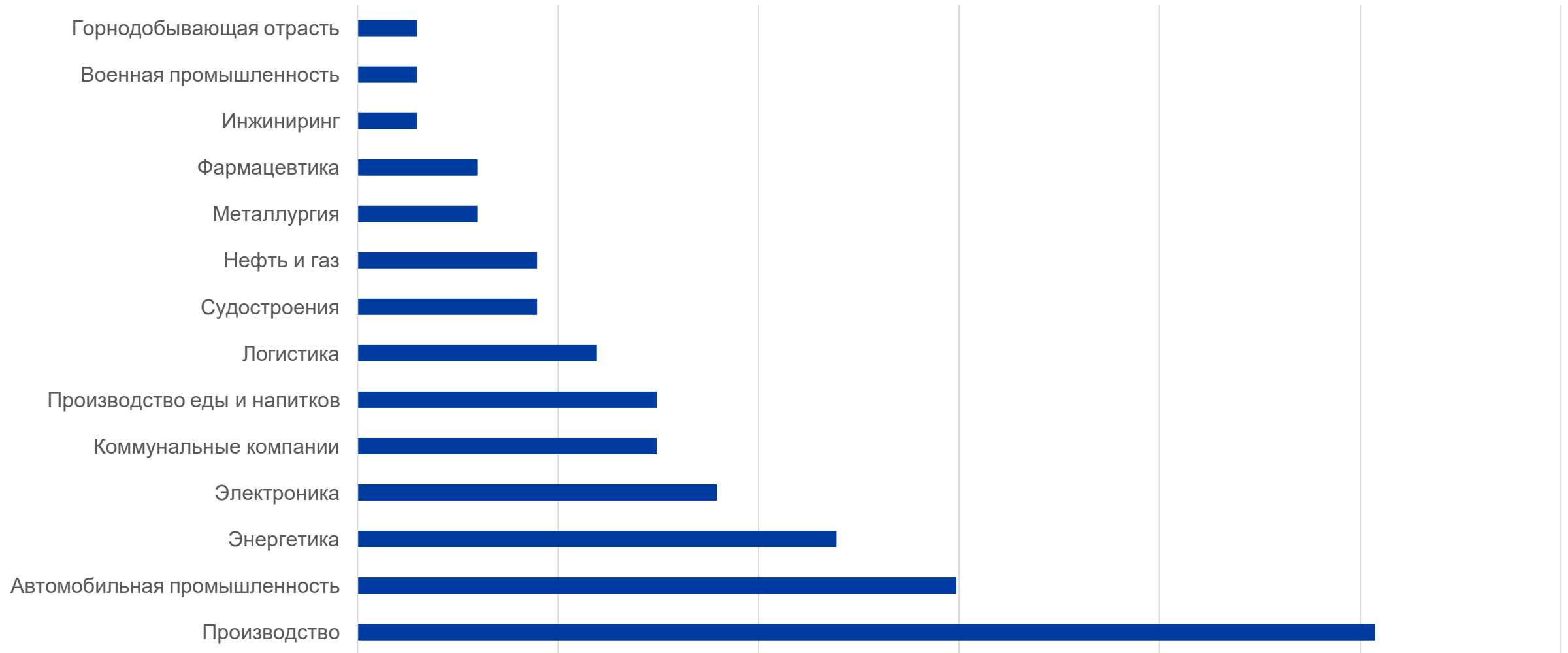




Консолидация усилий компаний электроэнергетики для совместного противодействия компьютерным атакам. Развитие центра компетенций на площадке Ассоциации «Цифровая энергетика»

Докладчики: Капустин А.В., Правиков Д.И.







Специфика отраслевых центров кибербезопасности базируется на следующих принципах:

01

Информационная безопасность в настоящее время имеет ярко выраженную отраслевую специфику (что подтверждается выводами по итогам Инфофорума 2024).

02

Экспертиза по отраслевой специфике обеспечения информационной безопасности сосредотачивается в отраслевых центрах (мнение НКЦКИ по итогам «Магнитки» 2024).

03

АЦЭ вырабатывает экспертизу отраслевой специфики совместно с Минэнерго России.

04

Требует проработки нормативная процедура формирования отраслевых центров (протокол рабочей группы по вопросам кибербезопасности Комитета РСПП по цифровой экономике от 20.12.2023)



Минэнерго России

- Координация деятельности в области информационной безопасности в электроэнергетике
- Взаимодействие с регуляторами по вопросам ИБ электроэнергетики
- Координация реагирования на компьютерные инциденты в электроэнергетике
- Оценка защищенности объектов электроэнергетики и системы в целом
- Мониторинг представления субъектами КИИ актуальных и достоверных сведений о категорировании
- Развитие взаимодействия и заключений соглашений с организациями ТЭК, а также другими отраслями

