ИТОГИ ОПРОСА

XII КОНФЕРЕНЦИИ

«Информационная безопасность АСУ ТП КВО»

2024 г.

Адаптация к турбулентной реальности в сегменте ИБ

Информационная безопасность – одна из немногих сфер, где строгое следование букве закона, указа, директивы, регламента или должностной инструкции не гарантирует исключения нештатных ситуаций. В сочетании с анализом специфики отрасли, опытом, должным уровнем культуры безопасности выше шансы обеспечить информационную защиту, своевременно принять меры профилактики и оптимизировать расходы на ИБ. Эксперты утверждают, что периоды освоения методик, насыщения сегмента АСУ ТП КВО технологиями, инструментами защиты, выстраивания процессов сменяются этапом наращивания компетенций, от которых в наибольшей мере зависит умение отражать атаки и сводить к минимуму их последствия. Не первый год Издательский дом «КОННЕКТ» на правах организатора конференции «Информационная безопасность АСУ ТП КВО» проводит опрос участников мероприятия, чтобы сформировать представление о тенденциях на рынке средств защиты для промышленных информационных систем и АСУ ТП. Не стала исключением и XII конференция.

Вопрос 1. Какую организацию вы представляете?
Голосов – 346

Наибольший интерес к тематике конференции проявили представители компаний – разработчиков/интеграторов (20%), на второй позиции – специалисты из нефтегазового комплекса (15%), на третьем – оборонной промышленности (12%). Четвертую позицию разделили металлурги и сотрудники прочих компаний, предприятий, организаций (по 10%), пятую – химики и электроэнергетики (по 9%). Вслед за ними – представители атомной промышленности (8%). С заметным отставанием по количеству ответивших – вузы и наука (4%), а также работники транспортной сферы (3%).

В прошлом году в лидерах были представители нефтегазового комплекса (17% ответов), электроэнергетики (16%), металлургии/химии (14%), предприятий ОПК (13%) и только на пятом месте – разработчики и интеграторы в сфере информационной безопасности. Популяризация решений отечественных ИБ-разработчиков дала результаты: как минимум пробудила интерес представителей различных отраслей к новинкам индустрии, а возможно, и к сегменту средств защиты КВО в целом.

Группа антирейтинга фактически не изменилась с прошлого года: транспортная отрасль, вузы/наука, атомная промышленность, которая, впрочем, удвоила свой предыдущий показатель (до 8%).

Вопрос 2. Какие системы на предприятии находятся в вашем подчинении?
Голосов – 296

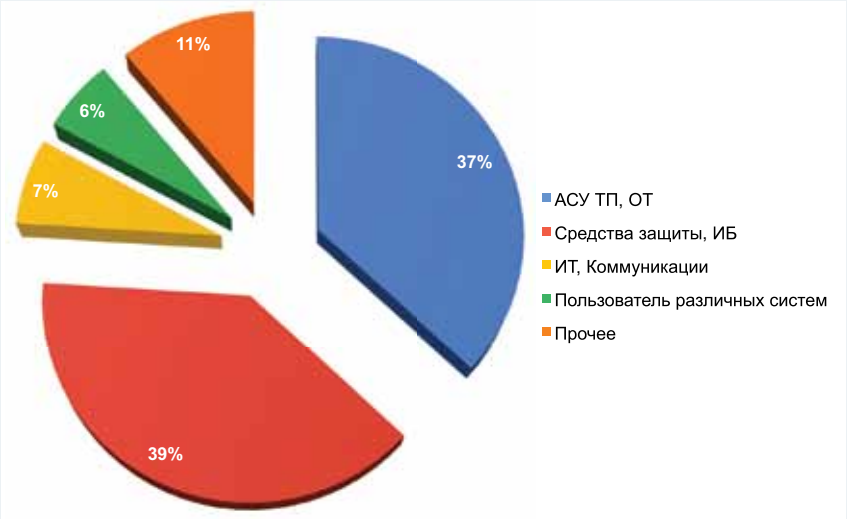
Относительно новый вопрос был включен в анкету на предыдущем мероприятии, чтобы понять, какие должности занимают или на чем именно специализируются делегаты, проявившие интерес к конференции.

Ответы распределились предсказуемо. На первом месте средства защиты, ИБ (39%), на втором – АСУ ТП, ОТ (37%), на третьем – категория «Прочее» (11%). С заметным отрывом идут ИТ, коммуникации (7%) и пользователи различных систем (6%).

