ИТОГИ ОПРОСА

XI КОНФЕРЕНЦИИ

«Информационная безопасность АСУ ТП критически важных объектов»

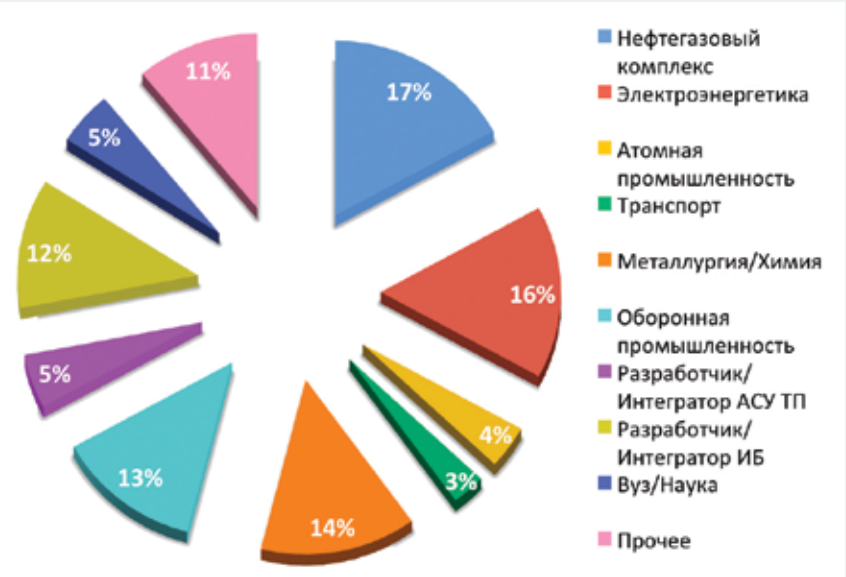
Организатор конференции
Connect!
ИЗДАТЕЛЬСКИЙ ДОМ

Перестройка и ускорение ИБ

Прошедший год сильно изменил ландшафт российского рынка информационной безопасности. С одной стороны, ушли ключевые иностранные производители средств защиты, а с другой – массовые атаки на отечественные предприятия повысили потребность в инструментах защиты. Эти факторы определили как перестройку всего рынка, так и ускорение процессов, которые на нем происходят. Хотя по-прежнему утверждается, что на отечественном рынке не хватает отдельных видов средств защиты (речь прежде всего идет о межсетевых экранах нового поколения), тем не менее уже несколько производителей заявили о том, что они выпускают подобные продукты. Путем анализа результатов опроса, который был проведен в рамках XI конференции «Информационная безопасность АСУ ТП критически важных объектов», мы постарались понять ситуацию, которая складывается на рынке средств защиты для промышленных информационных систем и АСУ ТП.

1. Какую организацию вы представляете?

Всего ответов – 268.

