ИТОГИ ОПРОСА

XIII КОНФЕРЕНЦИИ

«Информационная безопасность АСУ ТП критически важных объектов»

2025 г.

Организатор конференции
Connect
ИЗДАТЕЛЬСКИЙ ДОМ

Траектория безопасности критически важных объектов в цифровом мире

На 13-й конференции «Информационная безопасность АСУ ТП КВО», организованной Издательским домом «КОННЕКТ», наиболее активно делегаты обсуждали тенденции на рынке средств защиты АСУ ТП в свете законодательных требований по обязательному импортозамещению ПО и использованию программно-аппаратных комплексов на значимых объектах КИИ. Безопасность в цифровом мире – задача со многими неизвестными. Алгоритмы поиска возможных решений приходится корректировать по мере развития рыночной ситуации и осмысления опыта обеспечения безопасности объектов критической информационной инфраструктуры. За последнее время основной вектор кибератак сместился с субъектов КИИ на их подрядчиков, партнеров и персонал. Не первый год Издательский дом «КОННЕКТ» проводит опрос участников конференции, чтобы сформировать представление о тенденциях на рынке средств защиты для промышленных информационных систем и АСУ ТП. Не стала исключением и 13-я конференция.

Вопрос 1. Какую организацию вы представляете?

Голосов – 278.

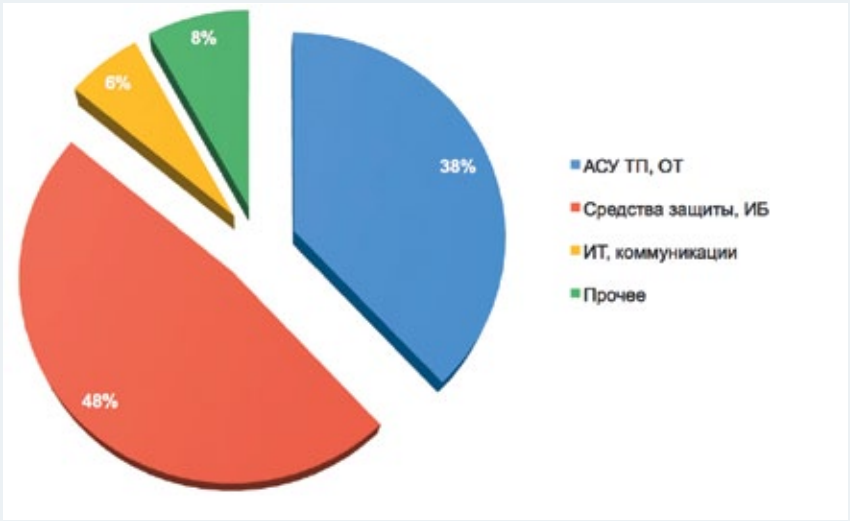
В этом году количество ответивших на первый вопрос уменьшилось (с 346 до 278). Наибольший интерес к тематике конференции проявили представители компаний ТЭК (26%). На втором месте респонденты из группы «Прочее» (20%). За ними – разработчики/интеграторы ИБ (18%). С заметным отрывом от них идут металлурги (9%), разработчики/интеграторы АСУ ТП (7%), сотрудники предприятий химической промышленности (6%), транспортных компаний (5%), ракетно-космической индустрии (4%), вузов (3%), научных учреждений (2%).

В прошлом году по количеству ответивших на этот вопрос лидировали представители компаний – разработчиков/интеграторов (20%), на второй позиции были специалисты из нефтегазового комплекса (15%), на третьей – оборонной промышленности (12%). Четвертое место разделили металлурги и сотрудники прочих компаний, предприятий, организаций (по 10%). На пятом месте были химики и электроэнергетики (по 9%). Вслед за ними шли представители атомной промышленности (8%). Значительно меньше было сотрудников вузов и научных организаций (4%), а также работников транспортной сферы (3%).

Таким образом, примерное распределение аудитории конференции по отраслям и сегментам прежнее с небольшим различием по количественному составу. При этом интерес к тематике информационной безопасности критически важных объектов не ослабевает.

Вопрос 2. Какие системы на предприятии находятся в сфере вашей ответственности?

Голосов – 239



Как и следовало ожидать, ответы распределились предсказуемо. На первом месте средства защиты, ИБ (48%), на втором – АСУ ТП, ОТ (38%), на третьем – вариант «Прочее» (8%). Четвертая позиция с 6% – за системами в сфере ИТ и коммуникаций.

Ровно такая же картина наблюдалась год назад. Лидировали средства защиты, ИБ (39%), на втором месте – АСУ ТП, ОТ (37%), на третьем – категория «Прочее» (11%). С заметным отрывом шли ИТ, коммуникации (7%) и пользователи различных систем (6%). Схожая ситуация наблюдалась и в позапрошлом году. Однако на этот раз изменилось процентное отношение: первое место «подросло» с 39 до 48%, а третье, напротив, пошло вниз с 11 до 8%.

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

Голосов – 260

Как и в минувшем году, лидирующие позиции сохранил за собой Федеральный закон № 187-ФЗ «О безопасности КИИ» (43%). На втором месте постановление Правительства РФ № 1912 (16%), на третьем – Методические документы ФСТЭК России (12%). Вслед за ними Указ Президента РФ № 250 (9%) и документы категории «Другое» (8%). Затем по убывающей идут требования внутренних документов или контрагентов (5%), отраслевых российских регуляторов (4%) и Указ Президента РФ № 166 (3%).

