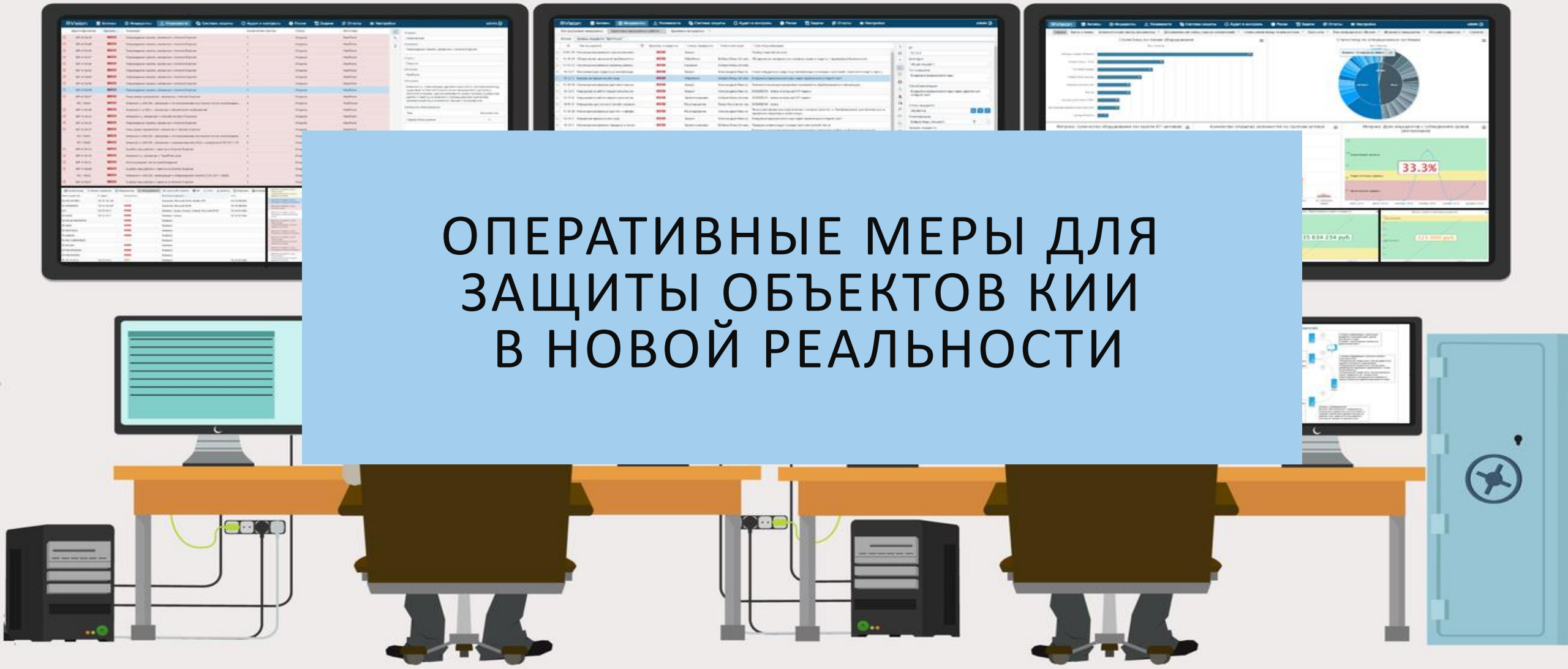


ОПЕРАТИВНЫЕ МЕРЫ ДЛЯ ЗАЩИТЫ ОБЪЕКТОВ КИИ В НОВОЙ РЕАЛЬНОСТИ

КОНСТАНТИН САМАТОВ

Член Правления Ассоциации руководителей служб информационной безопасности

ЧТО ПРОИСХОДИТ?

Остановка деятельности зарубежных производителей решений по защите информации, односторонний отказ от техподдержки, отзыв лицензий/блокировка

Массированные компьютерные атаки на информационную инфраструктуру:

- DDos
- Сканирование на уязвимости
- Дефейс внешних сайтов
- Фишинг: Remote Administration Tool, Ransomware

Проблемы с цепочками поставок: ИТ оборудование

Рост цен со стороны поставщиков и вендоров

Отсутствие отечественных аналогов

Уязвимости в исходном коде свободно-распространяемого ПО, ОС Linux

Усиление регуляторного влияния:

- Новый постоянный регулятор – Минцифры
- Псевдорегуляторы: Минообр, департамент ЖКХ
- Вал рекомендаций регуляторов (около 20 документов)
- Информирование, отчетность и выездные проверки

КУДА БЕЖАТЬ/ЧТО ДЕЛАТЬ?

