В июне Ассоциация «Цифровая энергетика» (АЦЭ) провела вторую в 2023 году встречу экспертной группы по кибербезопасности с участием профильных органов исполнительной власти – Минэнерго, ФСТЭК, Минцифры, Минпромторга, ФСБ России.

В мероприятии приняли участие эксперты от компаний Ассоциация крупнейших потребителей ПО и оборудования, Центр компетенций «Кибербезопасность» Национальной технологической инициативы «Энерджинет», РТСофт, Русгидро и крупнейшие электроэнергетические предприятия – участники АЦЭ: Госкорпорация «Росатом», ПАО «Россети», ПАО «Интер РАО», АО «СО ЕЭС» и АО «Интертехэлектро» и др.

«*Приветствуем участников нашего уже традиционного регулярного мероприятия. Тенденции ежегодного увеличения компьютерных угроз, в том числе на объекты ТЭК, требуют постоянного обмена опытом и выработки актуальных и специфических мер противодействия. Для обеспечения их эффективности необходимо поддерживать консолидацию усилий экспертного сообщества и органов власти и совместно прорабатывать пути решения актуальных задач, внедрять лучшие практики*», – выступил с приветственным словом исполнительный директор АЦЭ – Антон Зубков.

На повестке дня стояли вопросы контроля со стороны регуляторов и совместная выработка рекомендаций по развитию процессов ИБ для компаний электроэнергетики.

В ходе дискуссии центральными темами диалога стали вопросы импортозамещения, подготовки и реализации планов перехода на доверенные ПАК.

Участники встречи отметили:

1) Атаки, реализуемые нарушителями на сегодняшний день, требуют обладания низким и средним потенциалом. В связи с участившимися атаками на объекты ТЭК необходимо поддерживать высокий уровень оперативного реагирования служб информационной безопасности обеспечивая мероприятия по обучению сотрудников ИБ и анализу новых приемов нарушителей, т. к. возможно повышение эффективности реализации данных противоправных действий.

2) В силу вступления с 1 января 2023 г. отложенных норм требований по обеспечению безопасности значимых объектов КИИ (приказ ФСТЭК России от 25 декабря 2017 г. № 239) ФСТЭК России рассматривается возможность разработки рекомендации по реализации данных требований.

3) ФСТЭК России подготовлены изменения в требования к созданию систем безопасности значимых объектов КИИ (приказ ФСТЭК России от 21 декабря 2017 г. № 235) в части уточнения норм по наличию обязательной

технической поддержки ПО, целеполаганием которых является устранение имеющихся уязвимостей в данном ПО, а также нейтрализация угроз, связанных с данными уязвимостями (на момент проведения совещания указанные изменения находятся на государственной регистрации в Минюсте России).

4) Представители Минцифры России сообщили о проработке вопросов, связанных с организацией процесса по получению, предоставлению отчетности по реализации мер Указа Президента Российской Федерации от 01.05.2022 г. № 250 в электронной форме.

5) Представители Минэнерго России напомнили о наличии полномочий по мониторингу представления субъектами КИИ актуальных и достоверных сведений по результатам категорирования со стороны отраслевого регулятора. Разрабатывается порядок проведения мониторинга актуальности и достоверности сведений, представленных в ходе категорирования, куда будет включен раздел по выездным проверкам.

По итогам встречи сформированы предложения по развитию процессов ИБ компаний электроэнергетики с привлечением экспертизы Ассоциации, в том числе:

- необходимости усиления контроля сопряжение технологических сегментов с корпоративным сегментом сетей;
- необходимости решения проблем по импортозамещению на рынке средств защиты информации – класса решений NGFW;
- необходимости однозначного нормативного определения терминов ПАК; отечественный ПАК; доверенный ПАК. Также отмечена сложность определения критериев доверенности ПАК.

Это уже седьмая встреча экспертной группы АЦЭ по кибербезопасности, которая прошла с участием большого числа заинтересованных сторон. Как отмечает руководство Ассоциации, высокая вовлеченность в деятельности ЭГ свидетельствует об актуальности обсуждаемых вопросов и способствует эффективному взаимодействию участников в противодействии киберугрозам в электроэнергетике.