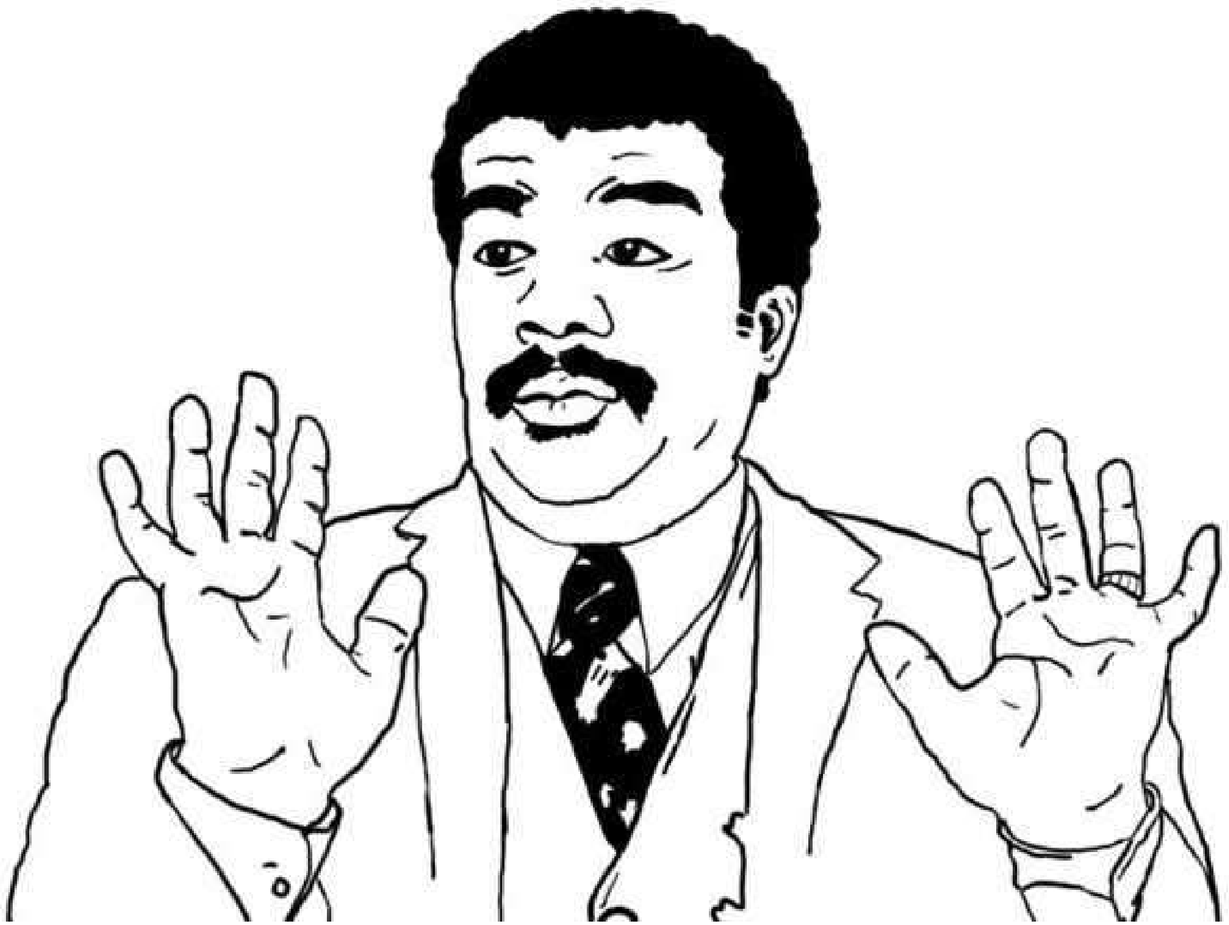
# Простыми словами о технических мерах защиты персональных данных

**Вероника Нечаева**
Директор по Информационной Безопасности
Команды CORTEL

# На кого распространяются требования по тех. мерам?

В соответствии ч.1. ст. 19 152-ФЗ Оператор ПДн обязан принимать или обеспечить принятие:

- Правовых мер защиты
- Организационных мер защиты
- Технических мер защиты



# Где конкретно про “технические меры” сз ПДн?

- **Постановление Правительства РФ от 01.11.2012 №1119**
  "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

- **Приказ ФСТЭК России от 18.02.2013 №21**
  "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

- **Приказ ФСБ России от 10.07.2014 №378**
  "Об утверждении Состава и содержания 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"

# Что такое СЗПДн?

Совокупность СЗИ и мер защиты ПДн предпринимаемых для обеспечения должного уровня защищенности ПДн, в т.ч. для нейтрализации угроз.