Почти такое же распределение было характерно и для прошлогоднего опроса. Половина всех ответов пришлась на Федеральный закон № 187-ФЗ «О безопасности КИИ», второе место разделили постановление Правительства РФ № 1912 и Методические документы ФСТЭК России (по 11%), на третьем был Указ Президента РФ № 250 и документы категории «Другое» (по 8%). С отставанием в один процент шел Указ Президента РФ № 166. В конце перечня значились требования отраслевых российских регуляторов (4%) и внутренних документов или контрагентов (2%).

Требования законодательства в новых геополитических условиях стимулируют развитие сегмента информационной безопасности в нашей стране. На конференции отмечалось, что прежде при обсуждении вопросов кибербезопасности ИБ-специалисты сталкивались с сопротивлением со стороны сотрудников по эксплуатации. Сейчас наблюдается движение в общем направлении, когда инструменты ИБ встраиваются в общую модель управления рисками бизнеса. Немалую роль в этом сыграло ужесточение санкций за неисполнение требований законодательства в области КИИ, введение обязанности проводить регулярный контроль защищенности.

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

Голосов – 212

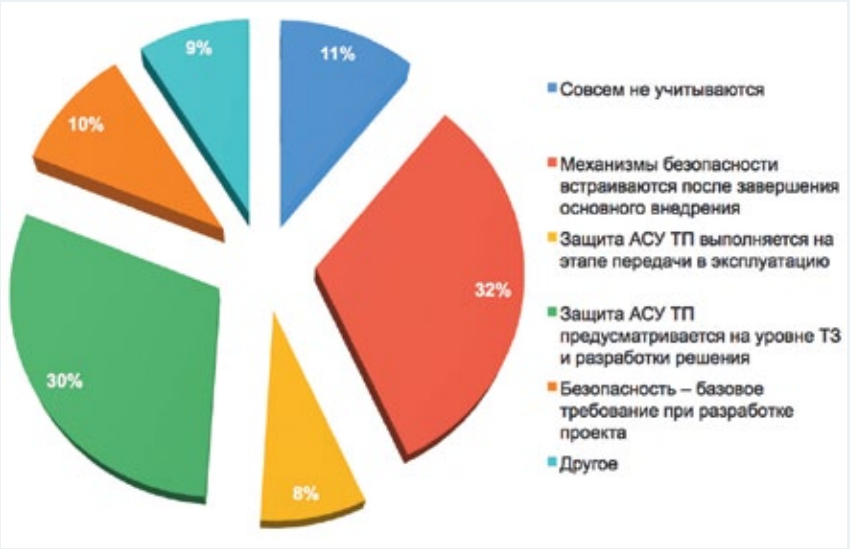
Неожиданностей ответы на этот вопрос не принесли. С опасением ИБ-специалисты по-прежнему относятся к облачным технологиям (40%), промышленному Интернету вещей (20%) и искусственному интеллекту (16%). Четвертое место разделили отечественная электроника и вариант «Другое» (по 9%). На пятой позиции с одинаковым результатом (по 3%) – роботы, ЧПУ-станки, 3D-принтеры и цифровые двойники.

Мнения участников конференции о рисках, связанных с цифровыми технологиями, почти не изменились. Разве что градус настороженности к облачным технологиям подскочил (с 31 до 40%). А применительно к промышленному Интернету вещей и искусственному интеллекту, напротив, наметилось движение вниз, пусть и незначительными темпами (в первом случае на 1%, во втором – на 3%).

Недоверие к облакам усиливалось по ряду причин. Достаточно вспомнить, как на фоне введения санкционных ограничений зарубежные провайдеры блокировали доступ к облачным ресурсам. В предыдущие годы таких фактов было достаточно, чтобы сформировать настороженное отношение к технологии. За последнее время значительно увеличилось количество кибератак на объекты критической информационной инфраструктуры, атаки стали более изощренными. Один из актуальных трендов состоит в том, что злоумышленники все активнее используют искусственный интеллект для реализации целенаправленных атак. По словам экспертов, одно из наиболее опасных направлений – развитие интеллектуальных фишинговых атак.

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

Голосов – 224

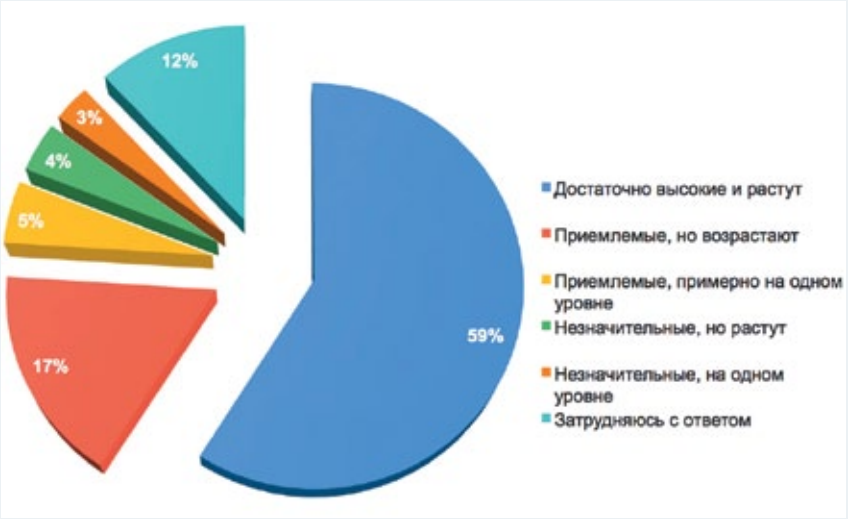


При ответе на этот вопрос превалировали две точки зрения с почти равным числом респондентов. Первая – «Механизмы безопасности встраиваются после завершения основного внедрения» (32%), вторая – «Защита АСУ ТП предусматривается на уровне ТЗ и разработки решения» (30%). Почти втрое меньше ответивших считают, что «совсем не учитываются» (11%). 9% выбрали вариант ответа «Другое» и столько же согласились с тем, что безопасность – базовое требование при разработке проекта. 8% полагают, что защита АСУ ТП выполняется на этапе передачи в эксплуатацию.

