



ИТОГИ ОПРОСА

конференции

**«Информационная
безопасность
АСУ ТП КВО»**

Организатор конференции

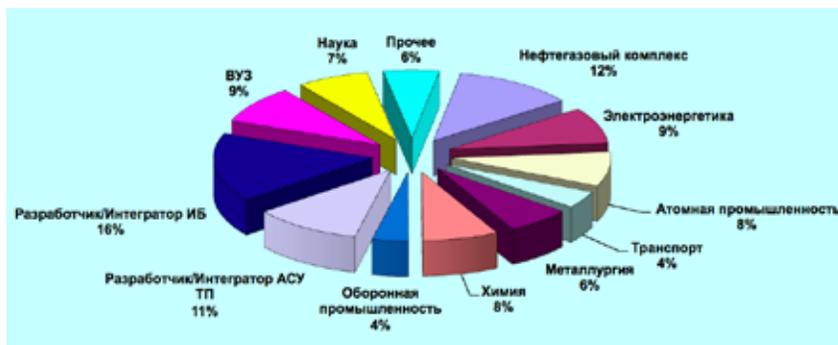
Connect.
ИЗДАТЕЛЬСКИЙ ДОМ

Контролируемая безопасность АСУ ТП

В рамках пятой юбилейной конференции «Информационная безопасность АСУ ТП КВО» Издательским домом «КОННЕКТ» был проведен опрос посетителей с целью выяснить ситуацию с обеспечением информационной безопасности в промышленных системах. В опросе приняли участие 245 респондентов, однако не каждый из них отвечал на все вопросы – это допускалось правилами, поскольку большинство вопросов относилось к клиентам. Всего участники опроса ответили на 11 вопросов по теме информационной безопасности на критически важных объектах.

Вопрос 1. Какую организацию вы представляете?

Первый вопрос, который интересуется любого социолога, – демографический состав отвечающих. В нашем случае оказалось, что небольшая доля принадлежит ИТ- и системным интеграторам – 15,2%, т. е. компаниям, которые занимаются внедрением решений по защите. Однако клиентские компании просто разделены на отдельные сегменты. В целом в опросе фигурировало 116 участников, которые ассоциировали себя с той или иной отраслью критически важных объектов, т. е. почти половина участников (точнее – 47,3%) представляли мнение промышленных компаний, эксплуатирующих различные



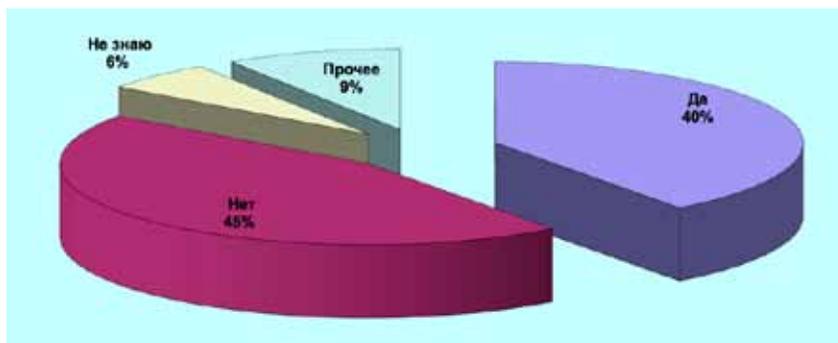
АСУ ТП. Тем не менее разработчиков, интеграторов, ученых и других было достаточно много, что, естественно, могло несколько исказить картину – это нужно иметь в виду. Впрочем, ответы разработчиков и интеграторов как компаний, обслуживающих

несколько клиентов, можно воспринимать в качестве обобщения, не сильно искажающего финальную цифру. Их представители, скорее всего, говорили не о своей компании, а о знакомых им проектах по защите критически важных объектов.

Вопрос 2. Является ли ваша организация оператором критически важных объектов?

Всего участников 206. Этот вопрос также является демографическим, поскольку его цель – определить, сколько участников опроса действительно относят свою компанию к критически важным объектам.