Примерно такая же ситуация наблюдалась и год назад. Разве что количество ответов специалистов по информационной безопасности снизилось с 44 до 39%, АСУшников осталось неизменным, сотрудников, занятых ИТ и коммуникациями, немного подросло. Достаточно внушительной остается группа «прочее».

Вопрос 3. Требования каких нормативных актов сейчас наиболее актуальны для вашей организации?
Голосов – 284

В безусловных лидерах Федеральный закон № 187-ФЗ «О безопасности КИИ» (половина ответов). Второе место разделили постановление Правительства РФ № 1912 и Методические документы ФСТЭК России (по 11%), на третьем – Указ Президента РФ № 250 и документы категории «Другое» (по 8%). За ними с отставанием в один процент – Указ Президента РФ № 166. В группе аутсайдеров – требования отраслевых российских регуляторов (4%) и внутренних документов или контрагентов (2%).



Движущей силой развития сегмента информационной безопасности в нашей стране остаются требования законодательства. Большое стимулирующее значение имеют нормы и требования, вводимые отраслевыми регуляторами. Изменение макроэкономической ситуации, а вслед за этим курс на импортозамещение подстегнули формирование потребности в защите информационных систем и АСУ ТП. Все эти факторы в совокупности создают предпосылки к осознанию важности развития в организациях и на предприятиях культуры безопасности. Все чаще специалисты выражают надежду на то, что созданию систем информационной безопасности будет предшествовать анализ, а не аварийный опыт эксплуатации. Рациональность такого подхода заключается в том, что, насколько бы оптимальными ни были требования законодательства, отраслевых регуляторов, не всегда удается исключить случаи внедрения навязанных сверху механизмов и инструментов защиты. Анализ специфики отрасли, опыт, культура безопасности в большей мере содействуют обеспечению защиты, своевременной реализации профилактических мер и оптимизации расходов на ИБ.

Вопрос 4. Какие цифровые технологии, по вашему мнению, существенно увеличивают информационные риски для предприятий?
Голосов – 269

Наиболее настороженно ИБ-специалисты относятся к облачным технологиям (31%), промышленному Интернету вещей (21%) и искусственному интеллекту (19%). За год мнение участников конференции фактически не претерпело изменений. Тройка лидеров та же, только с несколько иными показателями. Облачные технологии откатились вниз (по количеству ответов) на 3%,

промышленный Интернет вещей – на 11%. А искусственный интеллект, напротив, взлетел на 8%, хотя и остался замыкающим в первой тройке.

Недоверие к облакам понятно, особенно на фоне случаев блокировки доступа к ним зарубежными провайдерами. Таких фактов за последнее время накопилось немало. Тем не менее, общее количество разочарованных технологией среди участников конференции уменьшилось. В еще большей мере тренд стал очевиден применительно к промышленному Интернету вещей.

Обратная тенденция характерна для искусственного интеллекта – именно с ним риски связывают дополнительные 8% ответивших. Настораживает, что происходит это на фоне все более широкого проникновения ИИ в различные сферы.

Следом за тройкой лидеров идут отечественная электроника (9%), категория «Другое» (8%). Курс на снижение тревожности респондентов по сравнению с прошлым годом продолжили роботы, ЧПУ-станки, 3D-принтеры (с 7 до 5%), цифровые двойники замерли на отметке 4%, технология мобильной связи (5G) с 5% переместились к 3%.

Вопрос 5. Насколько, по вашим оценкам, вопросы информационной безопасности учитываются в проектах цифровизации современных производств?
Голосов – 255

В прошлом году мы предположили, что практика цифровой трансформации в части кибербезопасности вернулась в норму. Примерно такой же вывод можно сделать по ответам участников XII конференции. Самый популярный ответ «Механизмы безопасности встраиваются после завершения основного внедрения» (35%). Немногим уступает ему ответ «Защита АСУ ТП предусматривается на уровне ТЗ и разработки решения» (32%). Без малого втрое меньше (11%) набрал ответ «Совсем не учитываются». Примерно столько же респондентов (10%) считают, что безопасность – базовое требование при разработке проекта. 9% ответивших полагают, что защита АСУ ТП выполняется на этапе передачи в эксплуатацию. 4% предпочли ответ категории «Другое». Стоит отметить, что при той же структуре распределения голосов общее число ответивших возросло со 197 до 255.

