Ассоциация «Цифровая энергетика» создает Центр экспертизы по вопросам информационной безопасности в электроэнергетике – Энерго ЦИБ

В мировой и российской практике нашли широкое применение всем известные CSIRT (Computer Security Incident Response Team – группа реагирования на инциденты компьютерной безопасности), CERT (Computer Emergency Response Team – группа экстренного реагирования на инциденты компьютерной безопасности) или SOC (Security Operations Center – центр обеспечения безопасности). В России созданы и действуют корпоративные и ведомственные центры. В чем же причина и необходимость создания очередного центра безопасности?

КЛЮЧЕВЫЕ СЛОВА: Ассоциация «Цифровая энергетика», информационная безопасность, Энерго ЦИБ

Авторы:
Лев Палей,
Алексей Чугунов,
Александр Капустин

Необходимость создания Центра экспертизы (обмена и анализа информации) по вопросам информационной безопасности в электроэнергетике Энерго ЦИБ (ENERGY ISAC) и ее ценность для отрасли и ТЭК в целом обсуждалась на площадке Ассоциации «Цифровая энергетика» ведущими отраслевыми экспертами и членами Экспертной группы по кибербезопасности при правлении Ассоциации «Цифровая энергетика» более года. Концепция Центра создавалась с учетом предложений Минэнерго России, ФСТЭК, Минцифры России, НКЦКИ, а также была утверждена правлением и наблюдательным советом Ассоциации в сентябре 2021 года и поддержана Минэнерго России. Создание Центра позволит сформировать отраслевую площадку для взаимодействия компаний по информационной безопасности. Проект предлагается реализовать на базе Ассоциации «Цифровая энергетика».

Если смотреть мировую практику, Центры обмена информацией и ее анализа (Information Sharing and Analysis Centres, ISAC) создаются владельцами и операторами энергетической инфраструктуры, в некоторых случаях при содействии и поддержке правительства. Цель – содействие обмену информацией о передовой практике в отношении физических угроз и угроз в киберпространстве, а также для устранения последствий этих угроз. Как правило, это некоммерческие организации, которые охватывают определенный сектор экономики (отрасли), обеспечивают быструю передачу информации в широких масштабах и поддерживают осведомленность о ситуации (например, Национальный совет ISAC). Они помогают собирать, анализировать и распространять среди своих партнеров информацию, которая может быть использована для принятия упреждающих мер, а также предоставляют своим партнерам инструменты для уменьшения рисков и повышения общей защищенности. При создании Энерго ЦИБ Ассоциация подробно изучила мировой и российский опыты создания как CERT, так и ISAC (https://www.digital-energy.ru/activity/almanac/).

В России создание именно ISAC обусловлено следующим:

- компьютерные атаки на инфраструктуру ТЭК имеют свою специфику в векторах и инструментарии, используемых злоумышленниками, поэтому требуют соответствующих мер противодействия;
- особенность информационного обмена между объектами ТЭК, тесные взаимосвязи различных организаций, формирующих Единую энергосистему РФ, требуют учета угроз воздействия одних объектов отрасли на другие;
- наличие множества специфических протоколов обмена данными и технических решений, требующих нетипичных подходов в реализации мер защиты и мониторинга угроз;

■ отсутствие централизованного пункта агрегации и анализа статистических данных, связанных с распространением вредоносных программ и сетевых атак, позволяющего экономить кадровые ресурсы объектов отрасли, а также обеспечивать оценку применимости угроз для всей отрасли в целом.

Дополнительными факторами создания стали:

■ запрос Минэнерго России по обеспечению отраслевой экспертизы в области ИБ;

■ потребность энергетических компаний в организации совместного реагирования на актуальные угрозы информационной безопасности;

■ необходимость повышения эффективности процессов обеспечения информационной безопасности, направленных на повышение устойчивости энергетической системы от компьютерных атак.

За счет формирования единой отраслевой площадки Энерго ЦИБ позволит существенным образом сэкономить ресурсы компаний (организационные, финансовые, управленческие и административные), в части накопления практического опыта, распределения сервисов и информационных потоков, а также проведения совместных мероприятий в области информационной безопасности.

