Требования ФСБ России к обращению со средствами криптографической защиты информации

Владивосток, 2021

Нормативно-методические документы, действующие в отношении применения СКЗИ

«Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденное **приказом ФСБ России от 9 февраля 2005 года № 66**

«Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная **приказом ФАПСИ от 13 июня 2001 года № 152**

«Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утвержденный **приказом ФСБ России от 10 июля 2014 года № 378**

Основные требования к применению СКЗИ:

- действующий сертификат,

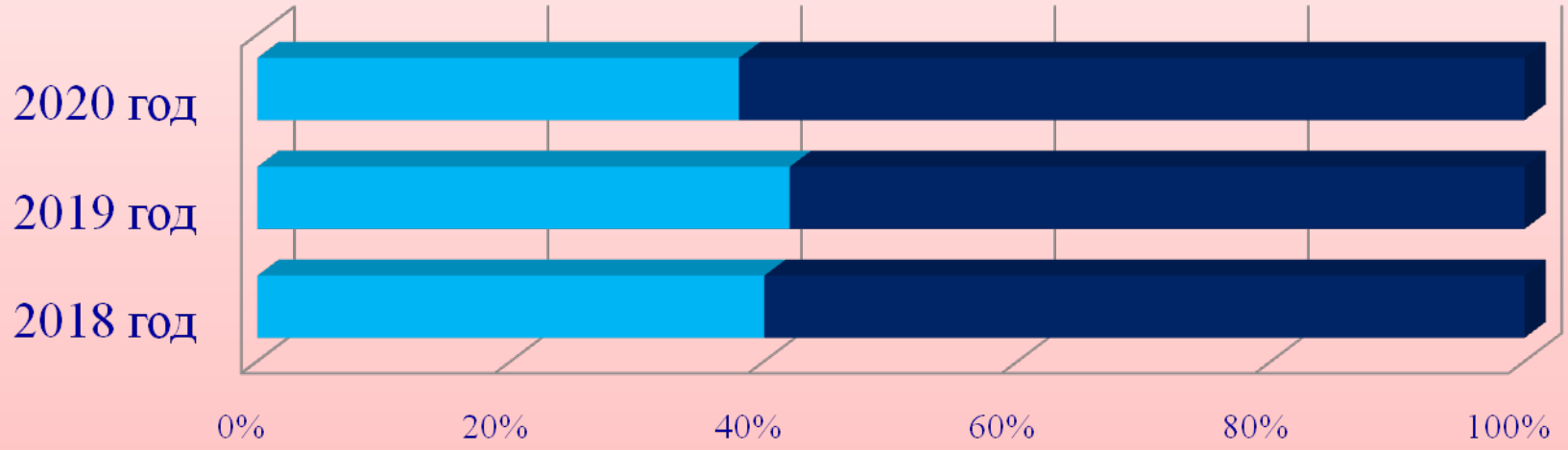
Перечень средств защиты информации, сертифицированных ФСБ России,
представлен на сайте
Центра по лицензированию, сертификации
и защите государственной тайны ФСБ России clsz.fsb.ru

Основные требования к применению СКЗИ:

- приобретение у лицензиатов ФСБ России,
- учёт по установленным формам,
- обучение пользователей с документальным оформлением,
- исключение несанкционированного доступа к СКЗИ,
- наличие дистрибутивов и формуляров.

В формулярах зачастую присутствуют требования по использованию дополнительных средств доверенной загрузки, антивирусных и иных средств защиты информации, а также необходимость внесения изменений в реестр для корректной работы СКЗИ.

Сравнительный анализ результатов контроля за обеспечением безопасности персональных данных с использованием СКЗИ (в процентном соотношении)



- без нарушений или с незначительными отступлениями от требований нормативных документов, не повлекшими мер административного воздействия
- с нарушениями требований нормативных документов, повлекшими применение мер административного воздействия

Меры административного воздействия:

- предписание об устранении выявленных нарушений;
- протокол об административном правонарушении;
- представление об устранении причин и условий, способствующих реализации угроз безопасности Российской Федерации

Инцидент ИБ

- вирусы различных видов (трояны, шифровальщики и др.),
- отказы в санкционированном доступе,
- нерегламентированная самостоятельная активность информационной системы и др.

Цели реагирования на инцидент ИБ:

- минимизация ущерба,
- скорейшее восстановление исходного состояния информационной системы,
- документирование следов инцидента и его расследование,
- выработка мер по недопущению подобных инцидентов в будущем.

CERT@primorsky.ru

Информирование об инциденте ИБ

- предполагаемый начальный вектор атаки,
- предполагаемые вредоносные программы и инструменты, использовавшиеся в атаке,
- какие системы были затронуты атакой,
- первичная оценка ущерба,
- завершена ли атака, достигнута ли цель атаки,
- первичная оценка временных рамок атаки,
- иная значимая на Ваш взгляд информация,
- контактные данные для связи (обязательно)

Рекомендации по первичным действиям

- локализовать скомпрометированные компьютеры,
- сохранить следы атаки,
- снять образ диска.

Спасибо за внимание!