Неожиданностей в структуре мнений не наблюдается, ситуация аналогичная прошлогодней. АСУ ТП становятся все более сложными, интегрируются с внешними системами и сервисами, что увеличивает их уязвимость. Среди наиболее актуальных задач участники конференции отмечали необходимость создания архитектурных решений, которые будут служить базой для проектирования защищенных АСУ ТП на предприятиях различного масштаба. Критериями оценки могут служить наличие механизмов защиты, инструментов мониторинга и реагирования, соответствие требованиям законодательства РФ, отказоустойчивость и восстановление (резервирование критических компонентов), совместимость с другими системами.

Вопрос 6. Как вы оцениваете затраты на выполнение требований по защите АСУ ТП как части КИИ предприятия и какова их динамика?

Голосов – 218



Подавляющее большинство ответивших отдали предпочтение варианту «затраты достаточно высокие и растут» (59%). В 2024 г. таковых было 60%, в 2023 г. – 47%, в 2022-м – 23%, в 2021-м – 27%. Тренд весьма красноречив, и едва ли требует дополнительных комментариев. 17% считают затраты приемлемыми, но возрастающими. 12%, как и в прошлом году, затруднились с ответом. Приемлемыми, примерно на одном уровне назвали затраты лишь 5% ответивших, на 1% меньше тех, кто считает их незначительными, но растущими. И лишь 3% выбрали вариант ответа «Незначительные, на одном уровне».

Надежная защита АСУ ТП крайне важна, так как речь идет об управлении жизненно важными процессами в любом промышленном сегменте. Взлом или нарушение работы таких систем в энергетике, водоснабжении, других отраслях может обернуться аварийными ситуациями, которые сопровождаются не только нарушением непрерывности бизнеса, экономическими потерями, но и человеческими жертвами. Ужесточение нормативных требований к защите АСУ ТП требует дополнительных финансовых расходов, несмотря на рекомендации экспертов проектировать системы на основе унифицированных решений.

В последнее время дает о себе знать дефицит кадров на всех направлениях кибербезопасности. Переквалификация ИТ-сотрудников в ИБ-специалистов требует времени и иных ресурсов на обучение и повышение квалификации (в условиях постоянно меняющихся угроз и появления новых технологий), что сопряжено с дополнительными расходами. Платить за безопасность приходится, чтобы в последующем не расплачиваться за отсутствие средств и инструментов защиты.

Вопрос 7. Есть ли у вас четкое понимание, как рассчитывать показатель состояния защиты информации и обеспечения безопасности объектов КИИ?

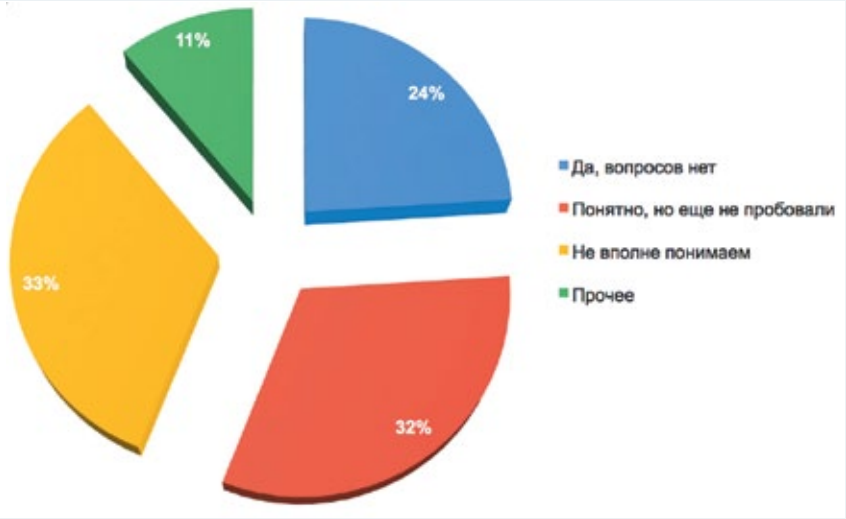
Голосов – 214

В этом году анкета была дополнена вопросом о расчете показателя состояния защиты информации и обеспечения безопасности объектов КИИ. Треть ответивших (33%) признались, что четкого понимания методики нет. Примерно столько же (32%) утверждают, что им понятно, как произвести расчет, но они не пробовали это делать. 24% ответили утвердительно (да, вопросов нет). 11% предпочли «скрыться» за вариантом «Прочее».

ФСТЭК разработала методику оценки текущего состояния защиты информации (обеспечения безопасности объектов КИИ) в государственных органах, органах местного самоуправления, организациях, в том числе субъектах