[Защита от воздействий злоумышленников]

Средства антивирусной защиты
Средства управления доступом пользователей
Средства регистраций событий безопасности
Средства обеспечения сетевой безопасности
Средства контроля и анализа защищенности

+

Организационные меры

Обеспечение выполнения требований регуляторов

# Требования к оценке угроз безопасности информации

- Проводится в целях определения угроз безопасности информации, реализация(возникновение) которых возможна в системах и сетях с заданной архитектурой и в условиях их функционирования – актуальных угроз безопасности информации.
- Должна носить систематический характер и осуществляться как на этапе создания систем и сетей, так и в ходе их эксплуатации, в том числе при развитии(модернизации) систем и сетей.
- На этапе создания систем и сетей проводится на основе их предполагаемых архитектуры и условий функционирования, определенных по результатам изучения и анализа исходных данных на них, при этом результаты оценки должны быть направлены на обоснование выбора организационных и технических мер по защите информации (обеспечению безопасности), а также на выбор средств защиты информации и их функциональных возможностей.
- Проводится с использованием экспертного метода (формируется экспертная группа).
- В ходе эксплуатации систем и сетей, в том числе при развитии(модернизации) систем и сетей, оценка угроз безопасности информации проводится для реальной архитектуры систем и сетей и условий их функционирования, полученных по результатам анализа исходных данных, инвентаризации информационных ресурсов, анализа уязвимостей и (или) тестирования на проникновение систем и сетей, а также иных методов исследований уровня защищенности систем и сетей и содержащейся в них информации, при этом результаты оценки должны быть направлены на оценку эффективности принятых технических мер, в том числе используемых средств защиты информации.
- Проводится подразделением по защите информации (отдельными специалистами, назначенными ответственными за обеспечение защиты) с участием подразделений или специалистов, ответственных за эксплуатацию систем и сетей (ИТ-специалистов, специалистов автоматизированных систем управления, специалистов связи и др.), основных (профильных) подразделений или с привлечением специалистов сторонних организаций.

# Типы актуальных угроз безопасности ПДн

**1** **Угрозы первого типа**

- связаны с наличием недокументированных возможностей в системном ПО, используемом в информационной системе.

**2** **Угрозы второго типа**

- связаны с наличием недокументированных возможностей в прикладном ПО, используемом в информационной системе.

**3** **Угрозы третьего типа**

- не связаны с наличием не документированных возможностей в системном и прикладномПО, используемом в информационной системе.

# Определение уровня защищённости персональных данных

| Тип ИСПДН | Категории субъектов | Количество субъектов | Тип актуальных угроз | | |
|---|---|---|---|---|---|
| | | | 1 тип | 2 тип | 3 тип |
| ИСПДн-С | Не сотрудников | Более 100 000 | УЗ 1 | УЗ 1 | УЗ 2 |
| | | Менее 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| | Сотрудников | Любое | УЗ 1 | УЗ 2 | УЗ 3 |
| ИСПДн-Б | Не сотрудников | Более 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| | | Менее 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| | Сотрудников | Любое | УЗ 1 | УЗ 2 | УЗ 3 |
| ИСПДн-И | Не сотрудников | Более 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| | | Менее 100 000 | УЗ 1 | УЗ 3 | УЗ 4 |
| | Сотрудников | Любое | УЗ 1 | УЗ 3 | УЗ 4 |
| ИСПДн-О | Не сотрудников | Более 100 000 | УЗ 2 | УЗ 2 | УЗ 4 |
| | | Менее 100 000 | УЗ 2 | УЗ 3 | УЗ 4 |
| | Сотрудников | Любое | УЗ 2 | УЗ 3 | УЗ 4 |

# Границы при оценке угроз в информационной инфраструктуре поставщика услуг

## Оператор

[on-premise]

### Инфраструктура оператора

- Приложения
- Данные
- Среда выполнения
- Связующее ПО
- Операционная система
- Платформа виртуализации
- Аппаратная платформа
- Система хранения данных
- Сетевая инфраструктура