Положительных ответов – 82 (39,8%). При этом из 116 отраслевых участников доля КВО оказалась довольно существенной. Участники, ответившие «нет», – таких большинство (92), скорее всего, являются как раз теми самыми интеграторами либо разработчиками средств ИБ или

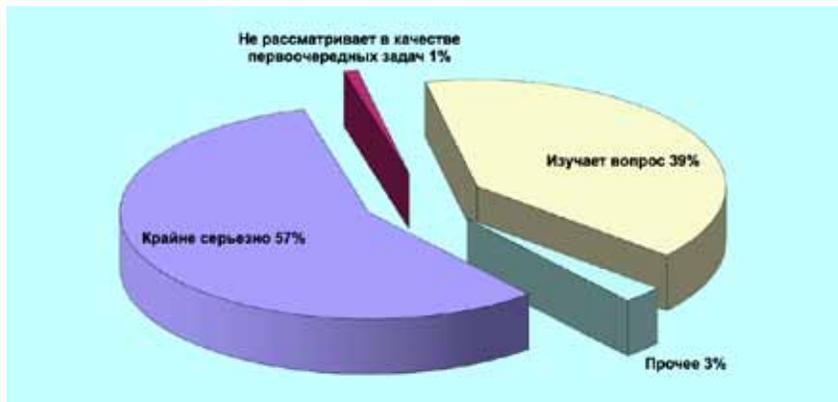


АСУ ТП. Как уже было отмечено, вероятно, на следующие вопросы они отвечали не про свою организацию, а обобщили опыт своих клиентов КВО. Вполне возможно, что они как разработчики

и внедренцы заинтересованы в повышении показателей защищенности. Впрочем, и сами представители КВО могли отвечать чуть лучше, чем есть на самом деле.

Вопрос 3. Насколько серьезно ваша организация относится к проблематике ИБ АСУ ТП?

Всего участников 225. На этот вопрос ответило максимальное число участников, если не считать первого вопроса. Этот факт сам по себе отражает заинтересованность отвечающих. Показательно, что 89 ответивших (40%) изучают вопрос: можно предположить, что это именно клиенты, которые исследуют рынок, т. е. представители КВО, заинтересованные в развитии средств защиты своих систем. При этом подавляющая доля (56,9%) – те, кто крайне серьезно относится к проблематике ИБ АСУ ТП. Видимо,

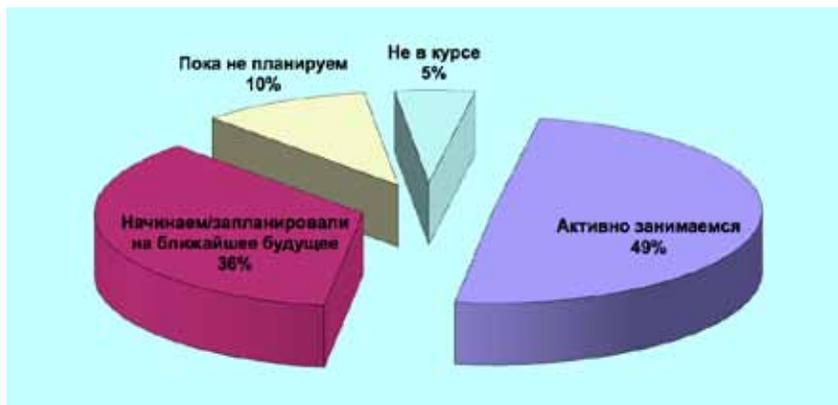


это разработчики средств безопасности, АСУ ТП и др. И лишь 0,9% (всего два ответа) не рассматривают безопасность в качестве

первоочередной задачи. Вероятно, эти двое являются клиентами, но, возможно, и производителями АСУ ТП.

Вопрос 4. Приступили ли на вашем предприятии к практической реализации мер по защите АСУ ТП?

Всего участников 208. Из них почти половина – 103 человека (49,5%) – ответили, что уже активно занимаются внедрением средств защиты АСУ ТП. Еще 35,6% запланировали внедрение на ближайшее будущее. Эти цифры говорят о том, что процесс аудита безопасности уже идет и в его рамках должны быть выработаны меры по обеспечению защиты. Ответы «пока не планируем» и «не в курсе», возможно, относятся не к КВО, а к другим классам отвечающих, например

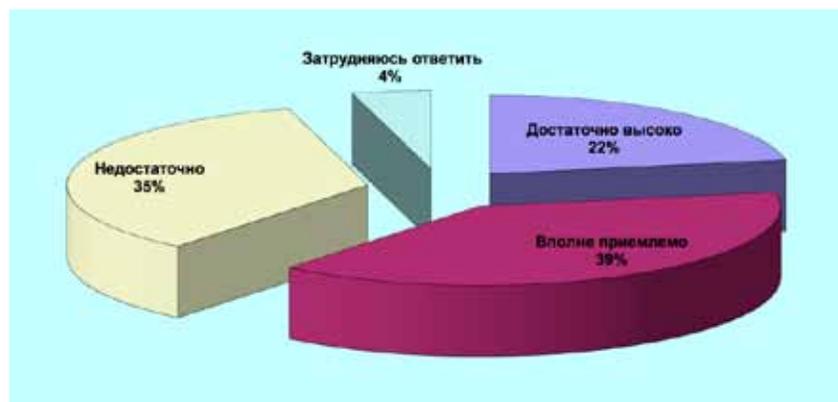


представителям вузов. Таким образом, можно констатировать, что промышленные предприятия, тем более

критически важные объекты, активно занимаются внедрением средств защиты производственных систем.