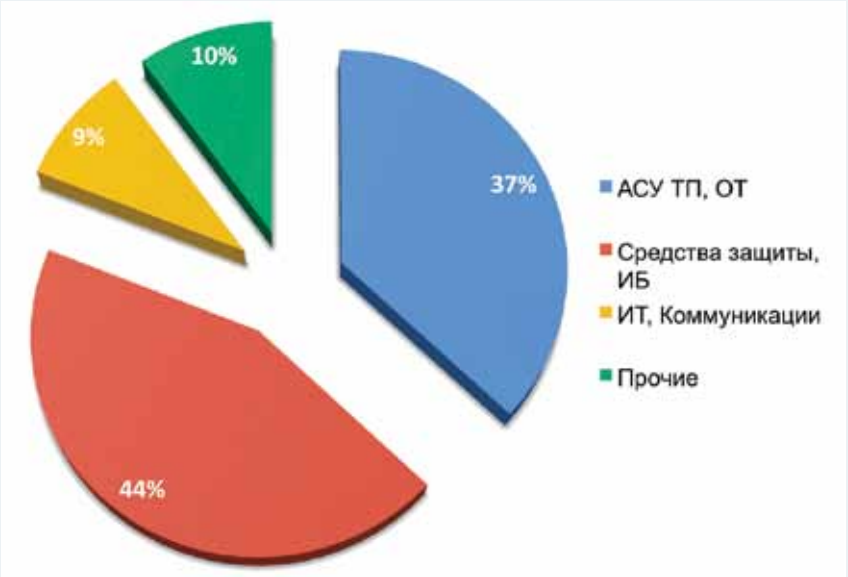


Данный вопрос касается демографии. В этом году лидерами стали нефтегазовый комплекс (17% ответов), электроэнергетика (16%) и металлургия/химия (14%). На четвертом месте также представители промышленности – ОПК с долей в 13% и только на пятом месте разработчики и интеграторы информационной безопасности. Их в текущем году было 12%, хотя в прошлом именно они стали лидерами с долей в 17,8%. Это подтверждает тенденцию на полное изменение состояния и интересов рынка информационной безопасности. Если раньше он двигался за счет пропаганды со стороны разработчиков и интеграторов ИБ, то сейчас интерес к нему проявляют сами клиенты – промышленные компании из критически важных отраслей российской экономики.

Антирейтинг ответов также показателен: меньше всего интереса проявляют компании транспортной (3%) и атомной промышленности (4%). Похоже, что это именно те отрасли, которые не очень беспокоятся об информационной безопасности своих АСУ ТП. Возможно, причина в том, что все проблемы ИБ у них полностью решены. Также минимальный интерес к теме выразили и научные заведения, и разработчики АСУ ТП. Казалось бы, именно от них зависит безопасность – они должны разрабатывать методы защиты оборудования технологических процессов, однако их не очень интересует компьютерная безопасность АСУ ТП. Показателен и ответ «Прочие» в 11%, который говорит о том, что в нем могут скрываться еще несколько «не очень озабоченных ИБ» отраслей.

2. Какие системы на предприятии находятся в вашем подчинении?

Всего ответов – 241.



Этот вопрос мы задаем впервые: фактически он является продолжением предыдущего, поскольку предназначен для выяснения должностей, которые занимают респонденты в своих организациях. Предсказуемо на конференции по безопасности на первом месте оказались специалисты по безопасности (44%), на втором – неожиданно не специалисты по ИТ и связи (всего 9%), а специалисты по АСУ ТП и в целом по операционным технологиям (37%). Таким образом, опрос в большей мере выражает мнение как безопасников, так и асушников, при очень незначительном влиянии айтишников. Доля прочих оказалась даже выше ИТ – 10%, т. е. их влияние на результаты опроса может оказаться даже выше, чем айтишников.

3. Требования каких нормативных актов сейчас наиболее актуальны для вашей организации?

Всего ответов – 218.

К сожалению, информационная безопасность в России зависит не столько от потребности в защите информационных систем и АСУ ТП, сколько от требований внешних факторов – законов, указов, отраслевых регуляторов. В прошлом году мы даже не задавали вопрос о требованиях к информационной безопасности, однако в 2021 г. такой вопрос был в нашем обзоре, и тогда доля нормативных требований ФСТЭК составила 51%, ФСБ – 21%, нормативных требований отраслевых регуляторов – 9%, т. е. регуляторы в целом определяли около 81% всех требований, предъявляемых к промышленным организациям. Сейчас ситуация усугубилась: только Закон № 187-ФЗ определяет примерно 61% требований, а к нему нужно еще добавить требования «первомайского указа» прошлого года (16%), других федеральных законов (5%), а также отраслевых регуляторов (7%). В целом получается: уже 89% требований определяется правительственными структурами, в то время как доля собственных требований сократилась с 13 в 2021 г. до 2%. Таким образом, можно констатировать, что отрасль информационной безопасности сейчас полностью регулируется государственными службами. Возможно, это хорошо – законодательные требования настолько оптимальные, что у компаний не возникает потребности в собственных разработках. Однако ситуация может оказаться и более сложной, когда компании вынуждены много сил и средств тратить на внедрение навязанных «сверху» механизмов защиты.

4. Какие технологии, по вашему мнению, существенно увеличивают информационные риски для предприятий?

Всего ответов – 205.

Впервые этот вопрос был задан в прошлом году, чтобы определить технологии, которые вызывают у безопасников и асушников наибольшие подозрения. Лидеры за год не поменялись – облачные технологии (34 в этом году и 28% в прошлом) и промышленный Интернет вещей (32 и 30% соответственно). Возросла озабоченность только технологией искусственного интеллекта с 9 в прошлом году до 11% в текущем. Технология 5G уменьшила долю «опасности» с 8 до 5%, а вот роботы и другое промышленное оборудование остались на уровне прошлого года, сохранив 7% респондентов, которые боятся данных устройств. Сократилась и доля ответов «Другой» с 9 до 7%. В лидерах прироста находятся облачные технологии, которые получили дополнительные шесть пунктов роста, на втором месте 5G с тремя пунктами, а третье место разделили промышленный Интернет вещей и искусственный интеллект.