В выступлениях на конференции отмечалось, что защищать системы от уязвимостей следует уже на этапе проектирования, чтобы не пришлось исправлять проблемы позже. В частности, такой подход рассматривается в качестве приоритетного при построении безопасных продуктов на платформе «ГосТех». По мнению экспертов, в условиях импортозамещения наступило благоприятное время для оптимизации и бизнес-процессов, и технологических цепочек. Стоит приложить усилия к тому, чтобы предусмотреть потенциальные уязвимости и спланировать их устранение в начале проектирования. Однако недостаточно проработаны методики, которые помогают заложить основы такого «конвейера» безопасности.

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

Голосов – 252

Структура ответов на этот вопрос имеет мало общего с результатами прошлого года. 60% ответивших считают, что затраты достаточно высокие и растут (в 2023 г. 47%, в 2022-м – 23%, в 2021-м – 27%). «Приемлемые, но возрастают» – такой вариант выбрали 18%, затруднились с ответом 12%. Весьма небольшая доля выбравших ответ «Незначительные, на одном уровне» (4%). 3% полагают, что затраты приемлемые, примерно на одном уровне, столько же придерживаются мнения «Незначительные, но растут».

Едва ли можно было рассчитывать на иное распределение мнений, когда многим предприятиям приходится производить замену ранее освоенных технологий и установленных решений, средств защиты новыми. Финансовые вопросы не утрачивают своей актуальности. По мере ужесточения требований по защите АСУ ТП (объект КИИ должен запускаться в эксплуатацию совместно с системой защиты) эксперты рекомендуют, например, создавать системы на базе унифицированных решений. Система управления ИБ должна быть интегрирована в систему менеджмента качества. За безопасность надо платить, чтобы не пришлось расплачиваться за ее отсутствие.

Вопрос 7. Как вы оцениваете ассортимент представленных на рынке отечественных продуктов и услуг по информационной безопасности АСУ ТП?

Голосов – 248

Как и в прошлом году, самым популярный ответ «Продукты есть, не хватает опыта внедрения и эксплуатации» (36%). На нехватку отдельных классов продуктов посетовали 27% опрошенных. 21% предпочли вариант «Недостаточный, выбор невелик». Удовлетворены ассортиментом 10%.

Рост количества неудовлетворенных ассортиментом продуктов и услуг по информационной безопасности АСУ ТП сохраняется на протяжении последних четырех лет: в 2021 г. – 9%, в 2022-м – 19, 2023-м – 23%, 2024-м 27%.

На фоне ухода зарубежных поставщиков и спешной переориентации на продукцию отечественных производителей тенденция выглядит вполне закономерной. Переломить ситуацию пока не удается, несмотря на то, что российские разработчики горят желанием не упустить открывшиеся в новых условиях рыночные возможности. В то же время настораживают темпы, с какими создаются или дорабатываются российские решения в целях импортозамещения. Не всегда удается найти баланс, чтобы гарантировать необходимую функциональность и обеспечить соответствие требованиям безопасности.

Вопрос 8. Как вы оцениваете доступность и ассортимент отечественных продуктов для АСУ ТП в свете вступления требований по импортозамещению для ЗО КИИ?

Голосов – 234

Трудно найти отечественные аналоги основных программных

компонентов – такое мнение разделяют 43% респондентов. 24% утверждают, что программные компоненты есть, и находятся в ожидании доверенного ПАК. Пятая часть опрошенных (20%) сетуют на нехватку отдельных компонентов. Вариант ответа «Прочее» выбрали 10%. Незначительная доля (3%) тех, для кого ассортимента вполне достаточно, все компоненты доступны.

За последнее время несколько регуляторных событий оказали значительное влияние на участников рынка. В частности, стоит отметить изменение правил категорирования, запрет на использование импортных продуктов, требование сформировать службы ИБ, наделение руководства предприятия, организации ответственностью за обеспечение информационной безопасности.

Признание информационной системы значимым объектом КИИ

означает пересмотр процессов ИБ и строгое соблюдение требований регуляторов.

Задача импортозамещения становится базовой, для ее решения зачастую не хватает экспертизы. Приходится оценивать дополнительные риски информационных угроз, возникающие на фоне глобальных изменений.