[IAAS]

### Инфраструктура как услуга

- Приложения
- Данные
- Среда выполнения
- Связующее ПО
- Операционная система
- Платформа виртуализации
- Аппаратная платформа
- Система хранения данных
- Сетевая инфраструктура

## Поставщик услуг

[PAAS]

### Платформа как услуга

- Приложения
- Данные
- Среда выполнения
- Связующее ПО
- Операционная система
- Платформа виртуализации
- Аппаратная платформа
- Система хранения данных
- Сетевая инфраструктура

[SAAS]

### ПО как услуга

- Приложения
- Данные
- Среда выполнения
- Связующее ПО
- Операционная система
- Платформа виртуализации
- Аппаратная платформа
- Система хранения данных
- Сетевая инфраструктура

# Что делать?

## 1. Определить угрозы ПДн

Определяем ущерб, в случае реализации угрозы, выявляем нарушителей, делаем оценку угроз, анализ БДУ ФСТЭК России.

## 2. Определить меры защиты

Решаем с помощью чего будем закрывать актуальные угрозы и выполнять требования регуляторов.

## 3. Разработать документацию по реализации мер

Готовим перечень мер защиты или техническое задание на создание СЗПДн, Технический проект на создание СЗПДн, которые помогут понять что, куда установить и как настроить, чтобы нейтрализовать угрозы и выполнить требования регуляторов.

## 4. Реализовать меры защиты

Настраиваем встроенные механизмы защиты, реализуем внедрение, настройку СЗИ и ввод в эксплуатацию СЗПДн.

## 5. Контролировать

На протяжении всего жизненного цикла СЗПДн проверяем актуальность настроек СЗИ, угроз ПДн, корректируем меры и СЗПДн.

# 12 шагов к обеспечению безопасности ПДн

1. Уровень защищенности по ПП РФ 1119. Перечень мер из приказа ФСТЭК №21.
2. Определение базового набора мер.
3. Базовый набор мер для установленного УЗ.
4. Базовый набор мер. Структурно-функциональные характеристики. Используемые технологии. Особенности функционирования.
5. Адаптация базового набора мер (исключение неприменимых мер)
6. Адаптированный, базовый набор мер.
7. Адаптированный,базовый набор мер Невыбранные ранее меры из приказа ФСТЭК №21.
8. Уточнение адаптированного, базового набора мер.
9. Уточненный, адаптированный, базовый набор мер.
10. Уточненный, адаптированный, базовый набор мер. Меры, установленные иными нормативными правовыми актами.
11. Дополнение уточненного, адаптированного, базового набора мер.
12. Дополненный, уточненный, адаптированный, базовый набор мер.

# Реализация мер защиты каждого из УЗ ПДн

| Группа мер | Тип средства защиты | Примечание |
|---|---|---|
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | Средство защиты от несанкционированного доступа, механизмы защиты операционной системы | |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | Средство защиты от несанкционированного доступа, механизмы защиты операционной системы | Отдельные меры реализуются криптошлюзами |
| III. Ограничение программной среды (ОПС) | Средство защиты от несанкционированного доступа, механизмы защиты операционной системы | Большую часть группы составляют организационные меры |
| IV. Защита машинных носителей персональных данных (ЗНИ) | Средство защиты от несанкционированного доступа, механизмы защиты операционной системы | |
| V. Регистрация событий безопасности (РСБ) | Любое средство защиты | |
| VI. Антивирусная защита (АВЗ) | Антивирус | |
| VII. Обнаружение вторжений (СОВ) | Средво обнаружения вторжений (IDS/IPS) | |
| VIII. Контроль (анализ) защищенности персональных данных (АНЗ) | Средство анализа защищенности (выявления уязвиомстей) | |
| IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ) | Средство защиты от несанкционированного доступа, механизмы защиты операционной системы | |
| X. Обеспечение доступности персональных данных (ОДТ) | Средство защиты от несанкционированного доступа, механизмы защиты операционной системы | |
| XI. Защита среды виртуализации (ЗСВ) | Гипервизор, хостововая операционная система, средство защиты среды виртуализации | |
| XII. Защита технических средств (ЗТС) | Организационные меры защиты | |
| XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) | Средство защиты от несанкционированного доступа, механизмы защиты операционной системы | Отдельные меры реализуются криптошлюзами, межсетевыми экранами |
| XIV. Выявление инцидентов и реагирование на них (ИНЦ) | Организационные меры защиты | |
| XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ) | Организационные меры защиты | |