Разочарование в облаках вполне объяснимо: международные операторы показали, как можно легко заблокировать облака и полностью лишить клиента доступа к технологиям. С 5G ситуация другая – его как не было, так и нет, но верят в его эффективность уже меньше. А вот промышленный Интернет вещей и искусственный интеллект – технологии, которые позволяют оптимизировать работу промышленных технологий, и возрастание недоверия к ним – симптом не очень хороший. При этом технология цифровых двойников, которая фактически является сочетанием промышленного Интернета вещей с искусственным интеллектом, оказалась по версии респондентов «самой безопасной».

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

Всего ответов – 197.

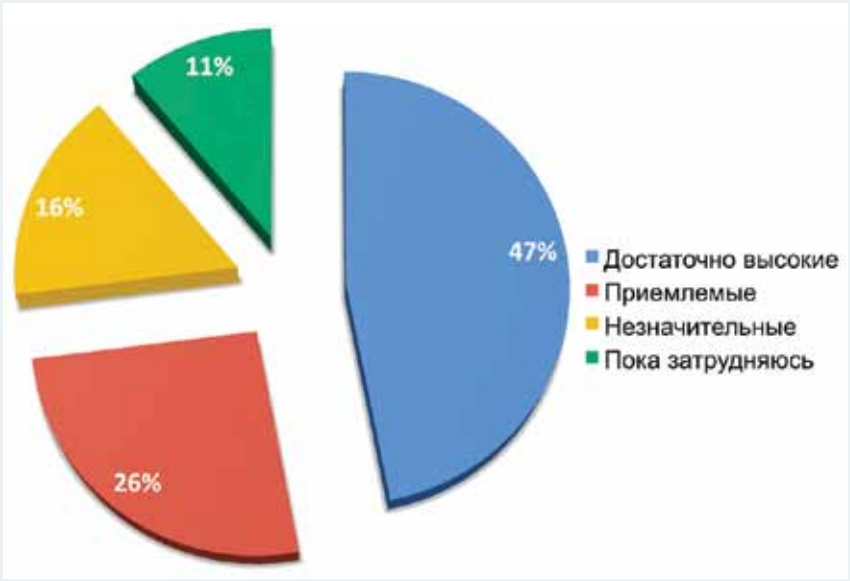
Цифровизация промышленных предприятий продолжается, невзирая на все проблемы, которые с ней связаны. Однако обеспечение безопасности в проектах по цифровой трансформации очень важно, поскольку ее отсутствие может привести к потере контроля над цифровизированным активом. Именно поэтому мы уже в прошлом году задавали вопросы по учету требований информационной безопасности в подобных проектах, рассуждая так: поскольку основные требования к информационной безопасности формируют законодательные акты (об этом мы писали выше), то и безопасность должна быть в проекте, как минимум, с технического задания. В прошлом году такой ответ действительно оказался самым популярным – его выбрали

37% респондентов. В этом году его доля уменьшилась до 33%, а на первое место вышел ответ «После завершения» с долей в 35% (в прошлом году – 26%).

Интересно, что по внешнему виду диаграмма нынешнего года похожа на аналогичное изображение 2021 г. Правда, прошлогодняя была с явным уклоном в безопасность – большая доля ответов про безопасность на уровне ТЗ и, что самое важное, невероятно большая доля ответов «Безопасность как базовое требование» – 23%. В 2021 г. доля этого ответа была незначительной (всего 1%), и сейчас она составляет 6%. Похоже, практика цифровой трансформации по части кибербезопасности вернулась в норму.