Вопрос 5. Как вы оцениваете на сегодня собственный уровень компетенции в сфере ИБ АСУ ТП?

Количество участников 212. Достаточно высоко оценивают свой уровень всего 22,2% посетителей, что говорит о потребности дальнейшего накопления компетенций и развития технологий. Даже на профильной конференции по безопасности собрались люди, которые оценивают свой уровень компетенции как «приемлемый» – таких оказалось 38,7%. При этом остается еще достаточно высоким процент тех, кто считает свой уровень компетенции неприемлемым, – 34,9%,



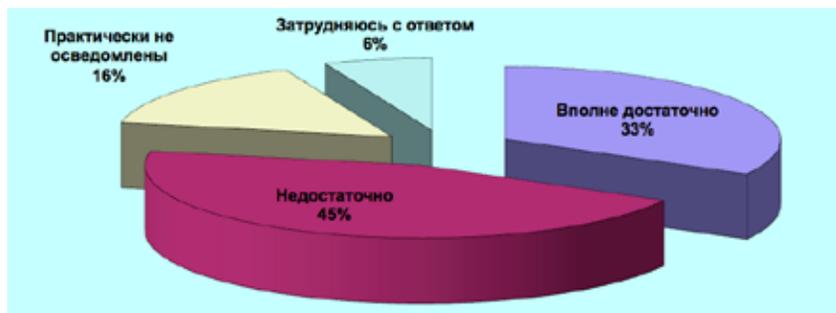
т. е. чуть больше трети. Таким образом, просвещение в области обеспечения защиты информационных систем, в частности

специалистов в сфере АСУ ТП, по-прежнему актуально. Именно для этого и предназначена наша конференция.

Вопрос 6. Как вы оцениваете уровень осведомленности персонала вашего предприятия в области защиты АСУ ТП?

Количество участников 206.

Почти треть ответивших (33,1%) считают, что персонал предприятия достаточно осведомлен о проблемах безопасности АСУ ТП. Возможно, это как раз представители компаний, эксплуатирующих АСУ ТП. Впрочем, наиболее популярным ответом все-таки является «недостаточно» – с долей 45,1%, еще 15,5% полагают, что персонал вообще ничего не понимает в информационной безопасности. Следует отметить, что для повышения осведомленности персонала не требуется внедрять никаких решений – достаточно обучить



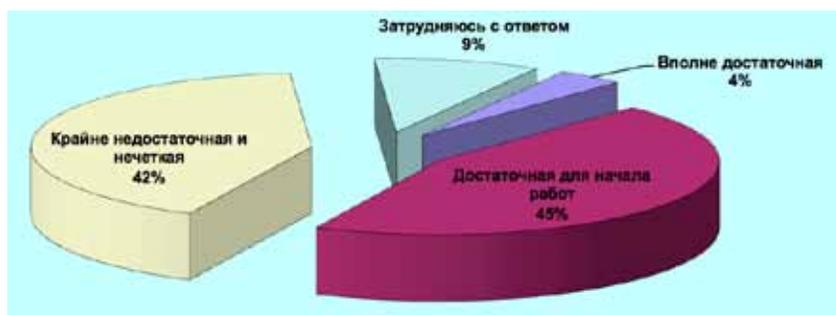
производственных специалистов и провести пару учебных тревог. В то же время именно повышению осведомленности компании уделяют внимание в последнюю очередь, хотя это можно сделать с самого начала без значительных затрат средств на покупку продуктов и консалтинг.

Вполне возможно, что после улучшения осведомленности эффективность уже используемых средств защиты существенно повысится. В то же время 6,3% безопасников вообще ничего не знают об осведомленности персонала по проблемам защиты АСУ ТП.

Вопрос 7. Как вы оцениваете нормативно-правовую базу в сфере ИБ АСУ ТП?

Количество участников 209.