Ведомственный центр ГосСОПКА

- Организации ИБ для Министерства и подведомственных организаций
- Проведение мероприятий по ИБ на подведомственных организациях и объектах электроэнергетики
- Мониторинг состояния ИБ и реагирование на инциденты ИБ
- Круглосуточный мониторинг информационной безопасности центрального аппарата Минэнерго и подведомственных организаций

Отраслевой центр кибербезопасности Минэнерго России (в перспективе)

- Круглосуточное информирование об атаках и угрозах и оперативное оповещение Минэнерго, ведомственного центра и предприятий отрасли о новых уязвимостях, угрозах и атаках
- Сбор информации о фактическом состоянии внешней инфраструктуры, оценка актуальности рисков и угроз для отрасли
- Взаимодействие с разработчиками ПО в части ИБ
- Проведение совместных киберучений, обучающих мероприятий
- Проработка методологий и отраслевых стандартов в области ИБ
- Проведение аудитов по ИБ и оценка защищенности совместно с предприятиями и регуляторами (ФСБ России, ФСТЭК России, ведомственный центр ГосСОПКА Минэнерго России)

Энерго ЦИБ на базе АЦЭ (ENERGO ISAC)

- Содействие организациям электроэнергетики в предотвращении и устранении последствий киберугроз, путем сбора, анализа и распространения среди своих членов информации, которая может быть использована для принятия мер, а также путем предоставления своим партнерам инструментов для уменьшения рисков и повышения устойчивости функционирования информационной инфраструктуры
- Содействие отраслевому (ведомственному) центру кибербезопасности Минэнерго России (в качестве аналитического центра экспертизы консолидированной информации и обеспечения оперативного взаимодействия с компаниями электроэнергетики)

Подразделения ИБ компании энергетического сектора

- Разработка корпоративных планов развития ИБ
- Реализация мероприятий по ИБ на предприятиях и объектах электроэнергетики, включая оценку защищенности объектов КИИ
- Мониторинг состояния ИБ и реагирование на инциденты ИБ



Энерго ЦИБ сегодня



1

Выстраивание партнерской сети и подготовка платформы для реализации задач

2

Обеспечение «профилирования» компаний электроэнергетики по результатам обмена информацией по соглашениям

3

Повышение осведомленности компаний электроэнергетики

4

Формирование каталога услуг Энерго ЦИБ



01

Выстраивание партнерской сети и подготовка платформы для реализации задач

Подготовлен проект списка возможных для сотрудничества организаций, имеющих практическое значение для членов АЦЭ с оценкой требуемых сроков для заключения соглашений (рассмотрен на встрече ЭГ от 31.08.2023).

Подготовлен отдельный раздел на сайте Ассоциации для Энерго ЦИБ. Размещаются актуальные материалы <https://www.digital-energy.ru/activity/expert-group/energy-csc/>

02

Обеспечение «профилирования» компаний электроэнергетики по результатам обмена информацией по соглашениям, заключенным в соответствии с предыдущим п.1

Периодически среди участников ЭГ организуем опросы и уточнениям приоритеты по реализации ранее запланированных задач/KPI проекта Энерго ЦИБ. Основные направления деятельности на 2024 год:

- 1) Аналитическая и экспертная деятельность;
- 2) Популяризация деятельности АЦЭ;
- 3) Участие в реализации задач в соответствии с Планом работы ЭГ по кибербезопасности;
- 4) Обеспечение внешней экспертной деятельности АЦЭ;
- 5) Повышение осведомленности.

Ведется уточнение потребностей на плановых и расширенных встречах ЭГ

03

Повышение осведомленности компаний электроэнергетики

Текущие приоритетные задачи:

- Разработка перечня учебных курсов по ИБ с учетом категории слушателей (ЛПР (ЗГД), специалисты по ИБ, сотрудники предприятий).
- Демонстрация УЦ пробного учебного модуля образовательного курса
- Иные задачи по плану работ

04

Формирование каталога услуг Энерго ЦИБ

В 2024 году планируем реализацию проекта «Паспортизация процессов разработки и обеспечения качества программного обеспечения».



Подготовка и
подписание соглашений
о сотрудничестве

Информационная
система/платформа обмена
информации и взаимодействия



Приглашаем присоединиться



Вузы:

- НИУ МЭИ;
- РГУ нефти и газа (НИУ) имени И.М. Губкина;
- Казанский государственный энергетический университет;
- Нижегородский государственный технический университет им. Р.Е. Алексеева;
- Ивановский государственный энергетический университет имени В.И. Ленина.



Ассоциации и консорциумы



Компании электроэнергетической отрасли

<https://www.digital-energy.ru/activity/expert-group/energy-csc/>



об угрозах и уязвимостях систем промышленной автоматизации в электроэнергетике



о курсах и преподавателях, которые могут обеспечить повышение осведомленности сотрудников предприятий электроэнергетики в области информационной безопасности в регионах



актуальных задачах в области информационной безопасности в электроэнергетике, которые могли бы быть использованы в качестве тем выпускных квалификационных работ