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

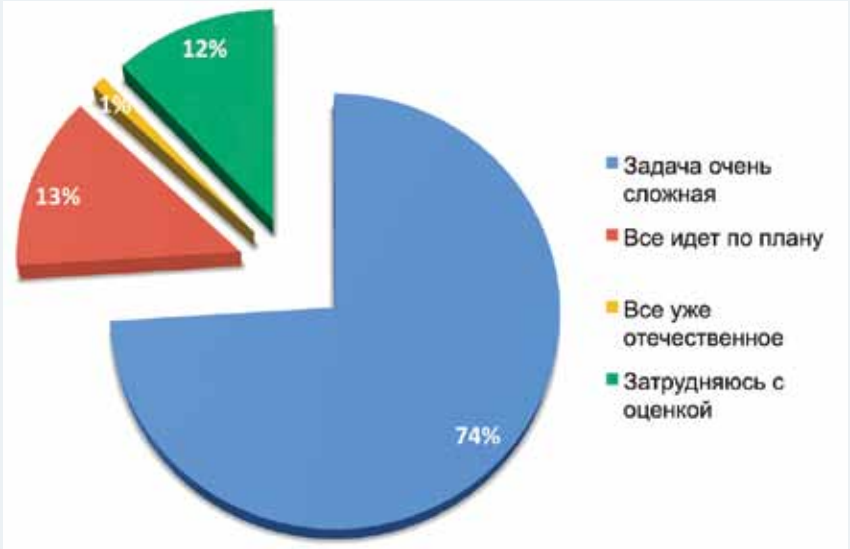
Всего ответов – 199.



Финансовые вопросы для безопасности были всегда очень существенными, однако сейчас они стали чрезвычайно важными. И если раньше доля ответа «Достаточно высокие» составляла от 23 в 2022 г. до 27% в 2021 г., то сейчас она резко увеличилась до 47%. Доля ответов «Приемлемые», которая несколько лет была в лидерах – примерно 35%, сейчас резко снизилась до 26%. Почти в два раза сократилась доля и «затрудняющихся» – с 23 до 11%. Возможно, это связано с тем, что компаниям приходится вкладываться в построение эффективной системы защиты, причем полностью заменяя уже установленные и отработанные ранее технологии новыми. Есть надежда, что это особенность только прошедшего года и дальше ситуация стабилизируется.

7. Как вы оцениваете процесс импортозамещения АСУ ТП на российских предприятиях?

Всего ответов – 209.



Этот вопрос стал продолжением предыдущего вопроса про бюджет обеспечения безопасности. В прошлом году он звучал несколько по-другому: «Как вы оцениваете перспективы импортозамещения КИИ в части, касающейся АСУ ТП?». И тогда большинство респондентов (57%) посчитали перспективы импортозамещения скромными. За год ситуация усугубилась – сложной назвали задачу импортозамещения 74%. В прошлом году перспективным назвали процесс импортозамещения 24%, на этот раз доля таких ответов существенно уменьшилась – всего 13%. В такой позиции чувствуется

определенное разочарование в вопросе импортозамещения, однако альтернатив у отечественных асушников практически нет – они вынуждены выполнять требования законодательства по части импортозамещения критически важных объектов. Сейчас этот процесс только начинается, и многие в нем сомневаются. Когда пойдет массовое импортозамещение с помощью подготовленных типовых решений, ситуация и отношение к ней отрасли могут значительно измениться.

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

Всего ответов – 199.

Здесь речь идет о средствах защиты, а не об АСУ ТП. В разработке средств защиты отечественные производители прошли достаточно большой путь, поэтому самым популярным и стал ответ «Продукты есть, не хватает опыта», который выбрали 42% респондентов. При этом доли ответов «Недостаточный, выбор невелик» и «Недостает отдельных классов продуктов» практически сравнялись – по 23%. Интересно, что в прошлом году ответ «Продукты есть, не хватает опыта» был менее популярен – 36%, а вот в 2021 г. его доля составила 52%. Причем ответ «Недостает отдельных классов продуктов» в течение последних трех лет держится на уровне четверти опрошенных специалистов, в то время как неудовлетворенность ассортиментом непрерывно растет: в 2021 г. она составляла 9%, в 2022 г. – 19, сейчас – уже 23%. Ситуация характерна для рынков, которые ограничены в своем развитии и не могут удовлетворить растущий спрос на перспективные технологии. Возможно, отечественным разработчикам все-таки удастся переломить эту неприятную тенденцию.

