СИСТЕМНЫЙ ОПЕРАТОР
ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ
RUSSIAN POWER SYSTEM OPERATOR

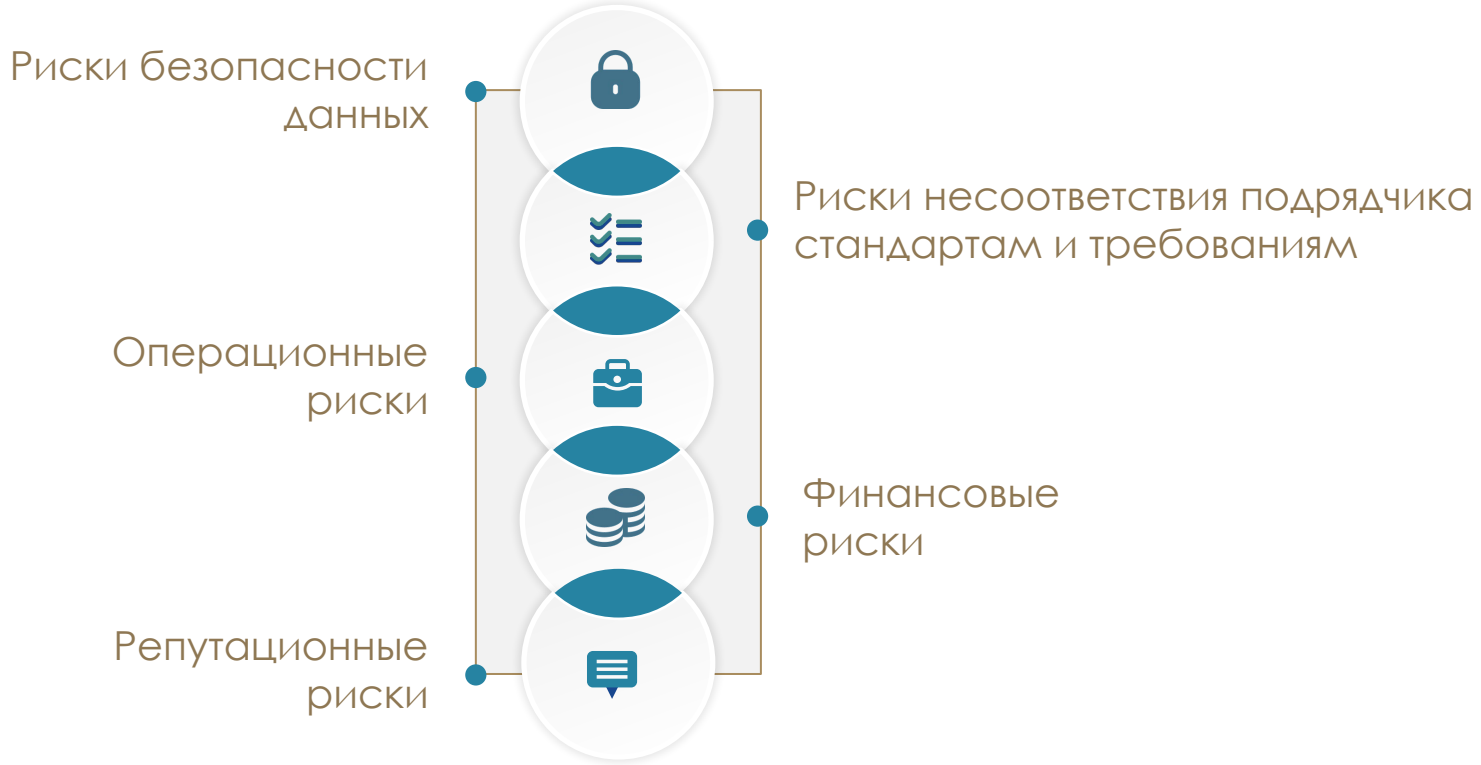
ЦИФРОВАЯ ЭНЕРГЕТИКА

УПРАВЛЕНИЕ РИСКАМИ ПРИ РАБОТЕ С ВНЕШНИМИ ПОДРЯДЧИКАМИ: ТАКТИКИ И ИНСТРУМЕНТЫ

ТБ Форум
Москва, 2025

Капустин Александр Владимирович
Заместитель начальника службы ИБ СО ЕЭС–
Заместитель руководителя ЭГ по кибербезопасности АЦЭ