# Какие СЗИ применять?

**п.4 Приказ ФСТЭК России №21:**

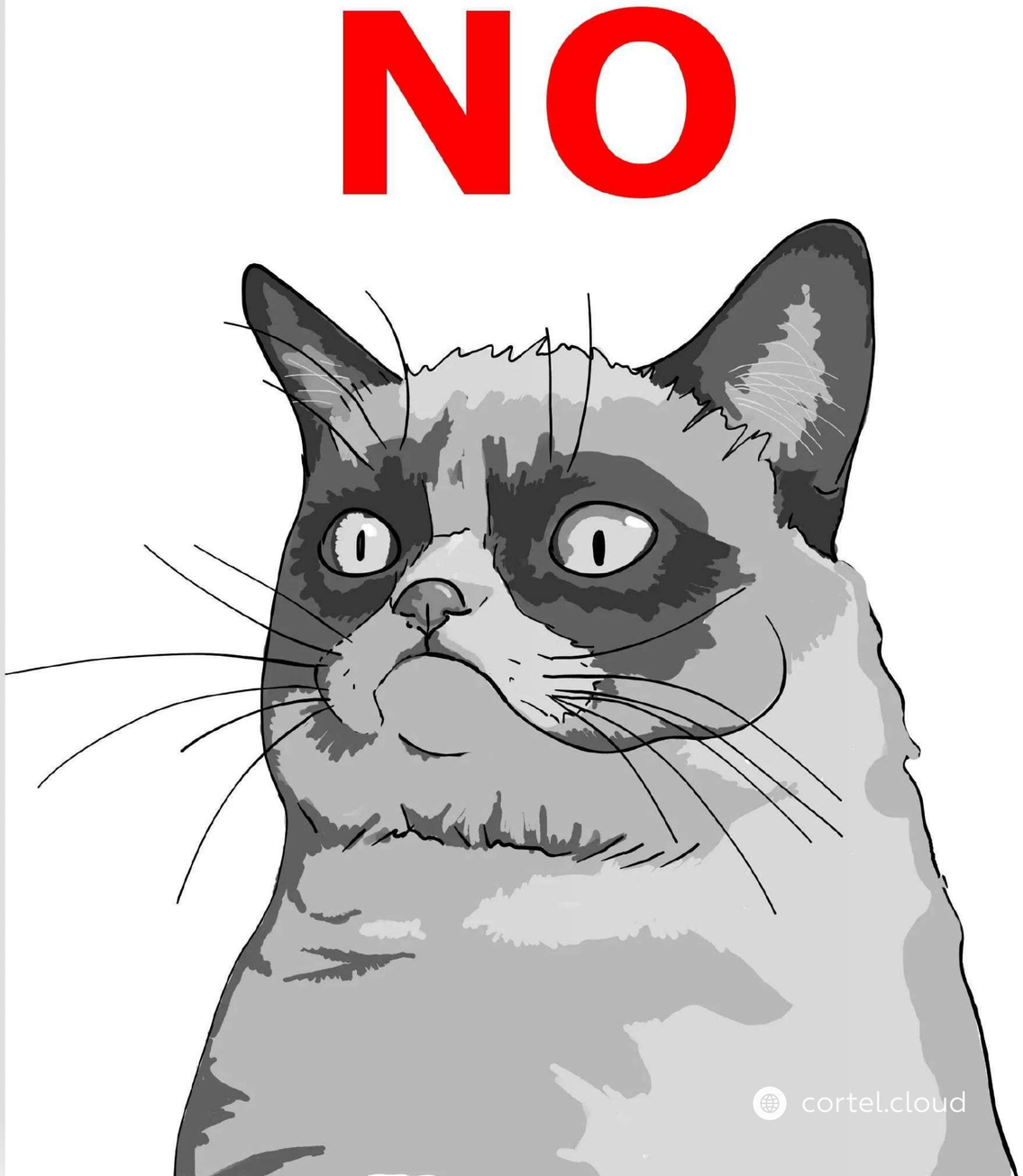
меры по обеспечению безопасности ПДн реализуются, в том числе, посредством применения в ИС СЗИ, прошедших, в установленном порядке, процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности ПДн.

