сейчас вырос до 23,1%. Таким образом, можно констатировать, что рынок научился адекватно оценивать деятельность служб ИБ на предприятиях.

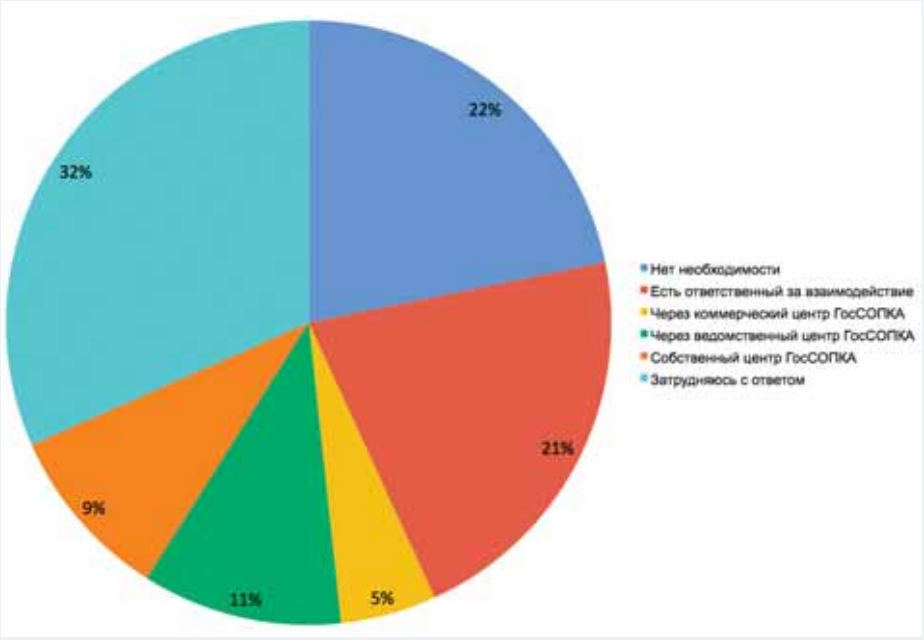
Вопрос 6

Диаграмма 7. Как у вашей компании организовано взаимодействие с ГосСОПКА? (2022 г.)

Общее количество ответов – 234.

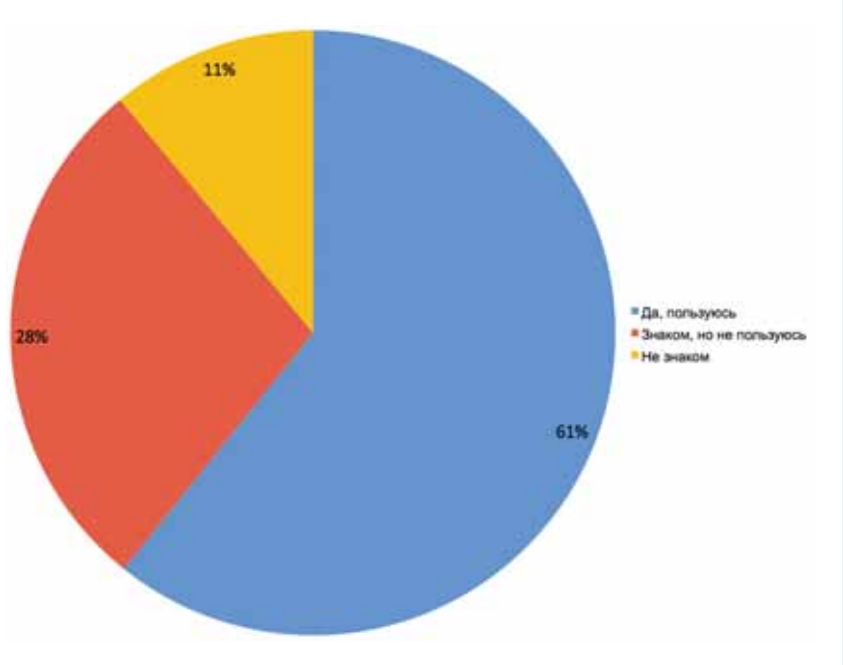
Взаимодействие с ГосСОПКА является основным компонентом организации защиты критически важных объектов, поскольку именно через него обеспечивается централизованное управление защитой по всей стране. При этом необходимо и отсылать сведения по инцидентам в ГосСОПКА, и адекватно реагировать на предупреждения, которые публикует НКЦКИ. Однако, как показывает опрос, большинство служб ИБ сконцентрировались на решении собственных проблем и не имеют четкого представления о том, как встроиться в национальную систему защиты. Количество затрудняющихся с ответом вышло на первое место со значением в 31,6%. Впрочем, ответ «Нет необходимости» с достаточно большой долей в 21,8% показывает, что еще не все участники опроса понимают важность единой системы координации действий, которой является ГосСОПКА. Впрочем, примерно столько же (21,4%) как минимум имеют специалиста для поддержания связи с ГосСОПКА, ещё 10,7% организуют взаимодействие через ведомственный центр реагирования. Чуть меньше (9,4%) построили собственный центр ГосСОПКА, а вот популярность подключения через коммерческие центры остается минимальной.

