ДИТ

Организационное обеспечение защиты от компьютерных атак

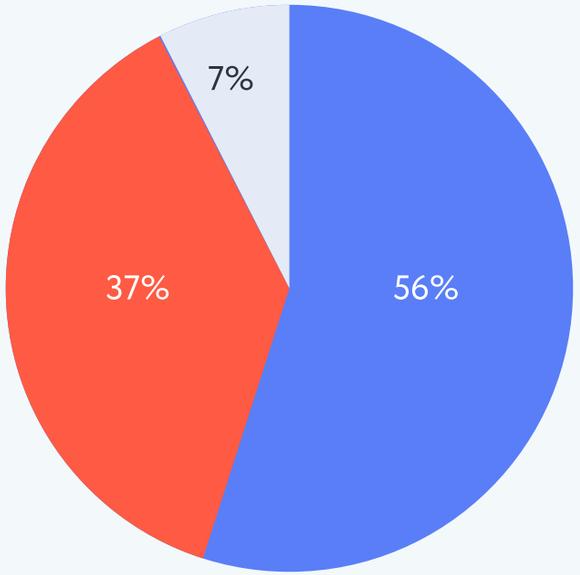
автоматизированных систем управления субъектов критической информационной инфраструктуры

Управление информационной безопасности
В. В. Комаров, ДИТ Москвы

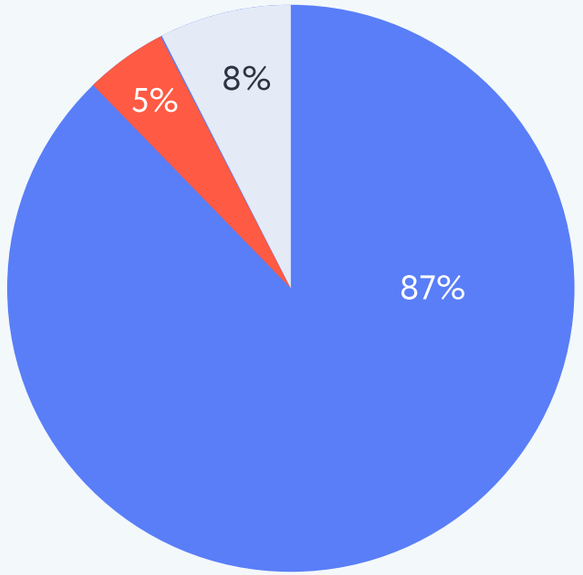
ДИТ

Объекты защиты

Распределение объектов КИИ по сферам городского хозяйства



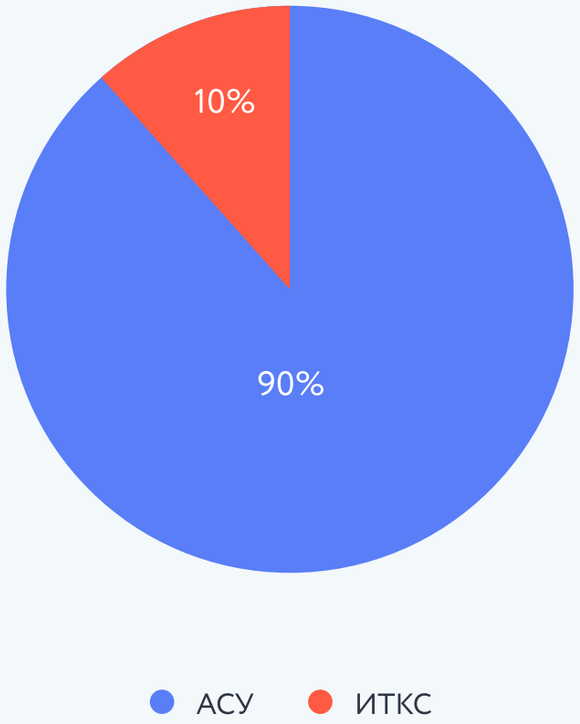
Распределение ЗОКИИ по сферам городского хозяйства