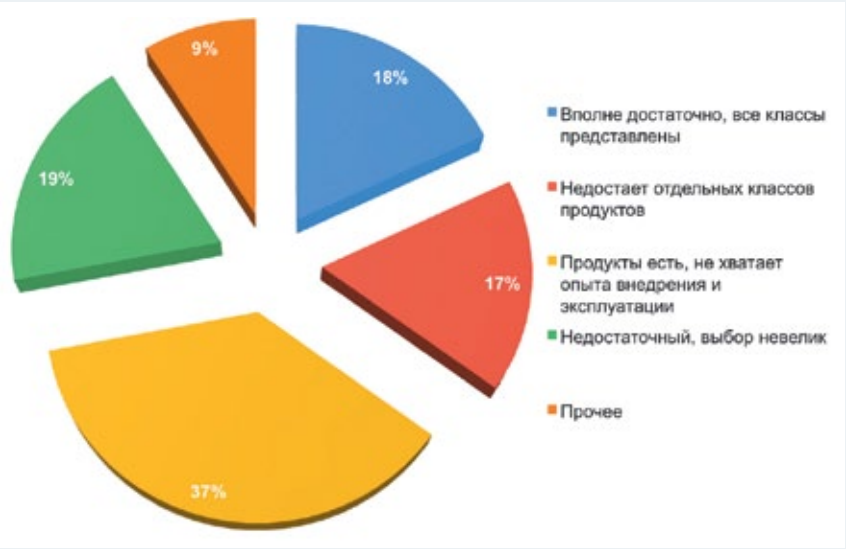
критической информационной инфраструктуры (Методика утверждена Приказом ФСТЭК от 02.05.2024).

Показатель текущего состояния защищенности (КЗИ), характеризующий текущее состояние защиты информации, должен стремиться к единице. ФСТЭК предложены градации защищенности. Полученное согласно методике значение показателя защищенности КЗИ служит критерием принятия в организации управленческих решений. Они могут быть связаны, в частности, с необходимостью реализации первоочередных мер по защите информации (обеспечению безопасности объектов КИИ) от угроз, их приоритетности и т. д.



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

Голосов – 227



С большим перевесом победила точка зрения «Продукты есть, не хватает опыта внедрения и эксплуатации» (37%). Разрыв между вторым, третьим и четвертым местами минимален – всего по 1%. Вариант «Недостаточный, выбор невелик» предпочли 19% ответивших. Для 18% ситуация благоприятная: «Вполне достаточно, все классы представлены». 17% аудитории недостает отдельных классов продуктов. Почти вдвое меньше (9%) выбрали вариант «Прочее».

В минувшем году наиболее популярным был ответ «Продукты есть, не хватает опыта внедрения и эксплуатации» (36%). На нехватку отдельных классов продуктов указали 27% опрошенных. 21% выбрали вариант «Недостаточный, выбор невелик». Удовлетворены ассортиментом 10% ответивших. Если оценивать ситуацию ретроспективно, то рост количества неудовлетворенных ассортиментом продуктов и услуг по информационной безопасности АСУ ТП сохранялся на протяжении четырех лет: в 2021 г. – 9%, в 2022-м – 19%, 2023-м – 23%, 2024-м 27%. На этот раз зафиксировано снижение данного показателя (с 27 до 19%).

Расширение мощностей промышленных предприятий требует полномасштабной автоматизации управления технологическими процессами и производством. После ухода иностранных производителей российский рынок оказался на перепутье. С 2022 г. рискованно ориентироваться на иностранные программно-аппаратные решения для АСУ ТП (дают о себе знать невозможность обновления ПО и прекращение технической поддержки). Госрегулирование в сфере автоматизации стимулирует создание собственных разработок в этой области, что требует инвестиций и времени. А это, в свою очередь, сдерживает спрос со стороны конечных заказчиков на отечественные решения.

Вопрос 9. Есть ли у вашего предприятия план перехода на доверенные ПАКи для КИИ? Как вы оцениваете их ассортимент на рынке?

Голосов – 207

Этот вопрос впервые был включен в анкету. 35% ответивших сообщили, что план есть, ассортимент скудный. 20% пока не приступали к составлению плана. 19% предпочти ответ «Прочее». 17% аудитории готовят план перехода. У 9% ответивших план есть, и ассортимент они считают достаточным.

АСУ ТП относятся к критической информационной инфраструктуре. Постановлением Правительства № 1912 ограничивается использование иностранных программно-аппаратных комплексов в отношении значимых объектов КИИ к 2030 г. При этом следует учитывать, что российский сегмент АСУ ТП развивается в условиях отсутствия собственной компонентной базы, недостаточного финансирования исследований и разработок. Скромный выбор отечественных предложений заставляет предприятия тестировать решения новых поставщиков, в том числе из дружественных стран, в частности, Китая.

До 1 января субъекты КИИ были обязаны направить в федеральный орган исполнительной власти копию плана перехода на доверенные ПАК (по действующим значимым объектам КИИ). В отношении новых ЗО КИИ, получивших или изменивших категорию после 1 сентября 2024 г., копия направляется в течение четырех месяцев. При каждом изменении категории объекта нужно будет повторять процедуру, так как внесение изменений в план перехода выполняется путем утверждения плана в новой редакции. Со следующего, 2026 г., субъектам КИИ предстоит ежегодно в срок до 1 марта направлять отчет о том, как реализуется план перехода на доверенные ПАК за прошедший год.

В профессиональном сообществе обсуждается вопрос, как стимулировать применение ПАК отечественного производства. Среди наиболее дискуссионных инициатив – предложение передать функцию присвоения категории значимости объектов критической информационной инфраструктуры от субъекта КИИ внешнему органу.

Вопрос 10. Есть ли у вас опыт применения российских NGFW, в том числе в интересах ИБ АСУ ТП? Как они себя показали?

