РЕЗОЛЮЦИЯ

Седьмой конференции «Информационная безопасность АСУ ТП КВО – 2019»

27–28 февраля 2019 г. в городе Москве состоялась VII конференция «Информационная безопасность АСУ ТП КВО». В ее работе приняли участие 396 человек. В течение двух дней было заслушано 28 докладов, проведен круглый стол по актуальным вопросам ИБ АСУ ТП. Ключевой темой обсуждения стала практическая реализация Федерального закона № 187-ФЗ, приказов ФСТЭК России № 235, 239, Постановления Правительства РФ № 127 и иных регулирующих документов.

По итогам работы конференции сформулированы следующие предложения и рекомендации.

- Признать, что риски целенаправленных атак на АСУ ТП продолжают возрастать в России и за рубежом.
- Отметить высокую оперативность ФСТЭК России в дальнейшем развитии нормативных документов, необходимых для реализации положений Федерального закона № 187-ФЗ.
- Отметить крайнюю необходимость принятия актуальной методологии определения актуальных угроз безопасности информации объектов КИИ. Рекомендовать до публикации методических рекомендаций по определению актуальных угроз безопасности информации использовать методики оценки угроз безопасности информации в КСИИ.
- Субъектам КИИ учитывать, что информационные системы, автоматизированные системы управления и информационно-телекоммуникационные сети могут принадлежать им не только на правах собственности, но и на любом ином законном основании, в том числе на основании договора аренды или аутсорсинга.
- Признать возможность подготовки материалов для категорирования объектов КИИ сторонними организациями при условии, что окончательные документы, содержащие результаты категорирования, утверждаются субъектом КИИ.
- Рекомендовать отраслевым регуляторам пересмотреть свои отраслевые нормативные акты и стандарты в целях приведения их в соответствие с требованиями Федерального закона № 187-ФЗ «О безопасности КИИ».
- Отметить, что при обеспечении защиты ИТКС нужно учитывать не только требования приказов ФСТЭК России, но и требования Минкомсвязи России.
- Разработчикам АСУ ТП рекомендовать использовать при проектировании своих решений российские стандарты безопасной разработки программного обеспечения, подготовленные ФСТЭК России.
- Признать необходимость разработки нормативного документа, определяющего классы и порядок использования средств криптографической защиты информации в составе системы защиты значимых объектов КИИ различных категорий.
- Участники конференции просят ФСТЭК России разъяснить порядок организации удаленной технической поддержки производителем импортного производственного оборудования в составе значимых объектов КИИ в гарантийный и постгарантийный период с учетом требований руководящих документов.
- Признать преимущества специализированных средств защиты для АСУ ТП над универсальными и встроенных в АСУ ТП над наложенными.
- Признать полезность средств автоматизации процесса категорирования и разработки моделей угроз на основе БДУ для ускорения категорирования в сложных холдинговых структурах.
- Рекомендовать субъектам КИИ обратить особое внимание на защиту не только систем управления технологическими процессами, но и вспомогательных и обеспечивающих процессов. Особое внимание рекомендуется обратить на защиту систем РЗА.
- Рекомендовать субъектам КИИ создавать собственные центры ГосСОПКА, для чего необходимо обеспечить выполнение Требований к подразделениям и должностным лицам субъектов ГосСОПКА и заключить соглашение о взаимодействии с НКЦКИ.
- Рекомендовать субъектам КИИ направлять в НКЦКИ инвентаризационную информацию о своих информационных ресурсах в целях получения обратной связи в части обеспечения процессов обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.
- Признать необходимость разработки с участием отраслевых регуляторов и крупных субъектов КИИ квалификационных требований по подготовке кадров для защиты критической информационной инфраструктуры. ■

Оргкомитет конференции