По сравнению с прошлым годом количество затрудняющихся с ответом увеличилось чуть более чем в два раза – с 15,5 до 31,6%, причем произошло это за счет всех вариантов центров реагирования. Это можно объяснить определенным разочарованием в технологии центров реагирования, требующих значительных расходов, причем их экономическая эффективность оставляет желать лучшего. Ситуация, когда пользователи не понимают, зачем им SOC, скорее всего, в будущем приведет к перестройке этого рынка. Альтернативное объяснение – появление отраслевых центров ГосСОПКА, которые изначально документами не предусмотрены и поэтому не были включены в наш опрос. Именно те клиенты, которые их используют, и могли выбрать вариант ответа «Затрудняюсь с ответом».



Вопрос 7

Диаграмма 8. Пользуетесь ли вы базой угроз ФСТЭК России? (2022 г.)

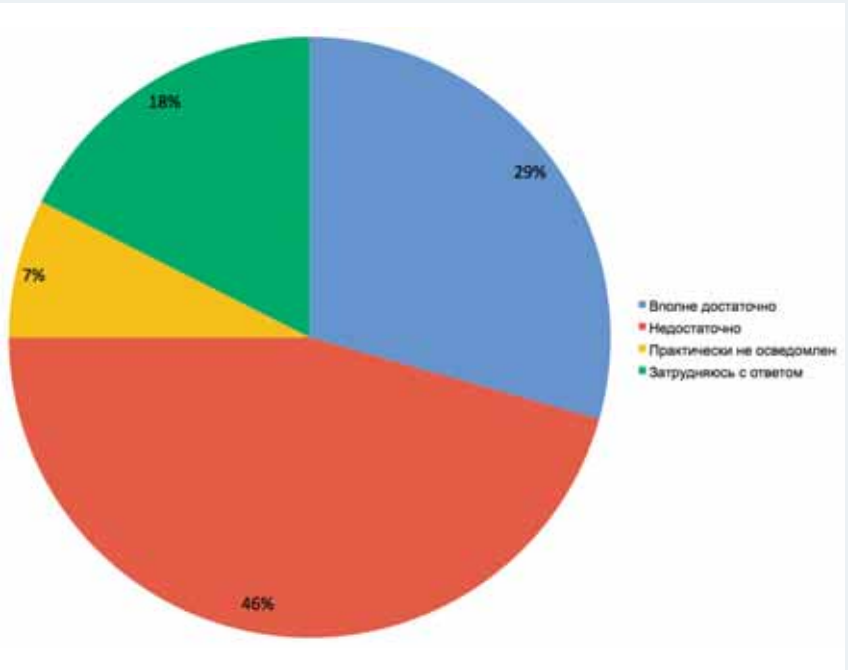


Общее количество ответов – 209.

База данных ФСТЭК по уязвимостям и угрозам за счет упоминания в стандарте безопасной разработки ПО также становится неотъемлемой частью государственной системы защиты, поэтому для нас важно было понять, насколько она популярна. Оказалось, что ею пользуются 60,8%, что является хорошим показателем. Не подозревают о ее существовании всего 11,0%, чуть больше четверти опрошенных (28,2%) не видят в ней особого смысла. Скорее всего, по мере внедрения стандарта на безопасную разработку и других действий ФСТЭК в ближайшее время она станет более популярной и займет свое место среди источников полезной информации для защиты промышленных объектов.

Вопрос 8

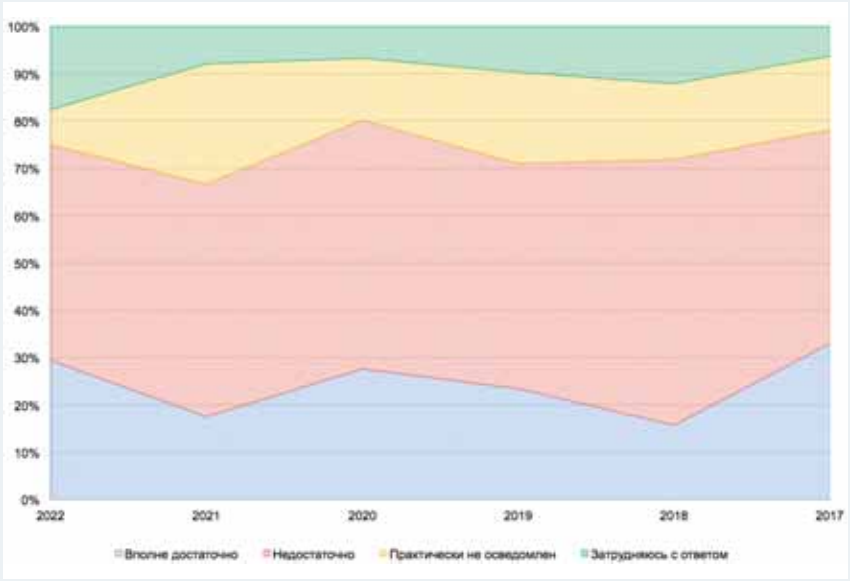
Диаграмма 9. Как вы оцениваете уровень осведомленности персонала вашего предприятия в области защиты АСУ ТП как части КИИ? (2022 г.)



