ИТОГИ ОКИТ–2023: КРУГЛЫЙ СТОЛ «ПРАКТИКА ЗАЩИЩЁННЫХ ПРОГРАММНЫХ РЕШЕНИЙ В CLOUD NATIVE ПОДХОДЕ ДЛЯ ЭЛЕКТРОЭНЕРГЕТИКИ»

В. КАРАНТАЕВ (Ассоциация “Цифровая энергетика”)

ЦИФРОВАЯ ЭНЕРГЕТИКА

Ассоциация “Цифровая энергетика” провела круглый стол в рамках Объединённой конференции ИТ-служб энергокомпаний в Казани. Темой экспертной дискуссии стала практика защищённых программных решений в подходе cloud native для электроэнергетики.

Модераторами круглого стола стали председатель правления АЦЭ **Тамара Меребашвили** и заместитель руководителя экспертной группы по кибербезопасности **Дмитрий Васильев**.

Тамара Меребашвили, *председатель Правления Ассоциации “Цифровая энергетика”, заместитель генерального директора – руководитель Блока корпоративных и имущественных отношений ПАО “Интер РАО”*

Дмитрий Васильев, *руководитель экспертной группы по кибербезопасности Ассоциации “Цифровая энергетика”, директор департамента ИБ ПАО “Интер РАО”*

Как подчеркнула **Тамара Меребашвили**, Ассоциация постоянно анализирует лучшие подходы к цифровой трансформации и работает на их внедрение в электроэнергетическую отрасль. Важнейшая задача российской электроэнергетики в настоящий момент – обеспечение технологического суверенитета в условиях постоянно усложняющегося ландшафта цифровых угроз.

Компьютерные атаки стали более комплексными, а деятельность злоумышленников – более организованной. Трендом являются атаки на цепочки поставок услуг и продуктов, применяемых в отрасли, что требует принятия как правовых, так и технических мер.

Разработка защищённого программного обеспечения, безопасное использование продуктов с открытым кодом – проблемы, требующие решения. Всё это определило выбор темы для открытого диалога.

Для круглого стола удалось сформировать сбалансированный состав участников.

Руководитель Центра Национальной технологической инициативы Московского энергетического института **Александр Волошин** представил взгляд отраслевого эксперта. Он объединил прогноз технологического развития отрасли на ближайшие несколько десятилетий с представлением результатов работы ЦНТИ МЭИ по разработке современных отечественных технологий. Среди них – цифровые двойники энергосистем, изначально созданные для размещения в облачной инфраструктуре.

Главным выводом, который сделал Волошин, является безальтернативность применения облачных решений для выполнения целого ряда отраслевых задач.

Опираясь на анализ мирового опыта, эксперт представил концепцию технологической платформы “частного промышленного облака”. В ней уже сейчас решены проблемы реализации интеллектуальной системы релейной защиты и автоматики, цифрового двойника, систем автоматического проектирования. При этом разработанные ИС РЗА не имеют аналогов в мире.

По мнению Александра Волошина, использование облачных технологий привнесёт новые качества в процессы технологического управления уже в краткосрочной перспективе. Однако требуется решить задачи эффективного проектирования информационно-управляющих систем, обеспечения кибербезопасности с применением практик создания безопасного программного обеспечения.

Вторым привлечённым экспертом стал менеджер группы продуктовой архитектуры команды Security & Compliance Yandex.Cloud **Рами Мулейс**. Он выступил с докладом "Что проще: безопасная разработка в публичном или приватном облаке".

Рами Мулейс подробно рассмотрел преимущества и риски использования публичных облачных платформ, а также предоставляемую ими защиту. Эксперт рассказал о работе Yandex по построению безопасной облачной инфраструктуры и о курсах для DevSecOps-инженеров, доступных на сайте оператора.

Модератор отметил важность и готовность коллег делиться экспертизой, добавив, что специалистам АЦЭ предстоит оценить применимость стандарта защиты Yandex при реализации отраслевых сценариев.

Представители другого облачного оператора – компании Softline – подхватили тему и рассказали о приватных облаках. Директор по продажам сервисов в электроэнергетике **Александр Бочаров** и руководитель отраслевой экспертизы ИБ в секторе ТЭК **Александр Фрайтер** представили доклад на тему "Private Cloud – максимально защищённое решение для электроэнергетики".

Как заявили докладчики, технологии частного облака позволяют быстро и эффективно выполнить требования президентских указов о технологической независимости и безопасности критической информационной инфраструктуры.

Александр Бочаров привел несколько примеров сценариев возможного использования частного облака. Так, оно может быть полезным для построения системы описания и автоматизации бизнес-процессов, а также для быстрого обучения персонала.