Вопрос 9. Как вы оцениваете уровень осведомленности персонала вашего предприятия в области защиты АСУ ТП как части КИИ?
Голосов – 239

Более половины (54%) предпочли ответ «Недостаточно». В прошлом году таковых было 49%. Вполне достаточным назвали уровень осведомленности 21% (в 2023 г. – 23%). 15% (против 17% годом ранее) отдали предпочтение варианту ответа «Практически не осведомлен». Затруднились с ответом 10% опрошенных. Защита промышленных систем предусматривает участие в этом процессе всех сотрудников предприятия или организации.

Открытым остается вопрос, как измерить уровень осведомленности персонала, чтобы сделать выводы о его динамике. К критериям осведомленности эксперты относят, в частности,

понимание сотрудником своих ролей и должностных обязанностей, требований и процедур ИБ, принятых в организации, а также персональной ответственности за свои действия и бездействие по отношению к безопасности. Не менее важно выработать механизмы, стимулирующие сотрудников повышать уровень знаний в сфере ИБ и применять их на практике.

Вопрос 10. Насколько полезными и корректными для вашего предприятия оказались отраслевые реестры типовых объектов КИИ?
Голосов – 231

В России сформированы перечни типовых отраслевых объектов критической информационной инфраструктуры. С прошлого года отраслевые ведомства вправе формировать такие перечни. При категорировании субъекты КИИ обязаны учитывать списки типовых объектов. В 2024 г. такие перечни утверждены в оборонной промышленности, химической,

горнодобывающей сферах, металлургии.

Самым популярным стал ответ «Не вполне корректные» (27%). Почти четверть (24%) признались, что пока не вникали в эти реестры. Примерно столько же (23%) опрошенных назвали их очень полезными и вполне корректными. У 16% респондентов они не востребованы. 9% предпочли категорию «Другое».

Вопрос 11. Насколько востребованы, по вашему мнению, отраслевые центры ГосСОПКА?
Голосов – 232

Тема отраслевых центров ГосСОПКА стала одной из приоритетных в прошлом году. Инициатива развивается усилиями регулятора ФСТЭК, профильных министерств. Ее актуальность была определена постановлениями Правительства РФ, которыми предусматривается распределение ответственности ведомств в сфере обеспечения информационной безопасности объектов критических отраслей. По результатам предыдущего опроса 35% опрошенных специалистов отметили необходимость подобных центров. Без малого пятая часть опрошенных назвали их бесполезной структурой, примерно столько же затруднились с ответом. Доли сомневающихся и поддерживающих инициативу оказались примерно равными. 12% респондентов подтвердили актуальность центров только для руководителей.

В текущем году также наибольшая доля ответивших (29%) придерживается мнения «Очень нужны», но по сравнению с предыдущим опросом цифра уменьшилась на целых 6%. Необходимость структур для руководства подтвердили 16%, ровно столько же относятся к отраслевым центрам ГосСОПКА как к бесполезной структуре. Эти доли были равными и в прошлом году, только сейчас они уменьшились на 2%. Ответ «Другое» выбрали 18%. Позиция «мы и сами разберемся» близка 13% опрошенных. Коммерческим центрам отдают предпочтение 7% респондентов.

Если резюмировать сравнение, то уменьшились доли активно поддерживающих, признающих такие центры бесполезными и предпочитающих коммерческие образования. В то же время возросло количество уверенных в собственных силах и признавших актуальность центров для руководства. Общий вывод состоит в том, что любая относительно новая инициатива должна пройти проверку на практике.

Вопрос 12. Как у вашей компании организовано взаимодействие с ГосСОПКА?
Голосов – 225

Ответ на этот вопрос подтверждает, что процедура формирования отраслевой информационной безопасности продолжается. Чуть меньше трети (29%) респондентов сообщили, что есть человек, отвечающий за взаимодействие. Нет необходимости в таком взаимодействии для 19%. У 15% опрошенных взаимодействие организовано через ведомственный центр ГосСОПКА, 10% построили собственный корпоративный центр, 7% отдали предпочтение коммерческому. Пятая часть

респондентов (21%) затруднились с ответом.

