

## Памятка

# Как работать со средствами криптографической защиты информации




### Статьи:

- [Как шифровать каналы связи и соблюдать требования регуляторов](#)
- [Кто, что и зачем пишет в журнале учета СКЗИ](#)
- [Защитить информацию и ничего не нарушить: какие вопросы мы задаем при работе с СКЗИ](#)
- [Производительность криптошлюзов: обещания вендоров и суровая реальность](#)
- [Полный compliance: на что обратить внимание при предоставлении СКЗИ по сервисной модели](#)

### Записи вебинаров и эфиров:

- [Как выбрать корпоративный VPN-шлюз](#)
- [По каким критериям выбирать криптошлюзы](#)
- [Как без боли заменить зарубежные VPN-шлюзы на российские криптомаршрутизаторы](#)

 [Шифрование каналов связи для различных сфер деятельности на конкретных примерах](#)

### Законодательство:

- [Общие сведения по сертификации СЗИ](#)
- [Документы по стандартизации, разработанные с участием организаций — членов и экспертов ТК 26](#)
- [Проект приказа ФСБ России «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных \(криптографических\) средств»](#)



Наша регулярная рубрика  
[«Compliance-дайджест: что изменилось в ИБ-законодательстве»](#)



Сервис шифрования каналов связи позволит организовать защищенное взаимодействие между геораспределенными объектами и выполнить требования российского законодательства.

[Подробнее](#)