**п.13ПП РФ №1119:**

Для обеспечения... уровня защищенности ПДн при их обработке в ИС необходимо выполнение следующих требований:...
г) использование СЗИ, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

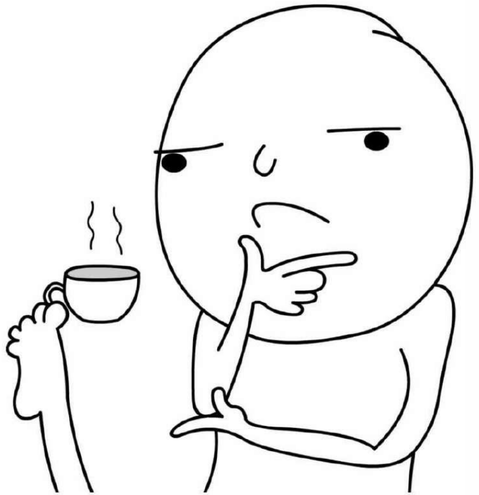
# СЗИ нужны только для выполнения требований регуляторов?

- Фиксация действий пользователей (определение инцидента или риска утечки ПДн, реагирование и пресечение утечек инцидентов)
- Снижение репутационных рисков (обоснование принятия мер защиты)
- Подтверждение надежности для взаимодействия с другими юр.лицами (в т.ч. при развитии бизнеса)



# Несертифицированные СЗИ

- Нужно показывать документы о проведении оценки, включая программу и методику.
- Обосновать применение СЗИ без сертификата.
- Актуальная техническая поддержка и обновление.



# Сертифицированные СЗИ

- Не нужно доказывать эффективность и функциональность.
- Есть сертификат и формуляр на соответствие определенному классу, уровню доверия.
- Закрывает требования регуляторов.

# А если часть СЗИ уже есть, но сертификата у них нет?

1

**Самостоятельная оценка**

Оператор может самостоятельно (без лицензиата ФСТЭК Росии)провести оценку соответствия.

2

**Программа и методика**

Разработать программу и методику испытаний, подобрать подходящий набор инструментов.

3

**Провести испытания**

Определить нейтрализует ли СЗИ угрозы и выполняет ли меры, закрывая требования.

4

**Заключение**

Оформление заключения о том, что СЗИ реализует весь функционал.

# Как выполнить требования?

CORTEL

Все записи

Рубрики

Поиск...

**Свежие записи**

Защита от кибератак финансового онлайн-сервиса

Импортозамещение виртуализации: платформа РУСТЭК

ТОП 5 книг о применении Lean и Agile в бизнесе

Двухскоростное ИТ: связь DevOps, Lean, ITIL и Agile в бизнесе

ТОП 10 мифов об облаках

**Рубрики**

Заметки директора по ИТ

Импортозамещение

Информационная безопасность

## Закон №152-ФЗ о персональных данных: новые требования

Владимир Путин подписал Федеральный закон от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности”.

Сами нововведения подробно описали в материале от 15 июля 2022.

8-800-775-9990

cortel.cloud

# Как подтвердить выполнение требований?

**Оценка эффективности**

Обязательна для всех Операторов ПДн.
Может проводиться самостоятельно.
Проводится на основании программы и методики испытаний(можно подсмотреть ГОСТы).
Не накладывает пространственных ограничений, кроме проведения не реже 1 раза в 2 года.

**Аттестация**

Добровольная для всех, кроме ГИС.
Проводится лицензиатом ФСТЭК России (органом по аттестации).
Регламентирована Приказом ФСТЭК России №77.
Подходит для фиксированного объекта информатизации, иначе обновление технического паспорта или повторная аттестация.

# Оценка эффективности применяемых мер защиты

В соответствии с пп.4 ст.19 152-ФЗ обеспечение безопасности персональных данных достигается, в том числе, оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн.

В соответствии с 21 приказом ФСТЭК оценка эффективности реализованных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе ЮЛ и ИП – лицензиатов ФСТЭК России. Указанная оценка проводится не реже одного раза в 3 года.