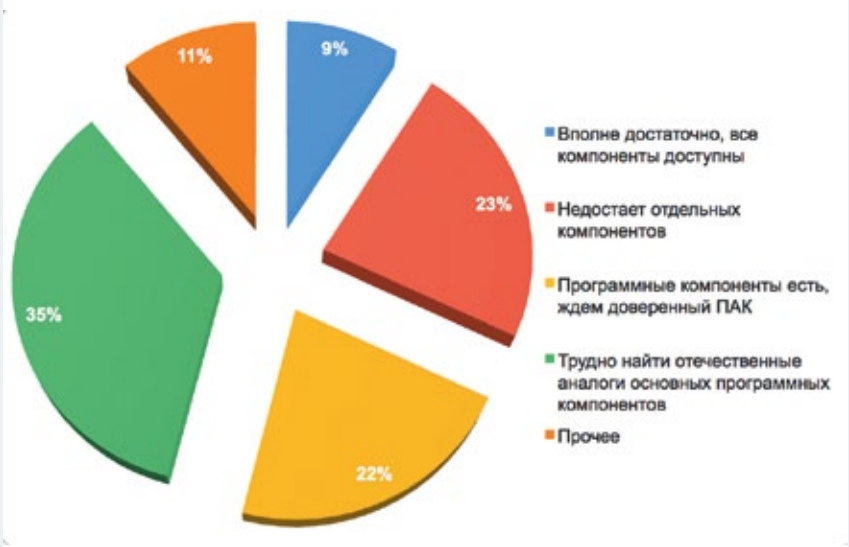
Ответов – 202

На этот, еще один новый вопрос анкеты без малого половина (47%) респондентов затруднились с ответом. 23% сообщили, что пока тестируют российские NGFW и столько же (23%) признали наличие опыта, но результаты скромные. Лишь 7% ответивших выбрали вариант «Есть, показали отлично».

Примечательно, что Банк России совместно с отечественными банками протестировал российские межсетевые экраны (NGFW). По словам представителя ЦБ, результаты оказались лучше ожидаемого. Ситуация с инструментами фильтрации сетевого трафика и защиты данных от несанкционированного доступа не критическая, но они требуют доработок. Банки предоставили инфраструктуру для испытаний, а в ходе тестов определились ведущие производители NGFW. К слову, из-за жесткой методики тестирования часть потенциальных разработчиков отказались участвовать испытаниях. Требования к производительности NGFW остаются высокими. В тестовых условиях характеристики подтверждаются, однако под серьезной нагрузкой проблемы дают о себе знать. У части решений обнаружены ошибки в ПО. Ключевая проблема российских NGFW – низкая пропускная способность.

Вопрос 11. Как вы оцениваете доступность и ассортимент отечественных продуктов для АСУ ТП в свете требований по импортозамещению для КИИ?

Голосов – 186



Трудно найти отечественные аналоги основных программных компонентов – такому варианту ответа отдали предпочтение 35% ответивших. На втором месте с 23% сторонники точки зрения о том, что недостает отдельных компонентов. Всего 1% уступают им приверженцы мнения, что программные компоненты есть, нужно дождаться доверенного ПАК. 11% завуалировали свою точку зрения вариантом ответа «Прочее». 9% ответивших полагают, что ассортимент достаточен, все компоненты доступны.

По сравнению с прошлым годом на 8% уменьшилось количество тех, кто затрудняется с поиском отечественных аналогов основных программных компонентов. В то же время на 3% возросло число выбравших вариант «Недостает отдельных компонентов». Примечательно, что в три раза увеличилось количество оптимистов, считающих, что ассортимента вполне достаточно, все компоненты доступны.

Ключевым драйвером данного сегмента рынка служит реализация планов перевооружения крупных предприятий. Госкомпании и субъекты КИИ последовательно реализуют проекты по импортозамещению, включая внутреннюю разработку программных решений. Как правило, они уверены, что подходящих решений в области промышленной автоматизации достаточно. Ряд предприятий занимаются собственной разработкой в надежде избежать дополнительной нагрузки на бюджет и сэкономить на приобретении ПО у внешних поставщиков. Частные корпорации занимают выжидательную позицию в рамках импортозамещения в расчете на то, что со временем повысится зрелость новых решений, предлагаемых отечественными разработчиками. При выборе поставщика промышленные предприятия ориентируются на три основных критерия: отказоустойчивость решения, надежность поставки и своевременная техподдержка.

Вопрос 12. Видите ли вы перспективы применения средств искусственного интеллекта в области ИБ АСУ ТП?

Голосов – 203

Почти треть (32%) ответивших скептически настроены по отношению к ИИ в ИБ АСУ ТП, поскольку выбрали вариант «практически незначительные». 29% сказали: «Да, но пока ограниченные». Немалая доля (23%) тех, кто затруднился с ответом. 16% видят перспективы применения средств искусственного интеллекта в области ИБ АСУ ТП, причем большие.

Каких бы полярных точек зрения об ИИ не придерживались ИБ-специалисты, искусственный интеллект настойчиво проникает

в повседневность, предъявляя дополнительные требования к навыкам человека. Наличие локальных ИИ-моделей, интегрированных с открытыми достоверными источниками информации, позволяет повышать производительность труда и освобождать квалифицированных специалистов от выполнения рутинных операций.