Со-модератор **Дмитрий Васильев** инициировал дискуссию о правовых и технических рисках применения частных и публичных облачных решений в электроэнергетике. Присутствующие в зале вспомнили негативный опыт непредсказуемого ухода с рынка провайдера Cloudmouse – в 2015 году компания из-за аппаратного сбоя потеряла десятки тысяч клиентских виртуальных машин без возможности восстановления.

Вторая часть круглого стола была построена вокруг докладов экспертов, реализующих решения DevSecOps в реальных проектах.

Её открыл ведущий архитектор ИБ компании Swordfish Security **Юрий Шабалин**, рассказавший о плюсах и минусах платформы безопасной разработки в cloud native.

Доклад был интересен обзором базовых практик – статического (работа с исходным кодом) и динамического (работа с приложением) анализа кода, а также корреляцию и оркестрацию средств анализа.

Юрий Шабалин рассмотрел совмещение инструментов анализа с системами непрерывной интеграции, доставки и развёртывания. Отдельно эксперт остановился на практиках композиционного анализа, которые приобретают значимость в условиях атак на цепочки поставок.

Стоит отметить, что проект национального стандарта, посвящённый построению и применению данных практик подготавливается техническим комитетом Росстандарта "Защита информации".

Также Шабалин дал несколько советов: отталкиваться от особенностей процесса разработки, пользоваться конкретными метриками и распространять требование защищённости на все этапы жизненного цикла ПО.

Всегда интересны практические доклады представителей электроэнергетической отрасли. О внедрении безопасной разработки в АО "СО ЕЭС" рассказал главный эксперт службы информационной безопасности компании **Александр Малахов**.

Он подчеркнул, что "Системный оператор" в основном заказывает разработку ПО у сторонних организаций. При этом, в части информационной безопасности объектов критической информационной инфраструктуры, основополагающей целью для компании является соответствие требованиям приказа ФСТЭК № 239, ввиду чего процесс безопасной разработки ПО в "Системном операторе" направлен на проведение контроля уровня информационной безопасности ПО и контроля выполнению требования приказа ФСТЭК № 239 со стороны разработчиков.

Со стороны "Системного оператора" взаимодействие с исполнителями осуществляет сотрудник с достаточно уникальным набором компетенций: это специалист по информационной безопасности, обладающий реальными навыками разработки программного обеспечения. Кроме того, требования информационной безопасности по созданию ПО распространяются на всех стадиях жизненного цикла, включаются в договора, и до устранения всех уязвимостей работа не принимается.

Александр Малахов также отметил, что компания проводит анализ исходных кодов ПО на соответствие требованиям ИБ, а также проводит компиляцию исходных кодов в своей инфраструктуре.

Завершился круглый стол ещё одним практическим докладом. Независимый эксперт **Кирилл Ильин** представил кейс выстраивания безопасного жизненного цикла разработки микросервисной инфраструктуры с нуля.

Он напомнил, что предпосылок для введения концепции DevSecOps достаточно. Многогранность cloud native подразумевает широкий пул возможных угроз, а инструментов для повышения защищённости и наблюдаемости не хватает, кроме того, провайдеры не всегда заботятся о проблемах безопасности.

Подход эксперта – взращивание в качестве security champions не только команды разработки, но и продакт-менеджера, архитектора, тестировщиков и других людей, вовлечённых в выстраивание безопасного жизненного цикла.

Главные рекомендации: поиск общих точек соприкосновения с остальными участниками команд и менеджмент сроков устранения уязвимостей. При этом эксперт предложил наглядный как для бизнеса, так и для разработчиков калькулятор критичности дефектов защиты, который показывает финансовые потери при эксплуатации той или иной уязвимости.

Самое главное, по словам Ильина, – формирование культуры безопасности и непрерывное повышение квалификации.

Результаты дискуссии свидетельствуют о необходимости создания отраслевой структуры требований в области разработки безопасного ПО. Регулирование должно распространяться на всё программное обеспечение, разрабатываемое в интересах электроэнергетической отрасли, включая объекты критической инфраструктуры.

Кроме того, электроэнергетика нуждается в организованной подготовке специалистов данной сферы и учреждении отраслевых центров анализа результатов разработки ПО.

Предполагается, что эти инициативы должны быть реализованы в координации с Минэнерго и регулятором в области ИБ – ФСТЭК, а также при непосредственном участии Ассоциации “Цифровая энергетика”.

Ещё один вывод: эксплуатация приложений, разработанных специально для облачной инфраструктуры, возможна при принятии мер по защите информации, а также определении актуальных отраслевых сценариев использования.

Ассоциация “Цифровая энергетика”
Владимир Карантаев *– эксперт Ассоциации “Цифровая энергетика”*
115093, г. Москва, ул. Щипок, д. 18, стр. 2
Телефон +7 (495) 211-52-00
E-mail: info@digital-energy.ru
https://www.digital-energy.ru/