- Форма проведения оценки эффективности СЗПДн: приемо-сдаточные испытания, аттестация.
- По результатам оценки оформляется заключение. К заключению прилагаются протоколы оценки,подтверждающие полученные результаты и обосновывающие вывод.
- Порядок проведения аттестации регламентирован приказом ФСТЭК России от 29.04.2021 № 77 “Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну”.
- Аттестат соответствия выдаётся бессрочно, каждые 2 года ЮЛ обязано подтверждать факт проведённых периодических контролей аттестованных объектов информатизации (сохраняются требования по проведению ежегодного периодического контроля).

  Все аттестаты, выданные до 01.09.21, действуют согласно прежним нормам и имеют срок действия 3 года.

# Безопасность систем требует разделения ответственности между клиентом и облачным провайдером

| | Собственная инфраструктура | IaaS | PaaS | SaaS |
|---|---|---|---|---|
| Управление доступом к данным | ● | ● | ● | ● |
| Безопасность приложений | ● | ● | ● | ● |
| Безопасность ОС | ● | ● | ● | ● |
| Сетевая безопасность | ● | ● | ● | ● |
| Резервирование | ● | ● | ● | ● |
| Шифрование | ● | ● | ● | ● |
| Логи аудита | ● | ● | ● | ● |
| Безопасность хранилища данных и оборудования | ● | ● | ● | ● |
| Сетевая безопасность | ● | ● | ● | ● |
| Физическая безопасность и катастрофоустойчивость | ● | ● | ● | ● |

8-800-775-9990

# Все ЦОД предлагают по договору:

- Сбор и хранение информации
- Отказоустойчивость
- Резервирование
- Отказоустойчивость
- Возможность организации выделенных зон и обеспечение физической и IT-безопасности от общих внешних угроз.

## Важно!

Такой договор не позволит привлечь ЦОД к ответственности перед оператором в случае утечки ПДн.

152-ФЗ говорит об ином договоре – договоре об обработке и хранении ПДн.

Такой договор может быть заключен в виде договора оказания услуг или договора поручения.

**Лицо, осуществляющее обработку ПДн по поручению Оператора, обязано соблюдать принципы и правила обработки ПДн, предусмотренные 152-ФЗ.**

В поручении Оператора должны быть определены перечень действий с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со ст. 19 152-ФЗ (в ней приведены меры по обеспечению безопасности ПДн при их обработке)

**Важно!**
Согласно ч. 4 и 5 ст. 6 152-ФЗ лицо, осуществляющее обработку ПДн по поручению Оператора, не обязано получать согласие субъекта ПДн на обработку его ПДн.

- ЦОД должен обеспечить те же принципы, цели и порядок обработки ПДн, что и Оператор.
- Оператор должен получить согласие в письменной форме Субъекта ПДн на передачу ПДн третьему лицу с четко сформулированной целью.
- Только при включении указанных положений в договор с ЦОД возможна реализация положения 152-ФЗ об ответственности лица, осуществляющего обработку ПДн по поручению оператора.

# SAFE CLOUD
# 152 - ФЗ

Готовый сервис для выполнения ФЗ-152 на аттестованной защищённой облачной инфраструктуре с лучшей стоимостью.

CORTEL 2024 г.

# ОДНО РЕШЕНИЕ ДЛЯ ВСЕХ ЗАДАЧ

Мы исследовали и проанализировали лучшие практики для 152-ФЗ и разработали сервис, который обеспечивает решение самых сложных задач в работе с персональными данными.

Учли опыт отрасли и уделили особое внимание компонентам, которые не представлены на рынке имеющихся решений.

