Центр информационных технологий Красноярского края

Атака через поставщика услуг: защита в собственных руках

Заместитель руководителя по ИБ КГКУ «ЦИТ»
Бычков С.С.

Центр информационных технологий Красноярского края

ИБ Красноярского края

Силы и средства

Лицензии: ТЗКИ ФСТЭК России, ФСБ России

Штат работников: 30 ш.е.

Круглосуточная линия ИБ: 5 ш.е.

Количество объектов мониторинга: 3 425

СКЗИ: ПАК: 695 ед., 7200 клиентов

МЭ + IDS: 14 ед.

Система корреляции: 6000 лицензий

Система автоматизации: 8 модулей реагирования

Сканер уязвимостей: 4000 лицензий

АВЗ: 32 000

Объекты защиты

ГИС – 47 (все ГИС аттестованы)

КИИ – 247 ОКИИ, из которых 7 ЗОКИИ

АРМ – более 25 000

ВМ – более 1500

Точки доступа в Интернет – 3224 точки

Отрасли перешедшие на обслуживании: социальная защита населения, культура, ЗАГС, Финансы, Экономика, Экология, Промышленность, Транспорт

Центр информационных технологий Красноярского края

Источник угрозы безопасности информации

— субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

[ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения»]

Подрядчик

Основная деятельность направлена на решение собственных задач, в рамках которых ИБ не является приоритетом

Центр информационных технологий Красноярского края

Аутсорсинг

профессиональный инструмент, который приносит много пользы и выгод, при его правильном применении, но, если им неправильно пользоваться - скорее всего все будет сломано.

- Универсального средства не существует, но всегда есть набор подходов.
- Описанные правила реализации помогут всем
- Четкое понимание возможностей приближает ожидание и реальность
- Концентрация на источнике проблем, а не на их последствиях/признаках

Центр информационных технологий Красноярского края

Задачи:

1. **Требования регуляторов**
   Выполнение мер по защите информации, в соответствии с установленными требованиями регулятора
2. **Реальный контроль**
   Решение задачи доступа подрядных организаций в реалиях возрастающего тренда киберугроз
3. **Гибкость применяемого решения**
   Организация доступа настраивается по различным сценариям

Решения:

1. **Применение PAM систем**
   Дополнительный фактор, который позволяет объективно следить за поставщиками
2. **Регламенты**
   Описание процедур и их утверждение приводят к неотвратимости процессов защиты информации
3. **Противопоставление ценностей**
   Работа с противоречиями и отрицаниями, указание на реальные цели и задачи.

Центр информационных технологий Красноярского края

ИБ – защита не только от киберугроз

Контроль реального времени работы
Наблюдение за реальным временем выполнения работ по ГК, а также за скоростью реакции на заявки

Поиск виновников при возникновении проблем при обслуживании
Анализ логов действий подрядчиков. Выявление момента возникновения проблемы

Анализ скорости реакции
Объективная оценка начала и окончания времени выполнения работ