Данный вопрос важен по той причине, что на конференции несколько раз высказывалось следующее мнение: службе безопасности не удастся убедить начальство в необходимости внедрения средств защиты, поскольку требования законодательства «мутные». Однако опрос показывает, что больше всего участников (45,0%) считает, что имеющихся документов вполне достаточно для начала работы, еще 3,8% полагают, что необходимости



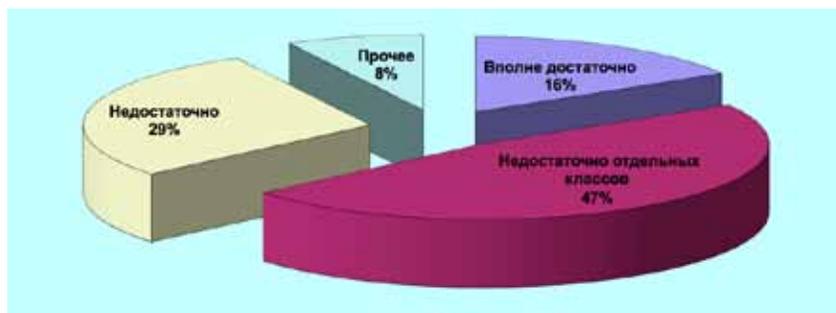
в дальнейшем их совершенствовании нет. В то же время 41,6% все-таки не уверены в безупречности нормативно-правовой базы и не торопятся реализовывать существующие требования,

ождая дальнейших разъяснений. Доля сомневающихся достаточно велика, поэтому потребность в дальнейшем совершенствовании законодательства в сфере защиты АСУ ТП все-таки остается.

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

Количество участников 207.

По мнению 16,4% специалистов, существующих средств защиты вполне достаточно для обеспечения безопасности АСУ ТП, хотя большинство посетителей (47,3%) конференции все-таки считают, что отдельных классов продуктов не хватает. Скорее всего, речь идет о технологиях защиты, оптимизированных под использование в конкретных системах АСУ ТП. Разработчики систем управления технологическими процессами часто требуют сертификации средств



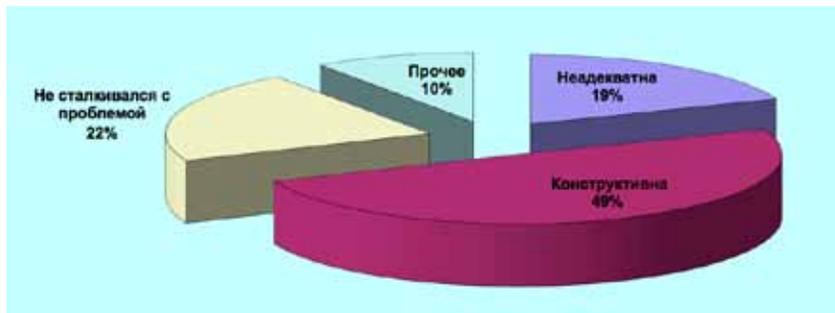
защиты на совместимость с их решениями, а иногда могут и снять с сопровождения систему, в которой установлено несертифицированное средство защиты. В то же время готовых комплексных решений

реализовано не так много. Тем не менее процесс проверки совместимости и создания специализированных продуктов уже запущен, и, возможно, вскоре доля неудовлетворенных специалистов уменьшится.

Вопрос 9. Насколько адекватна, исходя из вашего опыта, реакция производителей производственного оборудования на предложения по взаимодействию в области защиты АСУ ТП?

Количество участников 204.

Этот вопрос можно считать продолжением предыдущего в части выработки средств защиты для АСУ ТП. Конструктивная позиция (за нее проголосовали 49,5% отвечающих) в данном случае наиболее предпочтительна, поскольку предполагает выработку совместных решений разработчиков средств защиты и самой АСУ ТП. Впрочем, достаточно много отвечающих (21,6%)



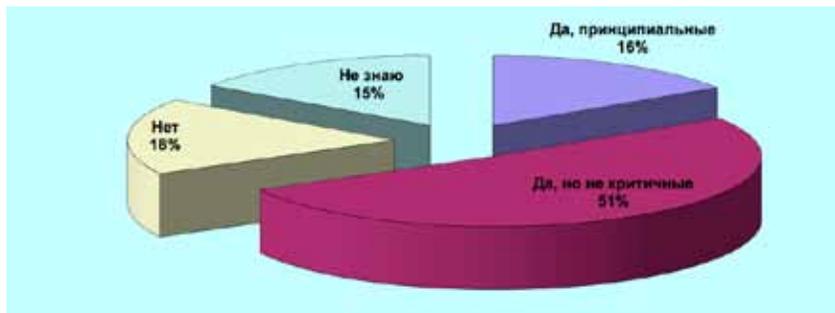
вообще не сталкивались с проблемой. И только в 19,1% случаев реакция была неадекватной – показатель достаточно высокий, но назвать его значительным все-таки нельзя. Это означает, что диалог между владельцами

промышленных систем, разработчиками средств защиты и АСУ ТП идет, следовательно, можно надеяться на улучшение ситуации с защищенностью промышленных объектов, особенно отнесенных к КВО, в самое ближайшее время.