ОСНОВНЫЕ РИСКИ ПРИ РАБОТЕ С ПОДРЯДЧИКАМИ



СПОСОБЫ УПРАВЛЕНИЯ РИСКАМИ

- Проведение анализа безопасности подрядчиков на этапе заключения договоров и регулярный пересмотр их статуса
- Внедрение политик взаимодействия с подрядчиками, закрепляющих процедуры по минимизации рисков
- Включение в планы реагирования на инциденты сценариев атак через подрядчиков, а также мониторинг критичных учетных записей

Оценка уровня риска ИБ подрядчиков до начала взаимодействия	2024 год	2022-2023 годы
Проводят свой/независимый аудит для критичных подрядчиков	36%	17%
Проводят только проверку по линии экономической безопасности	48%	68%
Третьи лица заполняют анкету с вопросами по ИБ	16%	15%

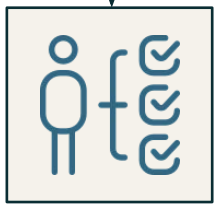
Реализованные меры по мониторингу событий ИБ, связанных с подрядчиком	2024 год	2022-2023 годы
Есть отдельные правила на учетки подрядчиков, СЗИ или критичную инфраструктуру, к которой подрядчики имеют доступ	48%	18%
Осуществляют мониторинг событий ИБ в целом, фокус на подрядчиков не делают	48%	77%
Иное	4%	5%

Формализован процесс безопасного взаимодействия с подрядчиками	2024 год	2022-2023 годы
Есть отдельный документ, детализирующий меры безопасности при работе с подрядчиками	48%	19%
Есть требования только по безопасной передаче информации подрядчикам	42%	71%
Нет или в процессе разработки	10%	10%

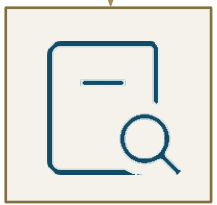
**По данным Анализа ландшафта угроз кибербезопасности за 2024 г. от Инфосистемы Джет*

ВЫБОР ПОДРЯДЧИКОВ

Минимизация рисков при отборе подрядчиков



Делегирование простых задач, ограничение доступа к ключевым ресурсам



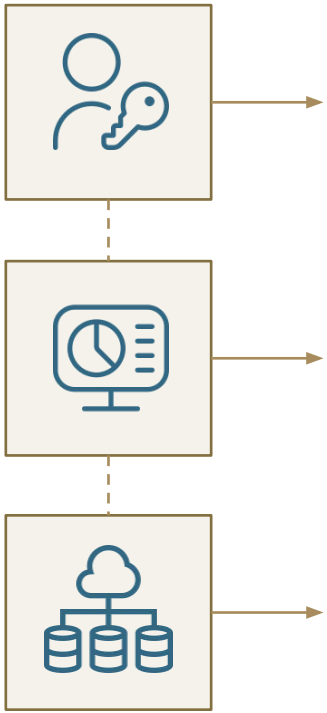
Оценка квалификации и сбор информации о потенциальном подрядчике

ЮРИДИЧЕСКИЕ ИНСТРУМЕНТЫ МИНИМИЗАЦИИ РИСКОВ

Соглашение о неразглашении (NDA)

Закрепление в договорах ответственности подрядчиков за соблюдение требований информационной безопасности заказчика (ЛНА и законодательство)

ТЕХНИЧЕСКИЕ ИНСТРУМЕНТЫ

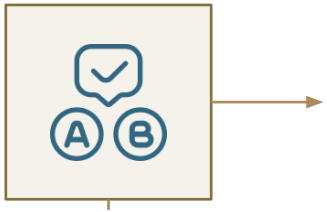


Управление доступом

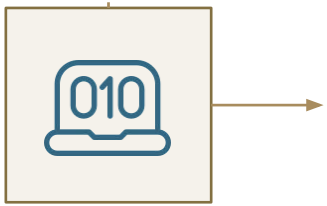
Системы мониторинга и обнаружения угроз (SIEM). Мониторинг со стороны SOC действий подрядчика (в части соблюдения мер ИБ)

Проведение тестирования на проникновение (пентеста) инфраструктуры подрядчика до начала выполнения работ

ОРГАНИЗАЦИОННЫЕ ИНСТРУМЕНТЫ



Разработка обучающего курса по требованиям ИБ заказчика для подрядчиков и тестирование их знаний перед началом работы (для критических систем при предоставлении доступа с административными привилегиями)