Общее количество ответов – 228.

Уровень осведомленности персонала в вопросах информационной безопасности – важный показатель для оценки влияния человеческого фактора на безопасность предприятия. Если сотрудники компании не стремятся соблюдать требования кибергигиены, то как бы ни старалась служба безопасности защитить информационные системы, фишинг будет работать. Именно он является сегодня одним из основных векторов атаки, в частности, на объекты критической инфраструктуры. Показатель «Неосведомленность» находится на минимальном уровне за все время проведения опросов – 45,6%. Только в самом начале были получены аналогичные показатели. Доля ответов «Вполне достаточно» возвращается тоже к результатам 2017 г. – 29,4%. По показателю «Практически не осведомлен» достигнут минимальный результат за все время существования опроса – 7,5%. Таким образом, можно констатировать, что работа с персоналом в части осведомленности ведется и сотрудники служб ИБ оценивают ее как успешную.

Диаграмма 10. Как вы оцениваете уровень осведомленности персонала вашего предприятия в области защиты АСУ ТП как части КИИ? (2017–2022 гг.)



Этот вопрос мы также задавали в течение всех шести лет проведения наших исследований. Ответ «Недостаточно» постоянно находился в диапазоне от 45 до 56%. То есть практически половина отвечавших недовольны осведомленностью своих сотрудников в вопросах информационной безопасности. В то же время именно от этого показателя зависит уровень «цифровой гигиены», т. е. соблюдения правил политики безопасности всеми участниками информационного взаимодействия, а не только сотрудниками служб ИБ. Эта тенденция показывает, что по крайней мере половина компаний предпочитают фокусироваться на построении технической защиты, а не на обучении линейного персонала по вопросам информационной безопасности.

Вопрос 9

Диаграмма 11. Были ли у вашего предприятия или холдинга инциденты информационной безопасности в части АСУ ТП в прошедшем году? (2022 г.)

Общее количество ответов – 180.

Следует отметить, что этот вопрос с минимальным количеством участников, т. е. респонденты не любят делиться информацией об инцидентах в принципе. Но даже если и отвечают, то чаще всего – «Инцидентов зафиксировано не было». Его выбрали, как и в прошлом году, ровно 70,0% респондентов. Впрочем, это, вероятно, говорит о том, что система мониторинга плохо фиксирует нападения. Во всяком случае, общая активность злоумышленников явно возрастает. Доля ответов «Были с ущербом для АСУ ТП» впервые за все время опроса превысила отметку в 1,5% и достигла значения в 1,67%. Аналогичный рекорд поставлен и по другому показателю – «Были с ущербом, но АСУ ТП не пострадала» (5,56%). Антирекорд поставлен в ответе «Были, но ущерба не было» – 15,6%. Именно этот пункт показывает эффективность работы системы защиты – она зафиксировала инцидент, отреагировала на него и предотвратила возможный ущерб. То есть в целом можно сделать вывод, что количество инцидентов все-таки растет, поскольку ущерб фиксируется, а системы мониторинга и тем более реагирования работают все менее эффективно. Возможно, именно с этим и связано определенное разочарование различными SOC, которое было зафиксировано при обсуждении вопроса 6.

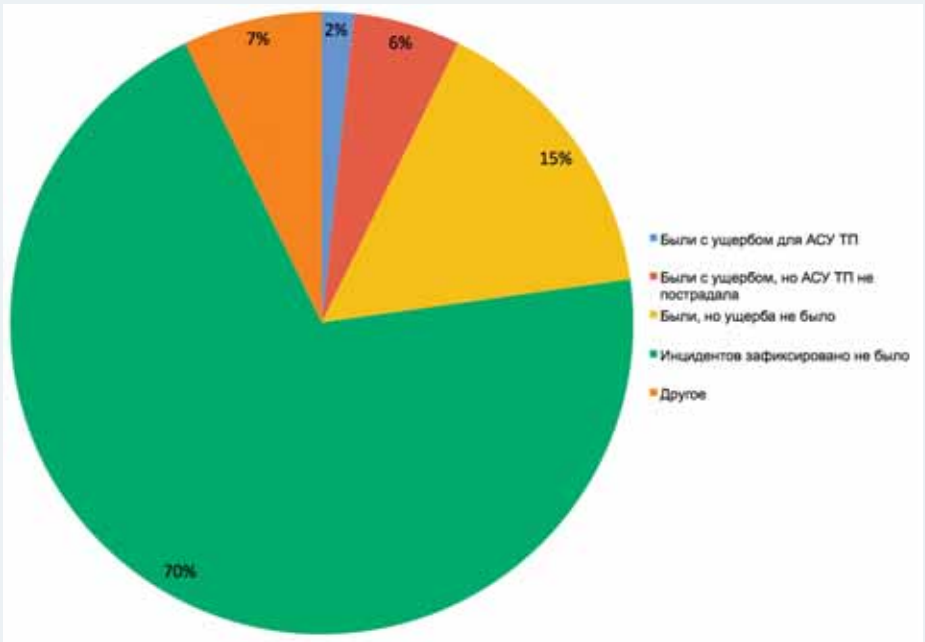
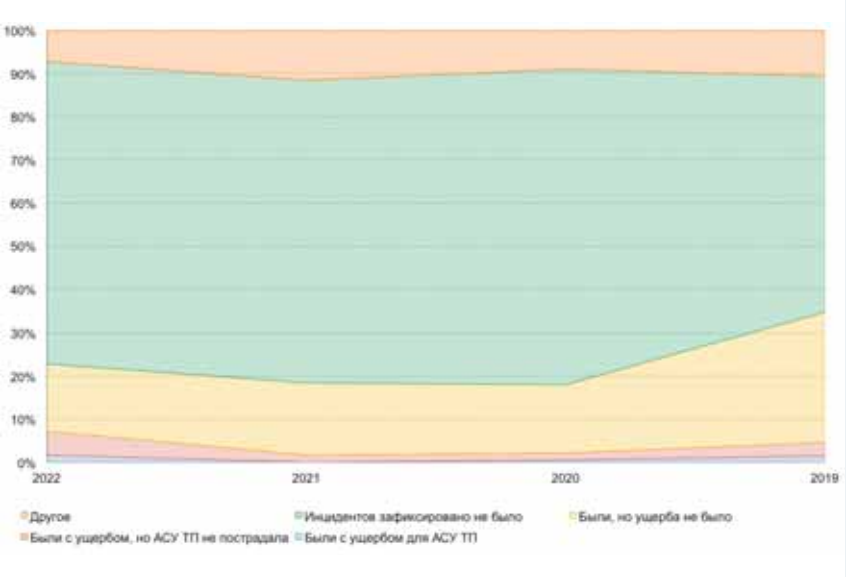