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

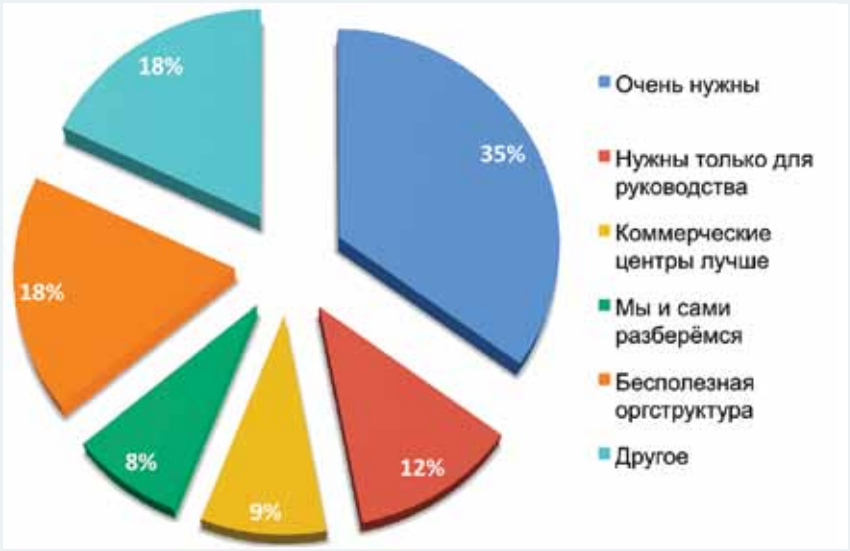
Всего ответов – 198.

Вопросы осведомленности всего персонала предприятия очень важны для обеспечения информационной безопасности, поскольку с помощью одних только специалистов защитить промышленные системы не получится. Необходимо, чтобы все сотрудники предприятия участвовали в соблюдении всех мер информационной гигиены и действовали по инструкциям службы информационной безопасности. На протяжении трех последних лет

наиболее популярным оставался ответ «Недостаточно» с долей в 2021 г. в 49%, в 2022 г. в 46 и в 2023 г. опять долей в 49%. Это небольшие колебания, что говорит о невозможности быстро решить проблемы осведомленности персонала. Колебания показателя достаточной осведомленности также характерны: в 2021 г. он был 17%, в 2022 г. – 29, а в этом откатился до 23%. В противофазе к нему колебался и показатель полной неосведомленности: в 2021 г. он был 25%, в 2022 г. резко снизился до 7, а сейчас также занял срединное положение в 17%. Это скорее говорит о том, что в прошлом году удалось мобилизовать персонал на соблюдение требований информационной безопасности, в то время как до и после ситуация была более расслабленной.

10. Насколько востребованы, по вашему мнению, отраслевые центры ГосСОПКА?

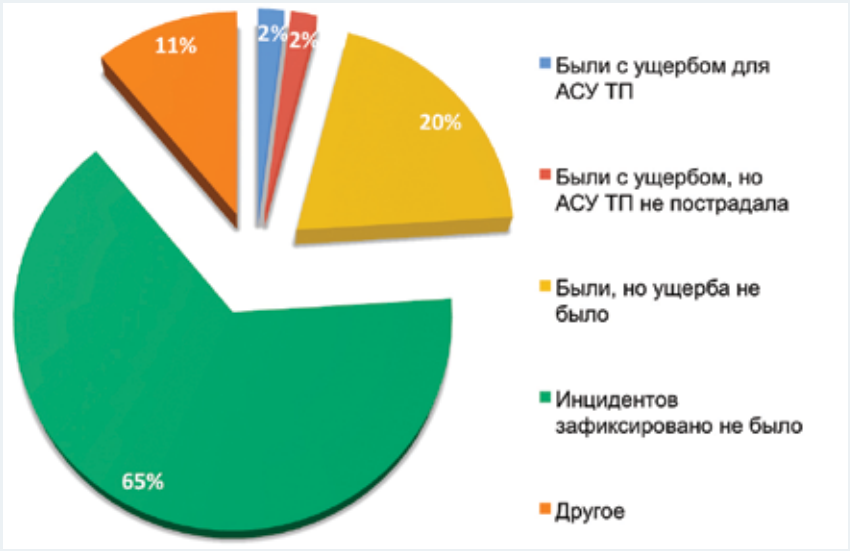
Всего ответов – 190.