Вопрос 10. Есть ли на вашем предприятии проблемы в понимании и расхождении позиций служб АСУ ТП и служб ИБ в отношении защиты АСУ ТП?

Количество участников 176.

Следует отметить, что на этот вопрос ответило меньше всего участников. Конфликты между службами ИБ и АСУ ТП сильно затрудняют и замедляют реализацию проектов по защите промышленных систем. Поэтому 17,6% ответивших «нет» – хороший знак. Во всяком случае, доля проектов с критическим разногласиями несколько меньше – 15,9%. Наиболее популярный ответ (51,1%) подтверждает наличие некоторых разногласий между



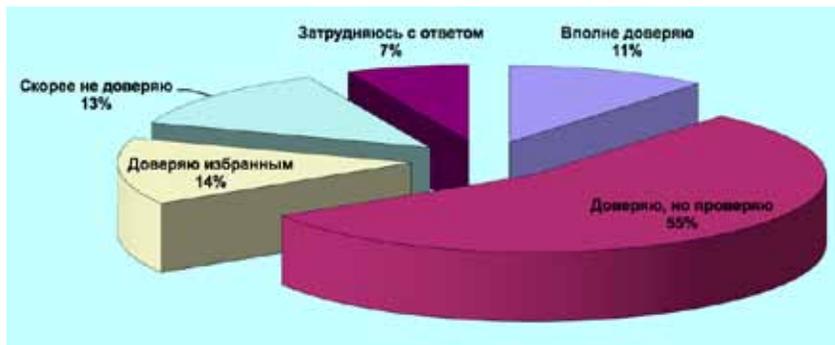
безопасниками и производственными службами, но разногласия эти не критические, что говорит о возможности выработки более взвешенных и конструктивных решений. В конце концов, для предприятий важен выпуск продукции,

а безопасность производства необходимо обеспечить как раз для недопущения аварий и остановок промышленных процессов. Поэтому именно безопасность необходимо подстраивать под производство, а не наоборот.

Вопрос 11. В какой мере вы доверяете предложениям разработчиков/интеграторов в области защиты АСУ ТП?

Количество участников 184.

Ответ «вполне доверяю» подразумевает, что в компании практически нет собственных экспертов по защите АСУ ТП, поэтому ей приходится доверять внешней экспертизе. К счастью, таких компаний минимум – 11,1%. С некоторой настороженностью к предложениям разработчиков средств защиты и интеграторам относятся еще 13,0% респондентов. Впрочем, все-таки больше тех производственных компаний, которые хотя бы



выбирают интегратора или разработчика (14,0%). Однако подавляющее большинство компаний (55,1%) имеют собственных экспертов в области безопасности, которые

занимаются проведением собственных проверок предлагаемых решений. Последний подход является наиболее взвешенным, хотя и требует дополнительных расходов.

Заключение

Результаты опроса показывают, что ситуация с пониманием проблем информационной безопасности на промышленных объектах достаточно хорошая – идет конструктивная работа, о чем свидетельствуют ответы на вопросы 3, 4, 5, 7 и 10. Ощущаются определенные проблемы с требованиями регуляторов, но большинство все-таки понимают необходимость активных действий по защите. В рамках реализации требований приказа № 31 ФСТЭК многие уже начали, как минимум, аудит информационных систем АСУ ТП на защищенность. Ожидается, что законопроект по критической

информационной инфраструктуре дополнительно прояснит ситуацию с законодательными требованиями и, возможно, сделает их обязательными.

Разработчикам промышленных систем, исходя из ответов на 9-й вопрос, следует более адекватно относиться к запросам на обеспечение безопасности их решений. Тем не менее работа по аудиту и интеграции средств защиты в АСУ ТП уже идет – этот рынок явно будет расти в самое ближайшее время. Когда требования по информационной безопасности станут обязательными, реализация мер защиты в АСУ ТП будет конкурентным преимуществом производителя.

Самим предприятиям стоит обратить внимание на осведомленность персонала: эта организационная мера не требует больших расходов, но способна повысить эффективность уже установленных средств защиты. Интеграторам и разработчикам средств защиты, исходя из ответов на 11-й вопрос, стоит поработать над имиджем собственных предложений в сфере безопасности АСУ ТП и продемонстрировать успехи в решении наиболее сложных проблем. В целом можно отметить, что за пять лет существования конференции ситуация в сфере информационной безопасности критически важных объектов улучшается. ■