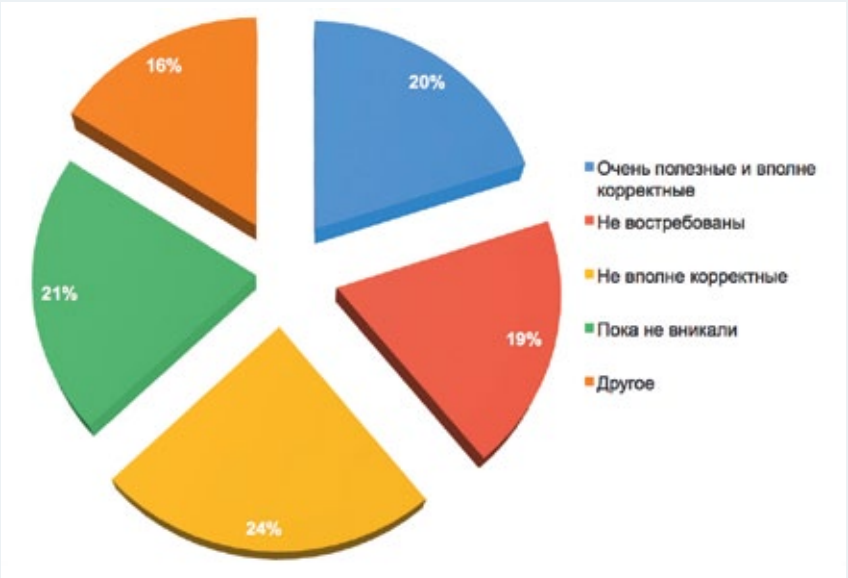
С ИИ эксперты связывают дополнительные возможности в области автоматизации процессов и цифровой трансформации производственных участков. Ассортимент ИИ-решений на рынке постоянно расширяется. Предприятиям рекомендуется обратить внимание на потенциал ряда технологических направлений с данной области. В частности, виртуальные помощники (или цифровые ассистент-системы) способны автоматизировать технологические и бизнес-процессы. Обнаружить закономерности, тенденции или аномалии проще, если воспользоваться системами прогнозирования и анализа данных на базе ИИ. Для анализа больших объемов информации (для прогнозирования параметров производства, выявления узких мест в бизнес-процессах) в них используются сложные алгоритмы машинного обучения. Цифровые двойники, или виртуальная копия объекта (системы) воспроизводят его поведение в реальном времени, помогают проверять гипотезы посредством такого метода анализа, как «что если».

Вопрос 13. Насколько полезными и корректными для вашего предприятия оказались отраслевые реестры типовых объектов КИИ?

Голосов – 186

Как и в прошлом году, самым популярным стал ответ «Не вполне корректные» (24%). Пока не вникали в эти реестры 21% ответивших. Пятая часть (20%) опрошенных назвали их очень полезными и вполне корректными. У 19% респондентов они не востребованы. 16% предпочли категорию «Другое».

В нашей стране составлены перечни типовых отраслевых объектов критической информационной инфраструктуры. При категорировании субъекты КИИ обязаны учитывать списки типовых объектов. С позапрошлого года отраслевые ведомства вправе формировать такие перечни. В большей части сегментов, указанных в Законе № 187-ФЗ, определены списки информационных систем, автоматических систем управления, информационно-телекоммуникационных систем. Как показывает опыт, одним из рисков для субъекта КИИ может стать существенное расширение перечня объектов критической информационной инфраструктуры. В результате будет труднее в них ориентироваться, что не исключает неточностей при составлении или пересмотре списков, отнесении новых объектов к категории КИИ.

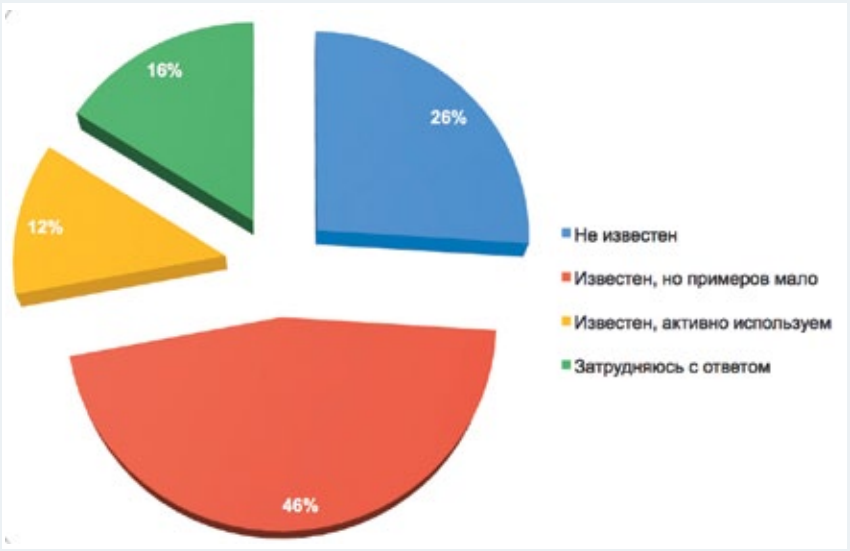


Вопрос 14. Насколько хорошо вам знаком опыт предприятий, подобных вашему, в области защиты АСУ ТП?

Голосов – 192

По традиции этот вопрос представлен в анкете, поскольку обмен опытом, знаниями, точками зрения по актуальным проблемам помогает в поисках решений. Не обо всем ИБ-специалисты готовы рассказывать с трибуны конференции, однако преимущество подобных мероприятий в том, что есть возможность кулуарного общения, камерных форматов в виде семинаров, практикумов, обмена мнениями в выставочной зоне и т. п.

Наиболее распространенный вариант ответа «Известен, но примеров мало» (46%). Чуть более четверти респондентов (26%) признались, что такой опыт им не известен. Затруднились с ответом 16%. И только 12% такой опыт известен, и они его активно используют.



В прошлом году структура мнения была следующей. Самый популярный ответ «Известен, но примеров мало» (51%). На втором месте ответ «Не известен» (24%). Годом ранее данный показатель был выше на 2%. Затруднились с ответом 14% (в текущем году их количество увеличилось). Об активном использовании опыта заявили 12% опрошенных: столько же, сколько и сейчас. Напрашивается вывод о том, что поиск новых форматов для общения представителей профессионального сообщества в рамках мероприятия – задача, которая не утрачивает актуальности.

Вопрос 15. Были ли у вашего предприятия или холдинга в 2024 г. инциденты информационной безопасности в части АСУ ТП?