Отраслевые центры ГосСОПКА – это тема текущего года. Ее развивают как ФСТЭК, так и отраслевые министерства, поскольку в нескольких постановлениях Правительства РФ было зафиксировано распределение ответственных ведомств по обеспечению информационной безопасности объектов той или иной критической отрасли. Однако далеко не все смогли по достоинству оценить предлагаемые нововведения. Хотя наибольшая доля специалистов считает, что такие центры очень нужны, 18% относится к ним как к бесполезной структуре, еще столько же не смогли определиться. В сумме эти доли составляют 36%, т. е. сомневающихся в данной концепции примерно столько же, сколько и активно поддерживающих ее специалистов. Если отбросить эти крайние точки зрения, то из оставшихся лидерами будут ответы: «Нужны только для руководства» с долей в 12%, любители коммерческих центров с долей в 9 и верящие в собственные силы – 8%. Пока отраслевые центры ГосСОПКА только формируются, поэтому мы будем и дальше наблюдать за процессом становления отраслевой информационной безопасности.

11. Были ли у вашего предприятия или холдинга в 2022 г. инциденты информационной безопасности в части АСУ ТП?

Всего ответов – 88.

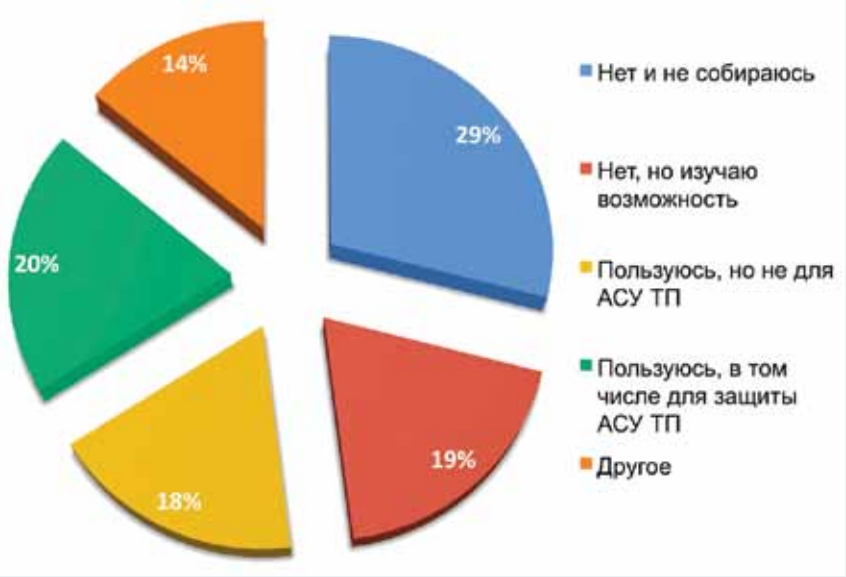


Традиционно самый непопулярный вопрос нашего анкетирования – количество ответов на него каждый раз является минимальным, однако в этом году ситуация изменилась. Два предыдущих года самым популярным ответом был «Инцидентов зафиксировано не было», раньше он держался на уровне 70, сейчас снизился до 65%. На втором месте по популярности – «Были,

но ущерба не было». Его доля увеличилась на 15 в прошлом и позапрошлом годах, сейчас до 20%. Доля ответов «Другое» всегда составляла примерно 10, хотя в прошлом году этот показатель уменьшился до 7%. Аналогично в прошлом году резко выросла сумма двух наименее популярных ответа «Были с ущербом для АСУ ТП» и «Были с ущербом, но АСУ ТП не пострадала». В прошлом году она оказалась на уровне 8%, в то время как 2021 г. этот показатель был всего 1, а сейчас 4%.

12. Пользуетесь ли вы услугами аутсорсинга в области ИБ?

Всего ответов – 187.



Аутсорсинг в сфере информационной безопасности, особенно промышленных объектов, очень важен хотя бы потому, что не хватает высококлассных специалистов по информационной безопасности, которые к тому же разбирались бы в особенностях защиты именно промышленных объектов. Самым популярным ответом последние три года был «Нет и не собираюсь» – в этом году он достиг 29%, хотя в 2022 г. был самым низким с долей в 27. В текущем году на второе место неожиданно вырвался ответ «Пользуюсь, в том числе для защиты АСУ ТП» с долей в 20%, хотя до этого он держался на уровне 14. За последние три года можно отметить неуклонное снижение доли ответа «Нет, но изучаю возможность»: в 2021 г. она составляла 31%, в 2022 г. – 25, сейчас 19%. Доля ответа «Пользуюсь, но не для АСУ ТП» также неуклонно росла: в 2021 г. – 6%, в 2022 г. – 11, а сейчас – 18%. В результате доли ответов «Нет, но изучаю возможность», «Пользуюсь, но не для АСУ ТП» и «Пользуюсь, в том числе для защиты АСУ ТП» практически сравнялись, что говорит о взвешенном подходе отрасли к использованию услуг аутсорсинга информационной безопасности.