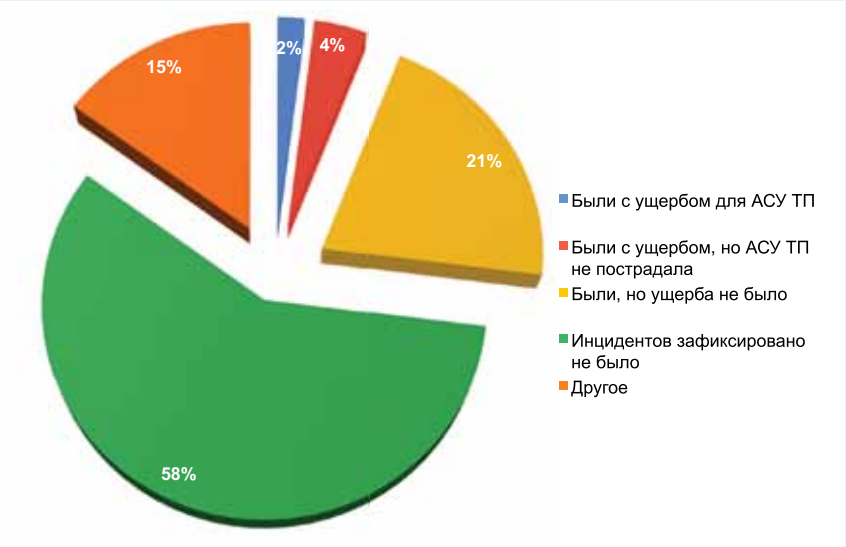
Поскольку этот вопрос включен в анкету впервые, то судить о динамике направления, а тем более о формирующихся тенденциях можно будет в следующем году. На конференции отмечалось, что центры ГосСОПКА должны соблюдать ряд обязательных требований, в частности, организовывать мероприятия по выявлению компьютерных атак и регистрации инцидентов, реагировать на инциденты и устранять их последствия, осуществлять оценку уровня защищенности информационных ресурсов от атак и т. д.

Вопрос 13. Были ли у вашего предприятия или холдинга в 2023 г. инциденты информационной безопасности в части АСУ ТП?

Голосов – 242

Обращаясь к аудитории конференции, мы подчеркивали, что опрос – анонимный. Однако несмотря на оговорку, данный вопрос оставался одним из самых непопулярных – с минимальным количеством желающих на него отвечать. В текущем году ситуация изменилась: 242 ответа против 88 годом ранее.

Несколько лет самым распространенным был ответ «Инцидентов зафиксировано не было». Первоначально он держался на уровне 70%, в прошлом году снизился до 65%, а в текущем до 58%. На второй позиции признание, что инциденты были, но обошлось без ущерба (21%). Примерно столько же показал прошлогодний опрос (20%). Доля ответов «Другое», обычно державшаяся на уровне 7 –10%, сейчас увеличилась до 15%.



4% респондентов признали, что инциденты были, но АСУ ТП не пострадала, и лишь 2% отметили наличие происшествий с ущербом для АСУ ТП. В сумме эти два ответа дали больше, чем годом ранее, когда было зафиксировано 4%. Стоит отметить, что объективная картина ущерба может стать очевидной для предприятия только по прошествии некоторого времени. Неслучайно эксперты бьют тревогу по поводу новой тактики киберпреступников. Злоумышленник может находиться в инфраструктуре продолжительное время, изучая уязвимые точки для атаки с наибольшим ущербом. На этом фоне особенно важно наладить взаимодействие специалистов, отвечающих за ИБ и за функционирование АСУ ТП.

Вопрос 14. Как вы оцениваете концепцию кибериммунности промышленных систем и использование встроенных средств безопасности АСУ ТП в целом?

Голосов – 222

С таким вопросом мы обратились к участникам конференции во второй раз. Напомним, что суть кибериммунных систем – в технологии встраивания эффективных механизмов информационной безопасности непосредственно в АСУ ТП. Такие системы могут самостоятельно, без использования наложенных средств защиты, обеспечить непрерывность и устойчивость технологического процесса.