Контроль процесса безопасной разработки ПО*

**На базе ЭнергоЦИБ - Ассоциация «Цифровая Энергетика» разработаны проекты документов:*

- *обоснование необходимости реализации процессов безопасной разработки ПО;*
- *методика самотестирования разработанного и предлагаемого к внедрению на предприятия участников Ассоциации ПО;*
- *чек-лист результатов самотестирования;*
- *шаблон технического заключения по результатам тестирования.*

ПРОБЛЕМЫ И ИХ РЕШЕНИЕ ГОСУДАРСТВОМ

Проблемы	Решение
Сложность предъявления типовых требований к исполнению обязательств по ИБ	Необходимы законодательные изменения, обязывающие подрядчиков выполнять требования по ИБ*
Отсутствие обязательного контроля со стороны регуляторов за исполнением обязательств в части ИБ, предъявляемых заказчиками к подрядчикам	Необходимо, чтобы надзорные органы обеспечивали контроль соблюдения подрядчиками установленных требований по ИБ

*Пример нормативного регулирования из Проект приказа ФСТЭК России «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»:

- *«**Обязанность подрядной организации** по выполнению политики защиты информации должна быть **указана в договоре** или ином документе, на основании которого передается информация, предоставляется доступ к информационным системам оператора или содержащейся в них информации»*
- *«**Обязанность подрядной организации** по выполнению внутренних стандартов и регламентов по защите информации должна быть **указана в договоре** или ином документе, на основании которого передается информация, предоставляется доступ к информационным системам оператора или содержащейся в них информации.»*

АЛГОРИТМ ДЕЙСТВИЙ ДЛЯ УСИЛЕНИЯ БЕЗОПАСНОСТИ РАБОТЫ С ПОДРЯДЧИКАМИ В ТЕКУЩИХ УСЛОВИЯХ

- С подрядчиками заключается соглашение о соблюдении требований по ИБ. Устанавливаются требования к оборудованию подрядчика, к парольной защите учетных записей, обязанности подрядчика при выполнении работ на информационных ресурсах
- Перед началом работ с информационными ресурсами заказчика со стороны подрядчика предоставляется заполненная анкета по вопросам ИБ, отчет об антивирусной проверке оборудования подрядчика, используемого для целей подключения к инфраструктуре заказчика
- По требованию заказчика, осуществляется прохождения работниками подрядчика инструктажа по ИБ организуемого заказчиком в соответствии с программой, разработанной заказчиком
- Осуществляется мониторинг, контроль, запись действий подрядчика (процессов, запускаемых от имени подрядчика) в части соблюдения мер ИБ
- При фиксации событий (инцидентов) ИБ в рамках выполнения работ подрядчиком приостанавливается выполнение работ непосредственно на информационных ресурсах и отключается доступ для подрядчика
- При выявлении инцидентов подрядчик обеспечивает проведение заказчиком оценки защищённости в инфраструктуре подрядчика

СИСТЕМНЫЙ ОПЕРАТОР
ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ
RUSSIAN POWER SYSTEM OPERATOR

ЦИФРОВАЯ ЭНЕРГЕТИКА

СПАСИБО ЗА ВНИМАНИЕ!

www.so-ups.ru
Официальный сайт

https://t.me/so_ups_official
Официальный телеграм-канал

Капустин Александр Владимирович
Заместитель начальника службы ИБ –
начальник отдела защиты КИИ

ПРИЛОЖЕНИЕ

РЕКОМЕНДАЦИИ ОТ НКЦКИ

Атаки через подрядчика. Что нужно предпринять*

1. Выдвигать требования по обеспечению безопасности инфраструктур подрядчиков
2. Контролировать действия внешних пользователей
3. Минимизировать каналы удаленного управления
4. Отслеживать информацию об инцидентах
5. Иметь план действий

*По данным доклада НКЦКИ на Инфофорум 2025

РЕКОМЕНДАЦИИ ОТ НКЦКИ

Атаки через подрядчика. Типовые недостатки инфраструктуры*

1. Подключение к инфраструктуре с любых IP-адресов
2. Отсутствие процесса проверки наличия ВПО
3. Отсутствие требований по ИБ к виртуальным серверам
4. Используются небезопасные протоколы удаленного доступа
5. Не производится обновление используемого ПО
6. Забытые каналы доступа в инфраструктуру заказчика

*По данным доклада НКЦКИ на Инфофорум 2025