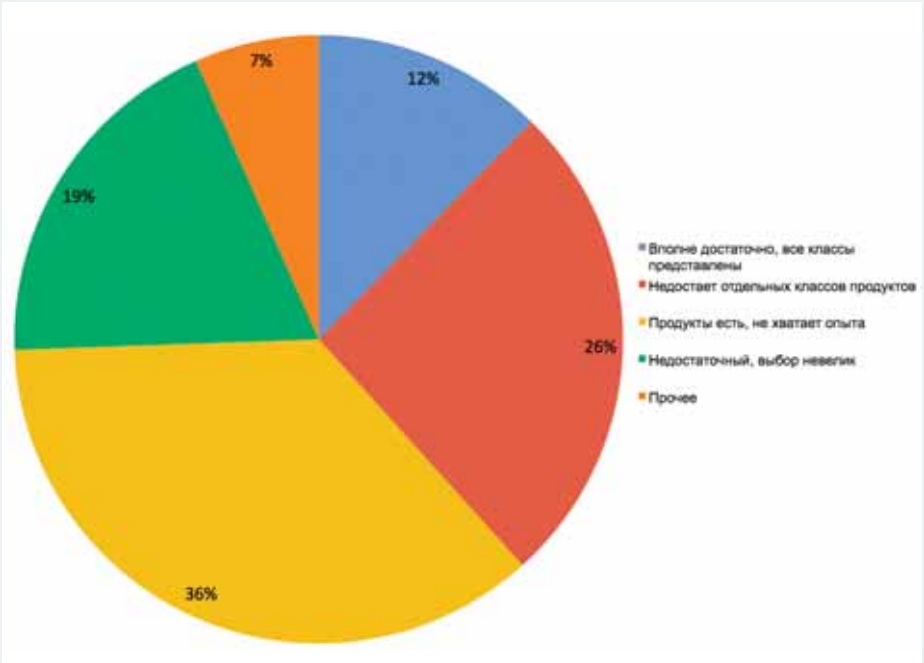
Диаграмма 12. Были ли у вашего предприятия или холдинга инциденты информационной безопасности в части АСУ ТП в прошедшем году? (2019–2022 гг.)



Этот вопрос мы не задавали в течение четырех последних лет. Доля тех, кто признает наличие инцидентов не очень большая, но она растет. Однако самым «правильным» должен быть ответ «Были, но ущерба не было», поскольку именно он показывает эффективность работы служб информационной безопасности – они фиксируют попытки атак, вовремя их выявляют и предотвращают ущерб. Однако в этом году доля такого ответа минимальна, хотя в первый год, когда данный вопрос задавался, она достигала практически трети ответов. В целом можно отметить, что количество успешных инцидентов выросло настолько, что не признавать это уже невозможно, а эффективность работы служб ИБ снизилась. И это при том, что более двух третей респондентов вообще не замечают опасности, т. е. не фиксируют инцидентов.