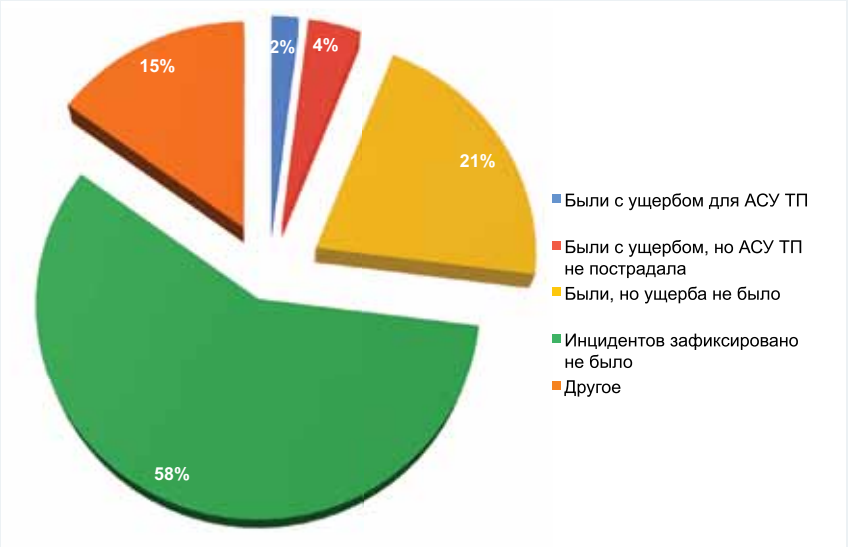
Концепцию можно использовать вместе с СЗИ – полагает половина опрошенных. В прошлом году этой точки зрения придерживались 54% респондентов. Несмотря на некоторое понижение данного показателя, значительная часть специалистов ратуют за комплексные решения по безопасности, сочетающие киберимунные АСУ ТП с наложенными средствами защиты.

22% участников опроса (год назад 23%) затруднились с ответом. Только так и надо защищаться – считают 14% респондентов. Почти столько же (13%) полагают, что наложенная защита надежнее. Как и в прошлом году, эти группы оказались примерно равны.

Вопрос 15. Насколько хорошо вам знаком опыт предприятий, подобных вашему, в области защиты АСУ ТП?

Голосов – 234

Это традиционный вопрос, на который мы просим ответить участников конференции. В новых условиях ценность обмена опытом повышается, хотя и не обо всем специалисты готовы рассказывать в публичном пространстве. Самый популярный ответ «Известен, но примеров мало» (51%). На втором месте ответ «Не известен» (24%). В этом году данный показатель снизился на 2%. Затруднились с ответом 14%. Об активном использовании опыта заявили 12% опрошенных, что также на 2% меньше, чем в прошлом году.

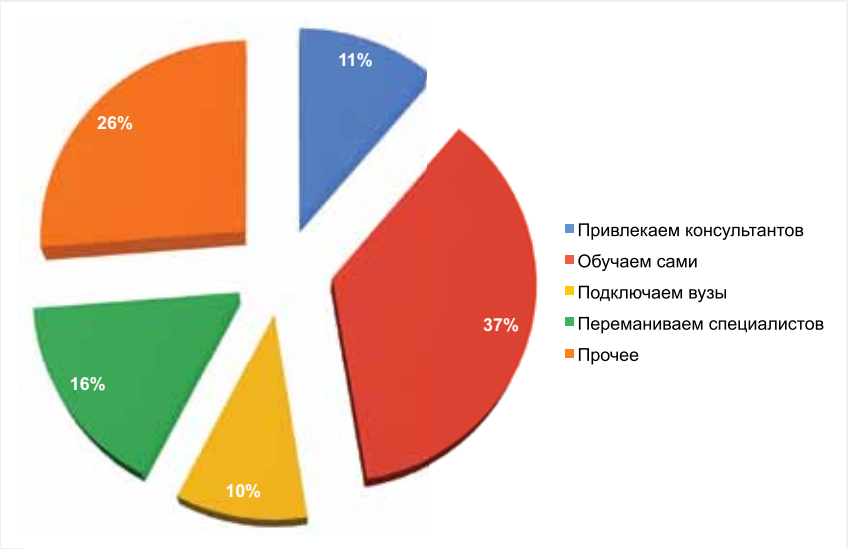


Предстоит находить новые форматы обмена опытом, чтобы не нарушать строгие требования законодательства и при этом в партнерстве с коллегами обсуждать практику защиты АСУ ТП, сообща анализировать результативность использования предлагаемых решений на конкретных примерах. В противном случае останется и так всегда доступная но малопродуктивная возможность учиться на своих ошибках.