Основные задачи Энерго ЦИБ:

■ участие в консолидированной разработке (с привлечением компаний электроэнергетики и экспертов ИБ) и формировании единой отраслевой методологии и стандартов по обеспечению информационной безопасности;

■ создание площадки для обмена опытом, результатами реализации проектов в области ИБ, инцидентов, реагирования на актуальные угрозы и атаки;

■ создание партнерства на добровольной основе для формирования и анализа информации для корпоративных центров обеспечения ИБ компаний электроэнергетики о новых уязвимостях в ПО/оборудовании, векторах атак и событиях ИБ, могущих оказать влияние на деятельность энергокомпаний. Обеспечение информационного взаимодействия Центра с другими профильными и специализированными организациями;

■ проведение мероприятий по повышению грамотности и популяризации знаний для специалистов ИБ с учетом отраслевой специфики;

■ получение оперативного доступа к консолидированной и проверенной информации, экспертизе по актуальным угрозам и рискам с учетом отраслевой специфики;

■ формирование базы знаний в области ИБ;

■ оказание услуг при построении и планировании систем защиты в компаниях (в рамках указанных выше задач);

■ экспертное сопровождение при организации процессов обеспечения ИБ;

■ предоставление информации и доступа к сервисам, находящимся в собственности или на правах аренды в Ассоциации;

■ участие в разработке локально-нормативной и проектной документации в части систем ИБ.

Среди функций Центра на первом этапе – информационно-аналитическая, а именно:

■ сбор и агрегация информации о новых угрозах и атаках, информирование компаний, заключивших соглашение с Центром;

■ сбор информации о фактическом состоянии внешней инфраструктуры компаний, заключивших соглашение с Центром;

■ оценка актуальности и рисков, связанных с новыми угрозами (вектора атаки, уязвимости) для отрасли в целом;

■ оперативное оповещение объектов отрасли о новых развивающихся атаках с конкретными техническими рекомендациями;

■ мониторинг ресурсов сети интернет на предмет чувствительной информации для компаний;

■ предоставление по запросу аналитических и статистических материалов по количеству обнаруженных уязвимостей, заблокированных атак, обработанных инцидентах информационной безопасности.

Уже на первом этапе Центр планирует заниматься популяризацией и распространением знаний, осуществлять сотрудничество, накопление и обмен знаниями.

На втором этапе к функциям первого добавляются экспертная аналитика и методологическая поддержка при развитии инцидента.

Участниками Центра могут быть:

■ компании ТЭК;

■ специализированные компании (поставщики оборудования и услуг в области информационной безопасности);

■ компании, оказывающие аналогичные услуги в области информационной безопасности;

■ компании, формирующие государственную политику в области информационной безопасности;

■ разработчики решений и ПО;

■ специализированные учебные заведения в области информационной безопасности.

На текущий момент сформирован состав Комитета по кибербезопасности при Наблюдательном совете Ассоциации «Цифровая энергетика» для контроля деятельности Энерго ЦИБ, а также подготовлен план работ Энерго ЦИБ на 2021–2022 гг.

Таким образом, Центр экспертизы (обмена и анализа информации) по вопросам информационной безопасности в электроэнергетике Энерго ЦИБ (ENERGY ISAC), создаваемый на базе Ассоциации «Цифровая энергетика», станет уникальным отраслевым центром в данной сфере. Необходимость его создания в данный момент критически важна для обеспечения защищенности объектов электроэнергетики от киберугроз, надежности, безопасности и дальнейшего развития отрасли и российской экономики в целом.

Association “Digital Energy” creates a Center of Expertise on Information Security in the Electricity Industry – Energo CIB

Lev Paley, Alexey Chugunov, Alexander Kapustin

The well-known CSIRT (Computer Security Incident Response Team), CERT (Computer Emergency Response Team) or SOC (Security Operations Center) are widely used in world and Russian practice. security). Corporate and departmental centers have been established and are operating in Russia. What is the reason and the need to create another security center?

KEYWORDS: Association «Digital Energy», information security, Energo CIB

Лев Палей, Алексей Чугунов, Александр Капустин, Экспертная группа по кибербезопасности при правлении Ассоциации «Цифровая энергетика»