Вопрос 10

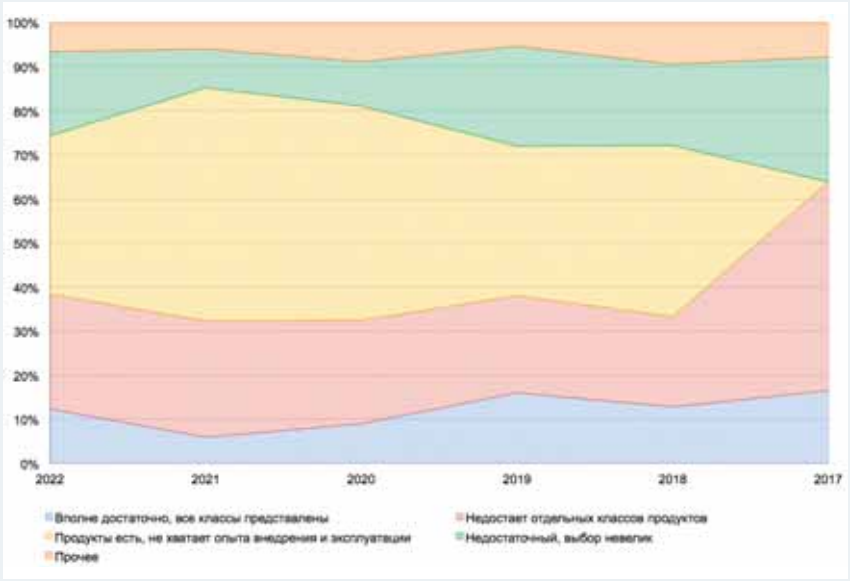
Диаграмма 13. Как вы оцениваете ассортимент представленных на рынке отечественных продуктов и услуг по безопасности АСУ ТП? (2022 г.)



Общее количество ответов – 227.

Сегодня импортозамещение – одна из самых важных тем. Обеспечение защиты ЗО КИИ не должно зависеть от поддержки производителя, который находится в иностранной юрисдикции. Однако переход на продукцию отечественных производителей не должен оказывать влияния на защищенность объектов КИИ. Опрос показал, что распределение мест по ответам сохранилось с прошлого года: первое занял ответ «Продукты есть, не хватает опыта внедрения и эксплуатации» с долей 36,1%, второе – «Недостает отдельных классов продуктов» (26,0%), третье – «Недостаточный, выбор невелик» (18,9%). Полностью удовлетворенных выбором – минимальное число (12,3%). Однако соотношение между этими ответами несколько сгладилось. Если еще в прошлом году более половины (52,9%) было «неопытных», то теперь их доля резко сократилась до 36,1%, а доли радикально противоположных ответов «Вполне достаточно, все классы представлены» и «Недостаточный, выбор невелик» выросли более, чем в два раза. В результате распределение стало более равномерным, т. е. рынок стабилизируется.

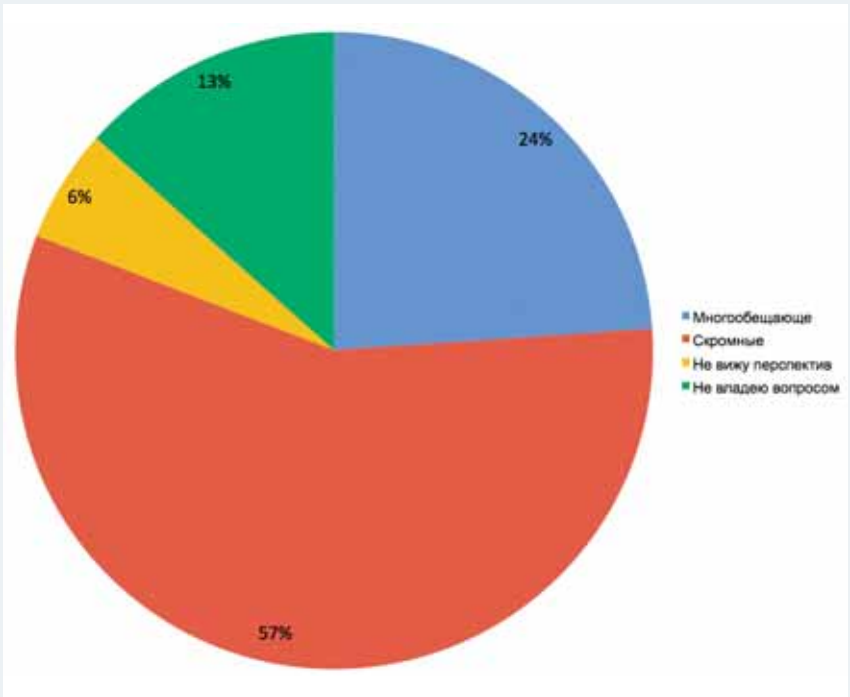
Диаграмма 14. Как вы оцениваете ассортимент представленных на рынке отечественных продуктов и услуг по безопасности АСУ ТП? (2017–2022 гг.)



Наиболее популярный ответ в прошлом году – «Продукты есть, не хватает опыта внедрения и эксплуатации». Этот ответ постепенно увеличивал свою долю, пока не пересек отметку в 50%. Однако в текущем году он резко сократился, практически до трети. Так же постепенно возрастала и доля ответа «Недостает отдельных классов продуктов». В прошлом году она пересекла отметку в 25%, а в 2022 г. осталась на достигнутом уровне. Противоположные ответы «Вполне достаточно, все классы представлены» и «Недостаточный, выбор невелик» практически синхронно до прошлого года снижали свою долю, а в этом резко увеличились более чем в два раза. Это говорит о резком увеличении неопределенности на рынке ИБ, в том числе с импортозамещением.