Голосов – 197

Обращаясь с этим вопросом к участникам конференции, мы указываем, что опрос – анонимный. Ремарка необходима, поскольку несколько лет подряд желающих отвечать (по сути, признаваться в инцидентах) было немного. В прошлом году количество респондентов увеличилось до 242 с 88 в анкете 2023 г. Однако в анкете 2025 г. это число уменьшилось до 197.

Пару лет самым распространенным был ответ «Инцидентов зафиксировано не было». Вначале он держался на отметке 70%, в позапрошлом году снизился до 65%, в прошлом – до 58%, а в текущем – до 56%. На втором месте вариант

«Другое» с 21%. В минувшем году такой же показатель продемонстрировал вариант «инциденты были, но обошлось без ущерба». В этом году признание в том, что инциденты были, но без ущерба – на третьей позиции (16%).

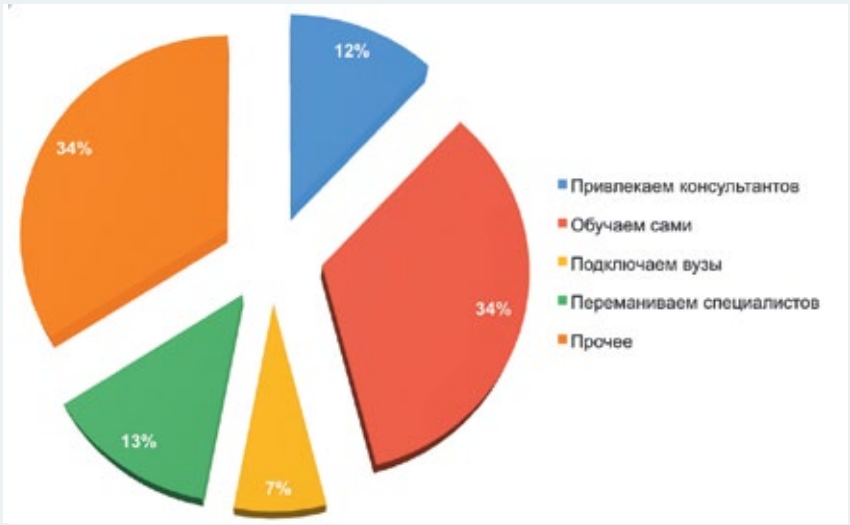
Незначительная доля тех сообщивших, что инциденты были с ущербом, но АСУ ТП не пострадала (4%). И всего 3% тех, что предпочел вариант ответа «Были инциденты с ущербом для АСУ ТП». Стоит заметить, что наличие ущерба может стать очевидным для предприятия только спустя время. Известна тактика киберпреступников находиться

в инфраструктуре долгое время, чтобы выбрать самые уязвимые точки для атаки.

Обращает на себя внимание и тот факт, что доля ответов «Другое», не превышавшая прежде 7–10%, продолжила увеличиваться: в прошлом году до 15%, в текущем – до 21%.

Вопрос 16. Как у вас решается кадровый вопрос в области ИБ АСУ ТП?

Голосов – 207



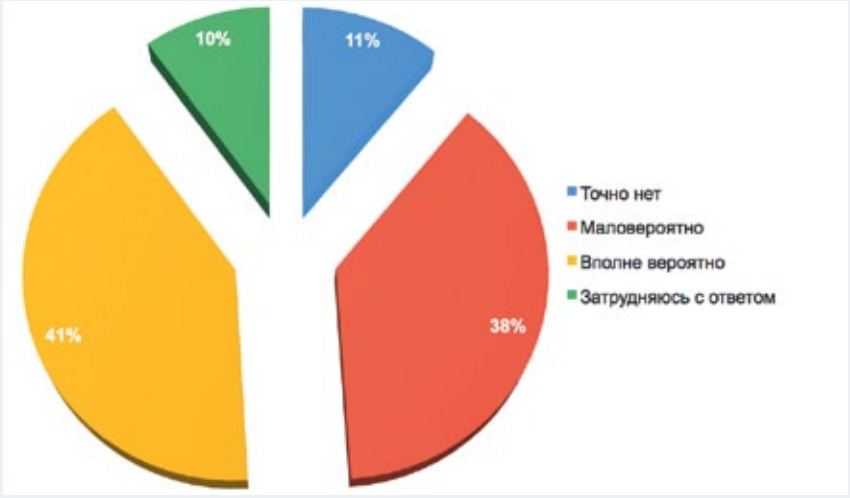
Когда год назад этот вопрос был включен в анкету, дефицит кадров в сфере ИБ, уровень их квалификации, объем работ в области автоматизации, цифровизации и т. п. входили в число наиболее обсуждаемых тем. Более трети респондентов в прошлом году выбрали вариант ответа «Обучаем сами» (36%). На втором месте был вариант «Прочее» (26%), на третьем – «Переманиваем специалистов» (16%). На услуги консультантов полагались 11% опрошенных. Почти столько же (10%) выбрали вариант «Подключаем вузы».

Сейчас структура ответов такова. Обучаем сами – 34% и столько же пришлось на вариант «Прочее». На второй позиции – «Переманиваем специалистов» (13%). На третьей с отставанием в 1% – «Привлекаем консультантов». На помощь вузов рассчитывают 7%. Таким образом немного (3%) уменьшилось число сторонников переманивать кадры и на 2% увеличилась аудитория, желающих обучать кадры самостоятельно.