13. Как вы оцениваете концепцию кибериммунности промышленных систем и в целом использование встроенных средств безопасности АСУ ТП?

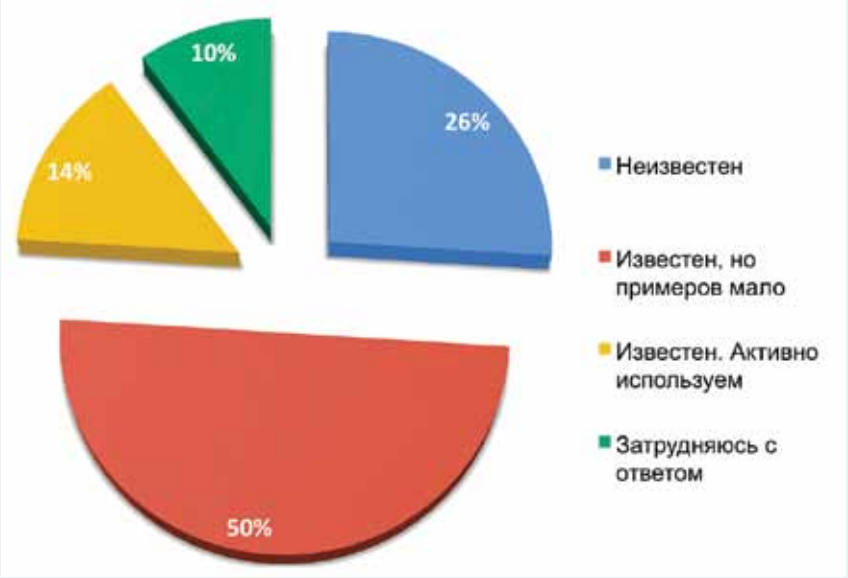
Всего ответов – 184.

Кибериммунные системы изначально были заявлены «Лабораторией Касперского», однако по своей сути это путь к встраиванию эффективных механизмов информационной безопасности прямо в АСУ ТП. Сейчас под кибериммунными подразумевают системы, которые могут самостоятельно, без использования наложенных средств защиты, обеспечить

непрерывность и устойчивость технологического процесса. В этом году мы впервые решили опросить участников конференции об их отношении к концепции киберимунности. Очевидно, что лидером среди ответов стал «Можно использовать вместе с СЗИ» с долей в 54%. Это означает, что большая часть специалистов выступает за создание комплексных решений по безопасности, которые сочетают кибериммунные АСУ ТП с наложенными средствами защиты. На втором месте оказались любители наложенных средств – 13%, адептов кибериммунности оказалось всего 10%. Впрочем, доля не определившихся по этому вопросу оказалась достаточно высокой – 23%. Стоит отметить, что этот вопрос оказался самым непопулярным по количеству ответов. Видимо, актуальность темы противостояния встроенных и наложенных средств защиты сильно преувеличена.

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

Всего ответов – 191.



Этот вопрос существует с самого первого нашего опроса, поскольку вся конференция была затеяна для обмена опытом специалистов по информационной безопасности различных промышленных предприятий. Лидером ответов по данному вопросу стало утверждение, что «Известен, но примеров мало» – сейчас оно оказалось на уровне 50, хотя еще в прошлом году падало до минимума в 40%. Доля ответа «Неизвестен» оказалась самой большой за все время проведения опросов – 26%. Это означает потребность собравшихся на конференции в получении новой информации и обмене опытом работы с ними. Ответ «Известен, активно используем» остался на среднем уровне – годом ранее он был 17, еще раньше – всего 10%.