ШАГ 1. ИНФОРМИРОВАНИЕ ПЕРСОНАЛА

Информирование работников организации о необходимости:
• отправки всех подозрительных электронных писем на специально выделенный почтовый ящик для проверки;
• внимательно проверять адреса отправителя, даже в случае совпадения имени с уже известным контактом;
• не открывать письма от неизвестных адресатов;
• проверять письма, в которых содержатся призывы к действиям («открой», «прочитай», «ознакомься»);
• не переходить по ссылкам, которые содержатся в электронных письмах;
• не нажимать на ссылки из письма, если они заменены на слова или фразы;
• внимательно относиться к письмам с большим количеством получателей или письмам на иностранном языке.

Ограничение на передачу информации в мессенджерах (в т.ч. телеграмм)

Проведите с сотрудниками организации занятия по информационной безопасности, противодействию методам социальной инженерии, а также принципам безопасной удаленной работы.

Проведение КШУ с персоналом

ШАГ 2. АКТУАЛИЗАЦИЯ ДЕЛОВЫХ ПРОЦЕССОВ

Резервное копирование на дату последних обновлений/ежедневное резервное копирование обрабатываемой информации (по крайней мере для критичных систем)

Ограничение на использование внешних облачных сервисов, принадлежащих зарубежным компаниям

Отключение автоматического обновления программного обеспечения. Установка обновлений после анализа вероятного воздействия.

Мониторинг информационных ресурсов и событий информационной безопасности

Организация дежурств персонала включая обеспечивающих функционирование и эксплуатирующих

Организация взаимодействия с провайдерами услуг анти DDos

Разработка и поддержание в актуальном состоянии планов реагирования (алгоритмов/скриптов действий) на основные типы инцидентов: DDoS-атака (сетевого уровня, прикладного уровня); дефейс сайта; несанкционированный доступ к интерфейсу управления; обнаружение утечки учетных данных и т.п.

Разработка планов импортозамещения

ШАГ 3. НАСТРОЙКА СЗИ

Настройка ограничений на межсетевых экранах: настройка МЭ на блокировку «белым списком», блокировка входящего трафика с зарубежных IP-адресов, из Tor, отключение неиспользуемых портов

Настройка ограничений на использование съемных носителей информации

Ограничение доступа на уровне операционных систем с целью исключения установки и запуска зарубежного ПО

Смена паролей учетных записей прежде всего административных

Проверка наличия дефолтных учеток и паролей с заменой

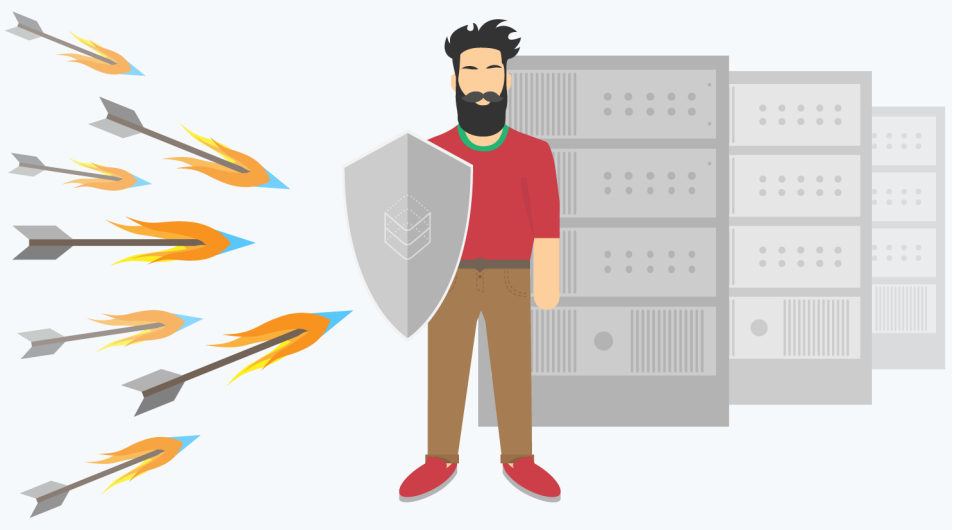
Переключение на Российские DNS сервера: корпоративные или российского оператора