Доступность технологий и средств защиты, выстраивание бизнес-процессов – значимые задачи, решение которых во многом зависит от наличия ИБ-специалистов с нужными компетенциями. Освоение практических навыков, закрепление их на киберполигонах, обмен опытом, удержание квалифицированных сотрудников, умение специалистов коммуницировать с персоналом других подразделений компании или предприятия – по-прежнему служат условиями, соблюдение которых обеспечит возможность проактивного реагирования, исключающего развитие ситуации в сфере ИБ по негативному сценарию.

Вопрос 17. Рассматриваете ли вы в обозримой перспективе вероятность возврата в Россию западных вендоров (АСУ ТП и ИБ)? Возможно ли возобновление сотрудничества при определенных условиях?

Голосов – 230



Рыночная ситуация меняется быстро под воздействием множества факторов, одним из которых являются геополитические тектонические сдвиги. Стоит напомнить, что год назад участники конференции отвечали на вопрос, как вы оцениваете вероятность дальнейшего роста риска безопасности КИИ со стороны иностранных государств.

На этот раз организаторы конференции сочли возможным поинтересоваться у аудитории о перспективах возвращения зарубежных вендоров, поскольку политическая риторика в глобальном масштабе приобретает новые краски.

Несмотря на то, что санкционные ограничения продолжают действовать, все чаще заходит речь о вероятности возвращения части западных компаний. Представители профессионального сообщества замечают, что, если окно возможностей сужается, надо ускоряться по многим направлениям, и автоматизация – не исключение.

Включенный в анкету-2025 вопрос стал одним из наиболее популярных по количеству желающих поделиться мнением. Любопытно распределились ответы. 41% респондентов не исключают возобновления сотрудничества («вполне вероятно»). Несколько меньше аудитория (38%) тех, кто настроен более пессимистично («маловероятно»). «Точно нет» – полагают 11% опрошенных, и почти столько же (10%) – затруднились с ответом.

Таким образом, точки зрения зафиксированы. В какой мере они отражают и текущую ситуацию, и настроения участников рынка, покажет время. Будем наблюдать.

Заключение

Неотложных задач в сфере безопасности технологических процессов великое множество. Сегмент инструментов защиты объектов КИИ быстро развивается, увеличивается количество российских производителей программно-аппаратных комплексов, инвесторы проявляют все большую активность. Как показал опрос, все это происходит на фоне ужесточения требований к информационной безопасности значимых объектов КИИ. Одним из препятствий на пути внедрения российских систем АСУ ТП эксперты называют дефицит кадров необходимого уровня квалификации.

Поскольку работоспособность существующих объектов по-прежнему на первом месте, а отказаться от импортного оборудования и ПО прямо сейчас невозможно, приходится обеспечивать безопасность в сложный переходный период, даже несмотря на то, что к проверенным решениям отношение теперь как к недоверенным.

Оптимизма придает тот факт, что все больше количество инженеров на производстве перестают воспринимать безопасность как дополнительную нагрузку к сложности, защита объектов КИИ не противопоставляется требованиям их цифровизации. Приходит понимание того, что буквальное следование мерам защиты приводит к усложнению рабочих процессов.

Различаются точки зрения делегатов относительно решения вопросов информационной безопасности в рамках проектов цифровизации производственных участков. Почти треть ответивших утверждают, что механизмы безопасности встраиваются после завершения основного внедрения, примерно столько же – что защита АСУ ТП предусматривается на уровне техзадания и разработки решения.

Комплексный подход, реализуемый специалистами в сфере информационных технологий, ИБ и эксплуатации в области защиты АСУ ТП, представляет собой единый процесс, требующий синхронизированных усилий для решения стоящих задач. Цифровизация выделенных сегментов приводит к эффекту «узкого горлышка» в масштабах предприятия.

Широкий разброс мнений и по поводу методики расчета показателя состояния защиты информации и обеспечения безопасности объектов КИИ. В Методике оценки от 02.05.2024 представлен алгоритм действий, которым можно руководствоваться при проведении самостоятельной проверки и подготовке к внешним контрольным мероприятиям. Методические материалы сгруппированы по четырем тематическим разделам: организация и управление, защита пользователей, защита информационных систем, мониторинг информационной безопасности. Данная методика применяется по нескольким направлениям: мониторинг организаций со стороны ФСТЭК, самооценка уровня защиты, оценка эффективности деятельности уполномоченного заместителя, ответственного за обеспечение ИБ, и подразделения ИБ.

Один из основных регуляторов в области КИИ – ФСТЭК обнаружил в прошлом году немало нарушений в сфере категорировании объектов критической информационной инфраструктуры. Как показал контроль субъектов КИИ, для 49% характерен низкий уровень защищенности, для 31% – средний, для 11% – базовый (соблюдение требуемых мер защиты). За последнее время зафиксирован рост количества атак на цепочки поставок – ИТ-компании, которые работают с субъектами КИИ. Стимулировать субъекты КИИ к повышению уровня безопасности призваны нормативно-правовые акты, регулирующие вопросы сертификации средств защиты, безопасной разработки, аттестации, моделирования угроз и т. п.

Остается немало вопросов относительно планов перехода на доверенные программно-аппаратные комплексы. С 1 сентября 2024 г. запрещено приобретать и эксплуатировать для значимых объектов КИИ недоверенные программно-аппаратные комплексы. Критерии доверенности ПАК: включен в реестр Минпромторга и реестр отечественного ПО, сертифицирован ФСТЭК (если выполняет функции защиты). Полный переход должен быть осуществлен в срок до 1 января 2030 г.

Дополнительные регуляторные требования, снижение зависимости от импортных продуктов открывают новые возможности для производителей и поставщиков решений в области кибербезопасности и промышленной автоматизации. Разработчики ИБ-продуктов стремятся занять значительную долю рынка, делая ставку на развитие решений, интегрированных в системы промышленной автоматизации. ■