Вопрос 11

Диаграмма 15. Как вы оцениваете перспективы импортозамещения КИИ в части, касающейся АСУ ТП? (2022 г.)



Общее количество ответов – 209.

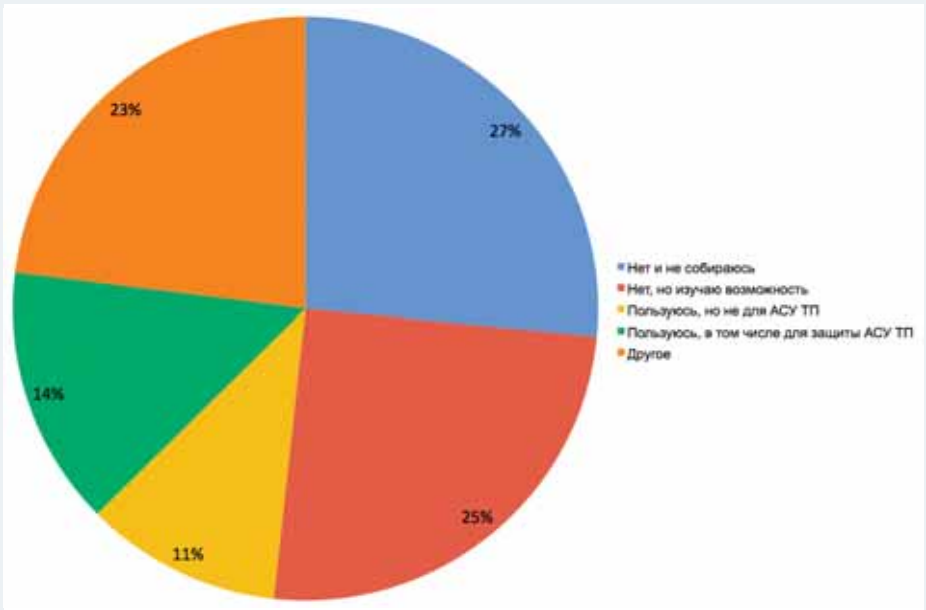
Впрочем, вопрос импортозамещения АСУ ТП не менее принципиален для улучшения безопасности промышленных объектов. И здесь оценки респондентов более сдержанные – свыше половины (56,9%) оценивают перспективы российских АСУ ТП как «скромные». Тем не менее это не означает, что они не будут внедрять подобные продукты. Скорее всего, переход на отечественные системы автоматизации для этого класса клиентов будет зависеть от результатов пилотного проекта. Разочарованы отечественными АСУ ТП минимальное количество ответивших – 5,7%, а почти четверть (23,9%) все-таки верят в перспективность российских разработок АСУ ТП. Фактически отечественным разработчикам выдан серьезный кредит доверия: если они смогут доказать, что в состоянии конкурировать с иностранными производителями промышленной автоматизации, то у них есть достаточно потенциальных клиентов, которые не относятся к ним предвзято.

Вопрос 12

Диаграмма 16. Пользуетесь ли вы услугами аутсорсинга в области ИБ? (2022 г.)

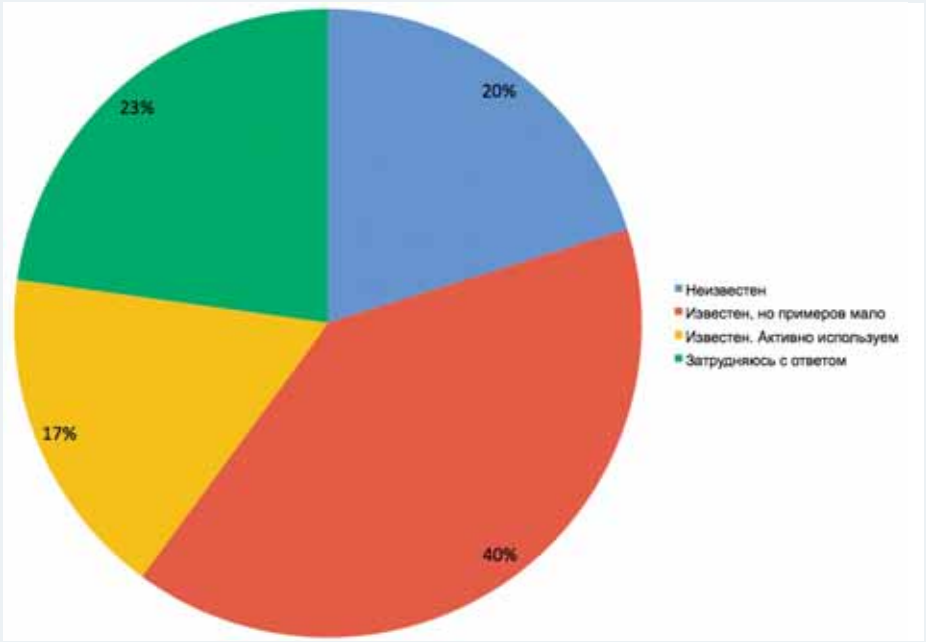
Общее количество ответов – 230.