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

Голосов – 241

В этом году мы предложили участникам конференции ответить на вопрос о кадрах в области информационной безопасности АСУ ТП. Ограничения по количеству персонала на предприятиях и нехватка на рынке специалистов в сфере ИБ, большой объем работ с комплексом сложных систем по безопасности, не подразумевающих ручного управления, – лишь некоторые проблемы, требующие решения. Более трети респондентов следуют правилу «постарайся помочь себе сам», поэтому выбрали вариант ответа «Обучаем сами» (36%). На втором месте вариант «Прочее» (26%), на третьем – «Переманиваем специалистов» (16%). На услуги консультантов полагаются 11% опрошенных. Почти столько же (10%) выбрали вариант «Подключаем вузы».

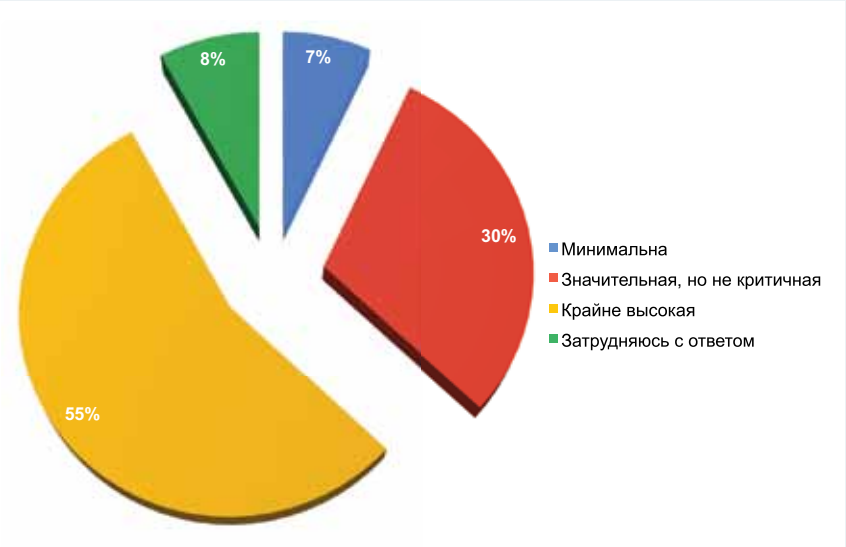


Комплексный подход к обеспечению безопасности АСУ ТП предусматривает не только подготовку, но и повышение

квалификации кадров. Фокус на расширение компетенций специалистов становится одним из ключевых трендов в области информационной безопасности. Позади этапы насыщения сегмента технологиями и средствами защиты, а также выстраивания процессов. Предстоящее десятилетие эксперты называют эпохой практических компетенций – специалистам необходимо уметь противостоять атакам и минимизировать их последствия. Дефицит ИБ-специалистов подталкивает к тому, что предприятия задумываются о формировании кадрового резерва службы ИБ на предприятии за счет непрерывного обучения практическим навыкам, отработке их на киберполигонах и т. д. Такой подход способствует повышению слаженности команд различных подразделений, что имеет решающее значение для оперативного реагирования и принятия грамотных решений.

Вопрос 17. Как вы оцениваете вероятность дальнейшего роста риска безопасности КИИ со стороны иностранных государств в 2024 г.?

Голосов – 271



В четвертый раз участники конференции отвечают на этот вопрос, и количество респондентов постоянно увеличивается. Анализ ответов в динамике позволяет проследить накал страстей и колебания настроений. Первоначально самый популярный ответ «Значительная, но не критичная» еще в позапрошлом году уступил пальму первенства варианту «Крайне высокая» с долей в 61%. В прошлом году эта доля сократилась до 52%, а в текущем возросла до 55%. Об опасности киберподразделений иностранных государств для промышленных предприятий не говорит только ленивый. Но в последнее время промышленности приходится адаптироваться к постоянно агрессивной среде. На этом фоне активность международных хакерских группировок воспринимается менее критично. Однако настроения в профессиональной среде колеблются в унисон общей нестабильной ситуации, ее градус определяется сведениями об инцидентах, которые попадают в публичное пространство. Стабилизации настроений посодействовало создание системы ГосСОПКА, отношение к которой варьируется (об этом речь шла в ответах на вопросы 11 и 12).