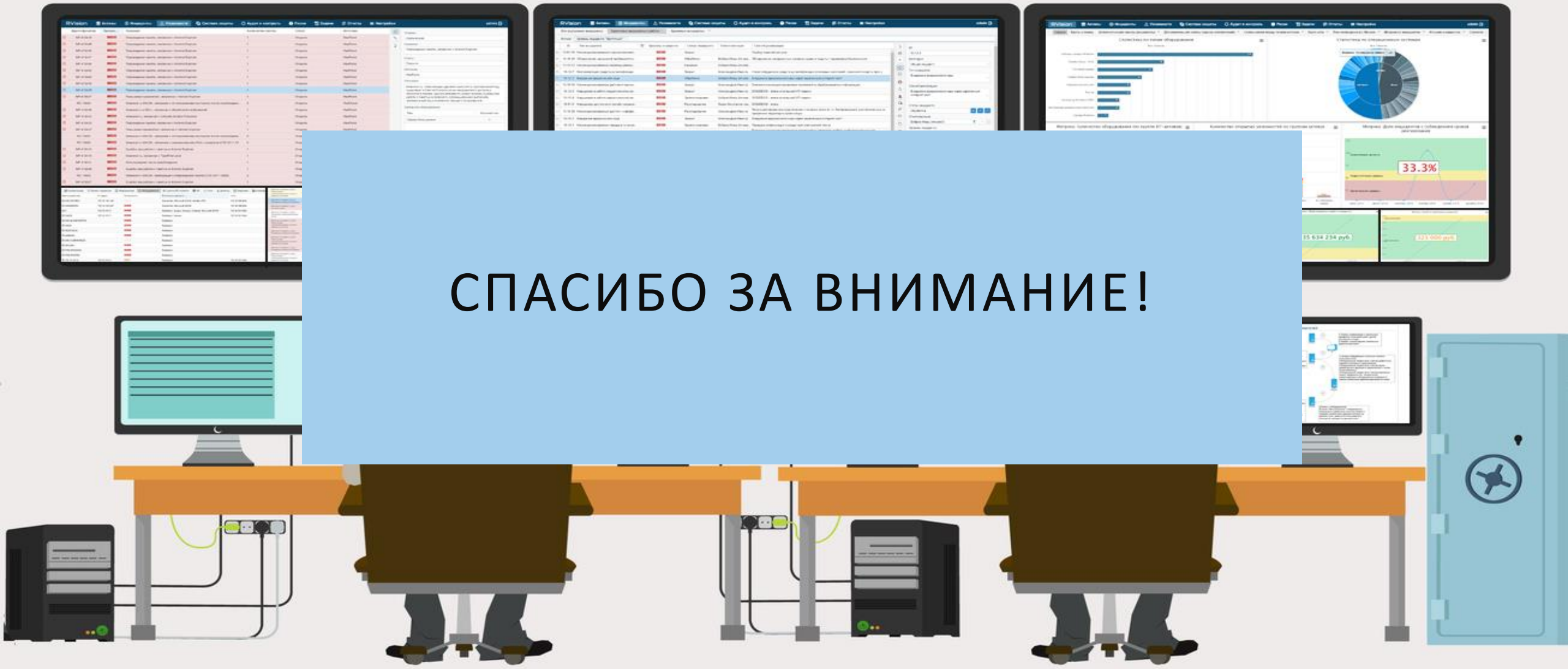
Отключение неиспользуемых сервисов

Переключение на безопасные версии протоколов

Анализ и устранение уязвимостей узлов, являющихся точками проникновения (например, с помощью ScanOVAL)

Переход на Российские браузеры Яндекс и Атом, либо попробовать сборку на хромиуме собрать





СПАСИБО ЗА ВНИМАНИЕ!

КОНСТАНТИН САМАТОВ

Член Правления Ассоциации руководителей служб информационной безопасности