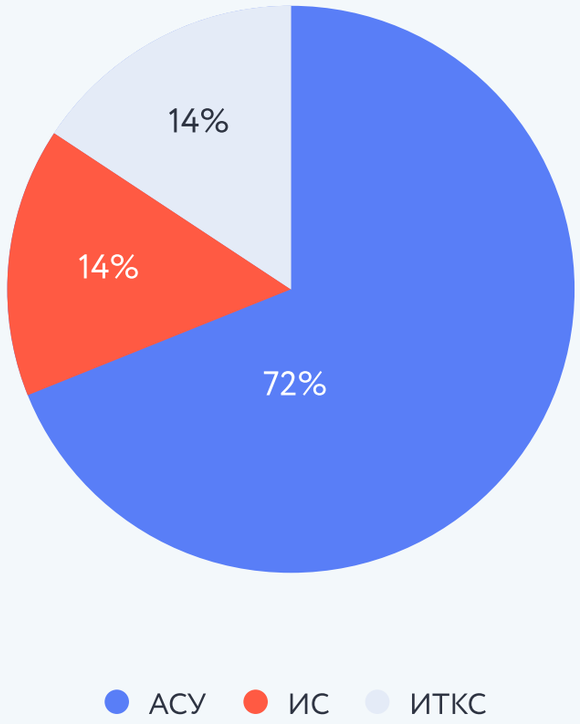
ЖКХ Здравоохранение Транспорт

Объекты защиты

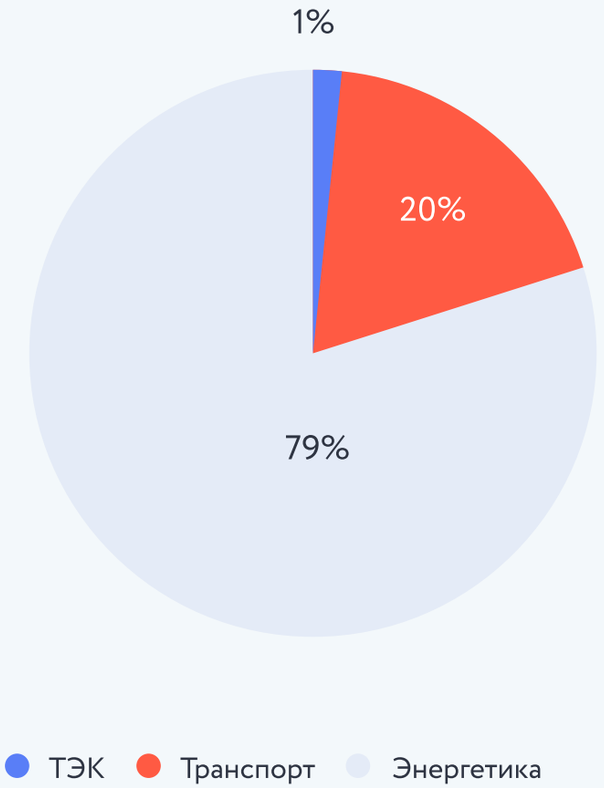
ЖКХ



Транспорт



ЖКХ



ДИТ

Главное – люди

— Мы внедрили техническое решение по защите объекта КИИ, теперь он в безопасности?

— Нет, если не решены следующие организационные вопросы:

01 Работник обучен использованию технического решения?

02 Техническая поддержка пользователя организована?

03 Контроль за технической поддержкой пользователя обеспечен?

04 Процедура реагирования на компьютерные инциденты?

05 Оценка эффективности защиты проводится на регулярной основе?

ДИТ

Знание – сила

Обучение работников:

01

Вебинары, семинары, инструктажи

02

Интерактивные курсы в системе дистанционного обучения

03

Памятки, постеры, экранные заставки по корпоративным каналам оповещения работников

04

Учения и тренировки

Работники службы технической поддержки требуют отдельного обучения и более пристального внимания службы ИБ

ДИТ

К победе идут командой

Работник на удаленной площадке не должен чувствовать себя одиноким и брошенным:

- Доступный канал обращений в техподдержку
- Доступный канал информирования о компьютерных инцидентах
- Резервирование каналов оповещения и взаимодействия со службой ИБ

Акцент на контроль:

- Оперативного реагирования службы ИБ на обращения работника
- Эффективности и достаточности плановых мер реагирования на компьютерные инциденты
- Доступа посторонних лиц к каналам взаимодействия

Планирование – основа успеха

У нас случился компьютерный инцидент на удаленном объекте, но мы знаем:

- Как восстанавливаем работоспособность
- Как предотвращаем аналогичные компьютерные инциденты на других объектах
- Как расследуем причину возникновения компьютерного инцидента
- Как используем результаты расследования
- Как будем взаимодействовать с внешними организациями, включая правоохранительные и надзорные органы, при серьезных компьютерных инцидентах

ДИТ

Всегда на связи!

mos.ru/dit

vk.com/ditmos

twitter.com/ditmos

facebook.com/ditmos

ok.ru/ditmos