Значительной, но не критичной сочли вероятность дальнейшего роста риска безопасности КИИ 30% опрошенных. В прошлом году таковых было 39%. «Затрудняюсь с ответом» – 8%, минимальной вероятность назвали почти столько же (7%). Последние два варианта ответов указывают на то, что основная масса специалистов предпочитают быть начеку. Как показывает практика, лучше переоценить угрозу, чем недооценить – выше шансы оказаться во всеоружии к любым возможным рискам.

Заключение

Конференция, задуманная в свое время для обмена опытом среди специалистов в сфере ИБ АСУ ТП, показала, что профессиональное сообщество нуждается в такой площадке для делового общения. Тем более что развернутая в фойе выставка с тестовыми зонами предоставляет возможность обменяться мнениями не только за трибуной, но и в кулуарах мероприятия. Неизменно широким остается отраслевой состав участников, корректируется он только в количественном отношении.

Опрос показал, что ключевым драйвером развития сегмента информационной безопасности в≈нашей стране остаются требования законодательства. Изменение макроэкономической ситуации, а вслед за этим курс на импортозамещение повысили уровень внимания к защите информационных систем и АСУ ТП. В сочетании с рядом иных обстоятельств формируются предпосылки к осознанию важности развития в организациях и на предприятиях культуры безопасности. Все чаще специалисты выражают надежду на то, что созданию систем информационной безопасности будет предшествовать анализ, а не аварийный опыт эксплуатации. Рациональность подхода заключается в том, что, насколько бы оптимальными ни были нормы законодательства,

отраслевых регуляторов, не всегда удается исключить требования о внедрении навязанных сверху механизмов и инструментов защиты.

Разделились мнения делегатов относительно проработки вопросов ИБ в рамках проектов цифровизации современных производств. Большая часть ответивших утверждают, что механизмы безопасности встраиваются после завершения основного внедрения, примерно столько же, что защита АСУ ТП предусматривается на уровне техзадания и разработки решения. В выступлениях на конференции отмечалось, что защищать системы от уязвимостей следует на этапе проектирования, чтобы не пришлось исправлять проблемы позже. В частности, такой подход реализуется в качестве приоритетного при создании безопасных инструментов на платформе «ГосТех».

Политику импортозамещения следует рассматривать как дополнительный шанс оптимизации и бизнес-процессов, и технологических цепочек. Специалисты прилагают усилия к тому, чтобы предусмотреть потенциальные уязвимости и спланировать их устранение на начальной стадии проектирования. Однако недостаточно проработаны методики, помогающие заложить основы такого «конвейера» безопасности.

По результатам анкетирования выяснилось, что увеличилось количество неудовлетворенных ассортиментом продуктов и услуг по информационной безопасности АСУ ТП. Переломить тенденцию не удается на протяжении нескольких лет, несмотря на то, что российские разработчики стремятся не упустить открывшиеся в новых условиях рыночные возможности. В то же время настораживают темпы, с какими создаются или дорабатываются российские решения, предлагаемые в качестве замены импортным. Не всегда удается найти баланс, чтобы гарантировать необходимую функциональность и обеспечить соответствие требованиям безопасности.

Другой стороной медали защищенности критически важных объектов является уровень осведомленности персонала предприятия в области безопасности АСУ ТП как части КИИ. Более половины опрошенных назвали его недостаточным, что превысило показатель прошлого года. Сохраняется потребность в выработке механизмов, стимулирующих сотрудников повышать уровень знаний в сфере ИБ и применять их на практике.

В этом году участники конференции были более активными в ходе анкетирования, общее количество респондентов значительно увеличилось. Более того, они не стали игнорировать традиционно непопулярные вопросы, например, связанные с ущербом от действий злоумышленников. Мы отдаем себе отчет в том, что на объективную картину потерь трудно рассчитывать, в частности, потому, что она может стать очевидной для самого предприятия только по истечении времени. Неслучайно эксперты бьют тревогу по поводу новой тактики киберпреступников. Злоумышленник может находиться в инфраструктуре продолжительное время, изучая уязвимые точки для атаки с наибольшим ущербом. На этом фоне особенно важно наладить взаимодействие специалистов, отвечающих за ИБ и за функционирование АСУ ТП.

Судя по всему, число атак на АСУ ТП увеличивается, и для все большего количества предприятий обеспечение защиты своих объектов и систем становится насущной необходимостью. ■