Аутсорсинг информационной безопасности – один из развитых рынков аутсорсинга, поскольку в России достаточно компаний, которые предоставляют подобные услуги. Мы уже третий год задаем вопрос участникам конференции, и ответы их показывают отрицательное отношение к аутсорсингу. В этом году, как и в прошлом, лидером стал ответ «Нет и не собираюсь» с долей 26,5%, однако второе место также занимает отрицательный ответ «Нет, но изучаю возможность» (доля 25,2%).



На третьем месте по популярности с долей в 23,0% находится ответ «Другое», т. е. достаточно много владельцев промышленных объектов еще не определились с эффективностью использования аутсорсинга для безопасности промышленных объектов. Но уж если специалисты верят в полезность аутсорсинга инструментов безопасности, то применяют их и для защиты промышленных сетей. Их доля больше тех, кто использует АСУ ТП только в непромышленных сегментах, – 14,4 против 10,9% соответственно. Причем такое соотношение остается на протяжении всего времени проведения опросов.

Впрочем, значения отрицательных ответов минимальны за все три года, когда мы задаем соответствующий вопрос, т. е. отрицательное отношение все-таки уменьшается. Максимальное значение получила графа «Другое» – ее отметили почти четверть респондентов (23,0%), что больше значений для положительных ответов. Это значит, что есть ответ, который мы не предусмотрели в своем опроснике, а он может прояснить ситуацию с аутсорсингом ИБ.



ВОПРОС 13

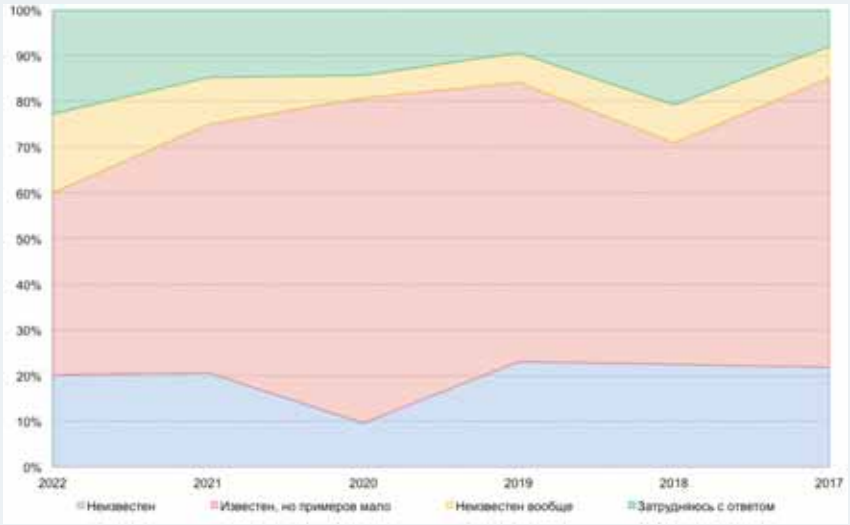
Диаграмма 17. Насколько хорошо вам знаком опыт предприятий, подобных вашему, в области защиты АСУ ТП? (2022 г.)

Общее количество ответов – 228.

Данный вопрос мы задавали с самого начала существования нашего опросника – с 2017 г., и лидер за все это время так и не поменялся. В текущем году, как и во всех предыдущих, им стал ответ «Известен, но примеров мало» с долей 39,9% – правда, это значение минимально за все время опросов. На второе место вышел пункт «Затрудняюсь с ответом», который получил максимальное значение за все

время – 22,8%. Это говорит о том, что появились новые обстоятельства, которые не очень укладываются в предлагаемую нами концепцию ответов. Возможно, опыт предприятий в связи с последними событиями нужно пересмотреть и переосмыслить. Тем не менее чуть больше пятой части опрошенных (20,2%) ответили, что опыт коллег им неизвестен. Наша конференция как раз и предназначена для обмена опытом, поэтому понятно, что среди ее посетителей много тех, кто пришел узнать о передовом опыте других компаний и ИБ-служб.

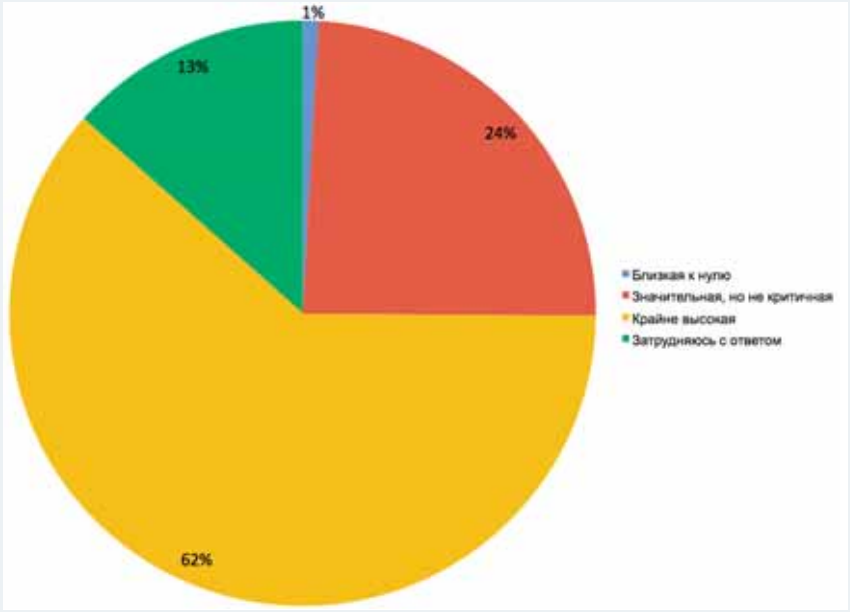
Диаграмма 18. Насколько хорошо вам знаком опыт предприятий, подобных вашему, в области защиты АСУ ТП? (2017–2022 гг.)