Таким образом, можно констатировать потребность специалистов АСУ ТП в обмене опытом, который сегодня может стать самым важным компонентом в образовании профильных специалистов. В то же время сейчас законодательство в части распространения информации о проблемах с ИБ идет по пути ужесточения, что ограничивает возможности публичного обмена опытом и совместного решения проблем. Возможно, что из-за угрозы наказания профильные специалисты из предприятий КИИ могут отказаться от обмена опытом и будут учиться только на своих ошибках. В результате может пострадать комплексная безопасность всей промышленной инфраструктуры, поскольку система защищена настолько, насколько защищено ее самое слабое звено.

15. Как вы оцениваете вероятность дальнейшего роста угроз безопасности КИИ со стороны иностранных государств в 2023 г.?

Всего ответов – 217.

Наиболее опасной угрозой для промышленных предприятий стали киберподразделения иностранных государств, которые сейчас концентрируют свои действия на отечественных промышленных предприятиях для введения их в убытки или, как минимум, для нарушения их штатного функционирования. Мы уже три года задаем подобный вопрос, поэтому можем проследить изменение настроений по вероятности нападения именно со стороны иностранных государственных структур, хотя чаще для этого используются такие термины, как «APT-группировки» или «информационные ЧВК». Если в первый год проведения опроса наиболее популярным ответом был «Значительная, но не критичная» с долей в 46%, то уже в прошлом году на первое место вышел ответ «Крайне высокая» с долей в 61. Сейчас накал страстей несколько снизился, и доля этого ответа стала 52% – больше половины респондентов не ожидают ничего хорошего со стороны иностранных

кибергруппировок. Доля ответов «Значительная, но не критичная» в прошлом году упала до 24%, а сейчас опять поднимается почти до стартовых показателей в 39. Возможно, это говорит о том, что промышленность за прошедший год хорошо адаптировалась к постоянной агрессивной среде Интернета и для нее активность международных хакерских группировок становится менее критичной. К тому же построенная система ГосСОПКА показала себя с лучшей стороны, не допустив серьезных инцидентов в самый опасный момент. Будем надеяться, что, несмотря на рост числа угроз для промышленности, он окажется действительно некритичным.

Выводы

Из ответа на первые два вопроса можно сделать вывод о том, что сейчас информационная безопасность интересует прежде всего именно промышленные предприятия, причем не только безопасников, но и самих асушников. Это позволяет надеяться на диалог между этими группами специалистов по выработке новых интересных решений и технологий, которые помогут сделать промышленные сети более защищенными, безопасными и надежными.

Однако ответы на пятый вопрос несколько настораживают: в процессах цифровой трансформации безопасность все чаще настраивается в последний момент. Причем еще в прошлом году требования по защите были едва ли не сутью всех проектов или хотя бы решались на уровне технического задания. Сейчас ситуация опять качнулась в сторону минимизации внимания к проектированию защиты с самого начала.

Новым вопросом анкетирования стал «Насколько востребованы, по вашему мнению, отраслевые центры ГосСОПКА?», который продемонстрировал перспективность и интерес респондентов к теме формирования структуры отраслевых центров ГосСОПКА. Такие структуры и законодательные акты помогут решить отраслевые вопросы обеспечения информационной безопасности промышленных предприятий, что не способны сделать общие регуляторы, в частности ФСТЭК и ФСБ.

Еще одним новым вопросом стал «Как вы оцениваете концепцию кибериммунности промышленных систем и в целом использование встроенных средств безопасности АСУ ТП?», с помощью которого удалось понять отношение общественности к идее встраивания всех средств в саму АСУ ТП. О таких мерах часто говорят сами производители АСУ ТП, требуя использования только собственных средств защиты, которые «максимально адаптированы и протестированы для работы с конкретными системами управления». Однако на деле специалистам безопасности больше нравится идея комплексной защиты АСУ ТП, где частично используются встроенные инструменты защиты, которые работают в связке с классическими наложенными средствами защиты.

Результаты 14-го вопроса показывают, что половина собравшихся на конференции заинтересована в более подробном разборе примеров для подражания и типовых конфигураций. Хотя законодательно такие обсуждения и ограничены, необходимо искать такие форматы обмена опытом, которые позволяли бы помочь неопытным специалистам лучше разбираться в работе отдельных механизмов защиты и во взаимодействии их друг с другом для создания комплексной системы реагирования на компьютерные инциденты. Мы постараемся в следующем году уделить такому обмену опытом больше внимания. ■