Данный вопрос мы также задавали с самого начала своей деятельности. Он, собственно, показывает, что на наше мероприятие по информационной безопасности собираются в основном те, кто хочет обменяться опытом. Во всяком случае, наиболее популярным за все время был ответ «Известен, но примеров мало». Это означает, что мероприятие воспринимается как хорошая площадка для обмена опытом использования ИБ-продуктов. Около пятой части всех ответов получил пункт «Неизвестен», т. е. примерно пятую часть на каждом мероприятии составляли новые посетители и специалисты, которые пришли знакомиться с опытом коллег. Только в 2020 г. показатель почему-то стал в два раза меньше – упал до 9,57%. Это было время первого прихода коронавируса, видимо, поэтому на нашу конференцию приехали опытные специалисты, которые хотели просто пообщаться.

Вопрос 14

Диаграмма 19. Как вы оцениваете в свете последних событий вероятность роста риска безопасности КИИ со стороны иностранных государств? (2022 г.)



Общее количество ответов – 231.

Этот вопрос мы задали второй раз. В прошлом году самым популярным был ответ «Значительная, но не критичная» с долей 46,3%. В 2022 г. в лидеры вышел ответ «Крайне высокая» с долей 61,5%, что объяснимо: массовые атаки на промышленные объекты были отмечены в момент проведения самой конференции. Год назад в этом пункте стояло не очень большое значение – 26,9%. Доля пункта «Близкая к нулю» в текущем году стремится к нулю (всего два ответа, которые дали значение в 0,9%), хотя в 2021 г.

данный пункт составлял целых 10,5%. При этом уменьшилась и доля затрудняющихся с ответом – с 16,4% в прошлом году до 13,4% в 2022-м. Действительно, ситуация с риском атак на КИИ со стороны иностранных государств стала более определенной, чем в прошлом году.

Заключение

В этом году интерес производителей средств защиты к конференции, посвященной безопасности промышленных объектов, явно увеличился. Вполне возможно, что они увидели перспективы на данном рынке, стремятся понять потребности участников и определить недостающие инструменты защиты. Впрочем, как уже было отмечено, возрос и интерес к информационной безопасности со стороны компаний, которые не относятся к КИИ. Безопасность в эпоху цифровизации становится важным элементом этого процесса. Впервые мы попытались понять, какие перспективные технологии могут вызвать максимальный риск, и получили, в принципе, предсказуемый результат – все, что связано с технологиями быстрой передачи данных и их обработкой на стороне производителей, вызывает большие подозрения. К этой категории рисков относятся и облака, и промышленный Интернет вещей, и искусственный интеллект, и Wi-Fi 6, и 5G. Однако цифровизация промышленности все-таки потребует внедрения всех перечисленных технологий, но делать это без учета требований по безопасности, хотя бы в составе технического задания, уже невозможно. Таким образом, информационная безопасность должна стать инструментом, который позволит не потерять контроль над внедряемыми технологиями и гарантировать получение прибыли от их внедрения.

В этом году важной стала тема импортозамещения, интерес к которой стимулирован поведением иностранных производителей как средств защиты, так и АСУ ТП. Российские промышленные компании не очень доверяют отечественным разработкам, особенно в части АСУ ТП, тем не менее внедрять их придется. Похоже, многие рассчитывают поменять средства защиты, которые не должны оградить иностранные продукты от постороннего влияния извне, однако замены именно АСУ ТП будут стараться всеми силами избежать. Впрочем, если отечественные разработчики смогут предложить защищенные и современные АСУ ТП решения, то их внедрение именно сейчас может привести к максимальному результату.

В целом можно отметить, что рынок средств защиты промышленных объектов в России становится достаточно развитым. На нем учитываются все современные тенденции – от непопулярного аутсорсинга до распространения культуры кибергигиены на промышленных предприятиях. К сожалению, отечественные специалисты в области ИБ не очень доверяют коммерческим SOC и в целом аутсорсингу сервисов защиты, тем не менее их популярность постепенно растет. Во всяком случае, именно аутсорсинг помогает обеспечить развитие систем защиты в ногу со временем и построение внешнего периметра защиты адекватно существующим угрозам. Даже доверие к государственной системе защиты ГосСОПКА возрастает по мере понимания ее роли в координации действий всех значимых объектов критической информационной инфраструктуры. ■