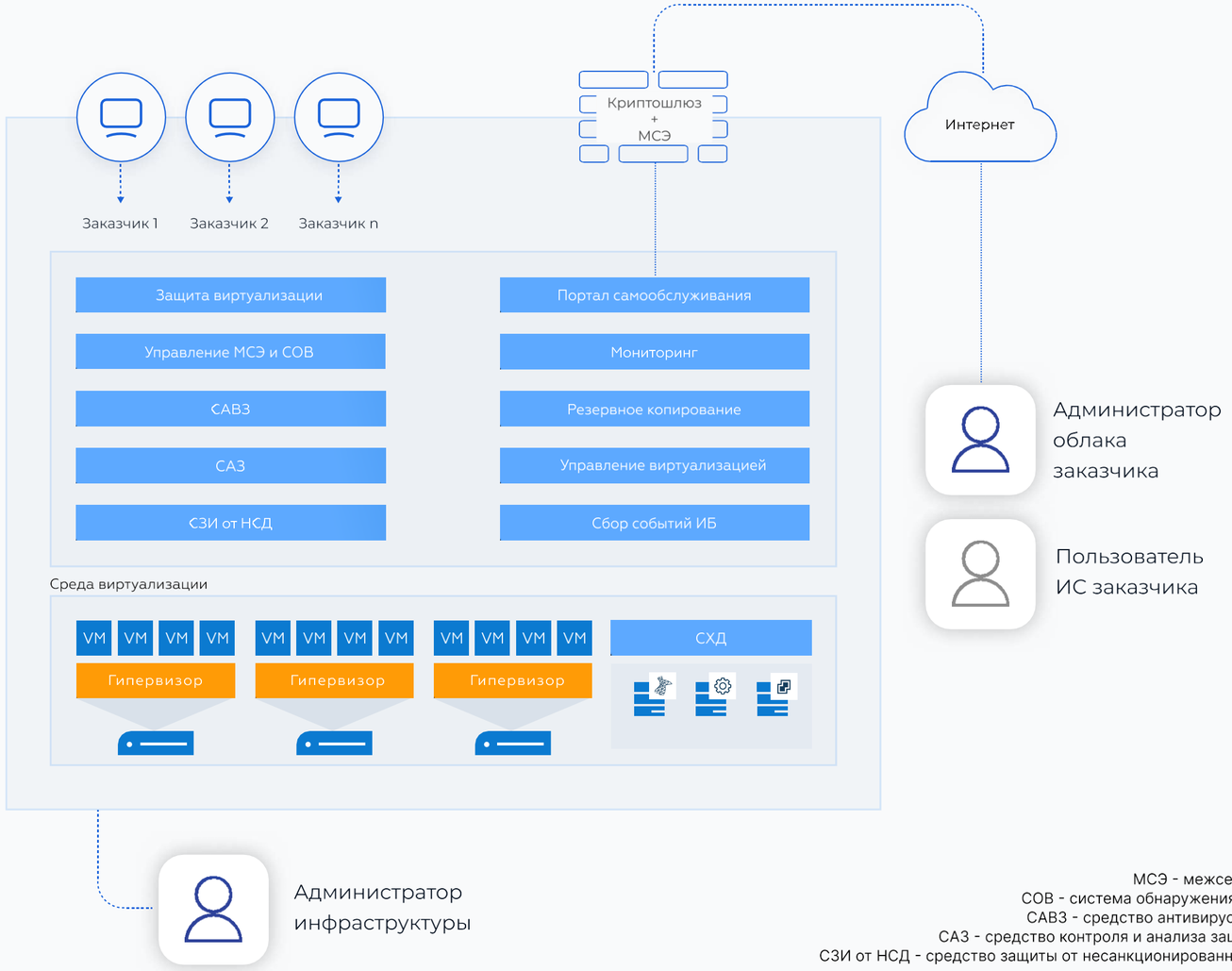
1. Пакет документов для выполнения 152-ФЗ
2. Технические меры защиты уже в Safe Cloud
3. Делигирование ответственности за утечку ПДн в CORTEL
4. Прямой доступ к экспертам
5. Легкая бесшовная миграция

# SafeCloud 152

**Все меры защиты** уже
в готовом удобном сервисе.

Защищенный сегмент CORTEL сразу подходит для информационных систем с ПДН, требующих 2 уровня защищенности и класса защищенности 2, включая размещение:

- медицинской тайны;
- специальных категорий ПДН;
- данных несовершеннолетних;
- биометрических данных.




МСЭ - межсетевой экран
СОВ - система обнаружения вторжений
САВЗ - средство антивирусной защиты
САЗ - средство контроля и анализа защищенности
СЗИ от НСД - средство защиты от несанкционированного доступа

CORTEL

# ГАРАНТИИ

### Соответствие ФЗ

ИТ инфраструктура аттестована по 17 и 21 приказам ФСТЭК. Реализованы меры защиты до уровня защищенности 2 и класса защищенности 2.

### Делегирование ответственности

Ответственность за обработку ПДн делегируется в рамках договора CORTEL.

99,95%

### Доступность сервиса

Safe Cloud 152 может быть недоступен не более 5 часов в год.

Договор SLA даёт финансовые гарантии.

### Экспертиза

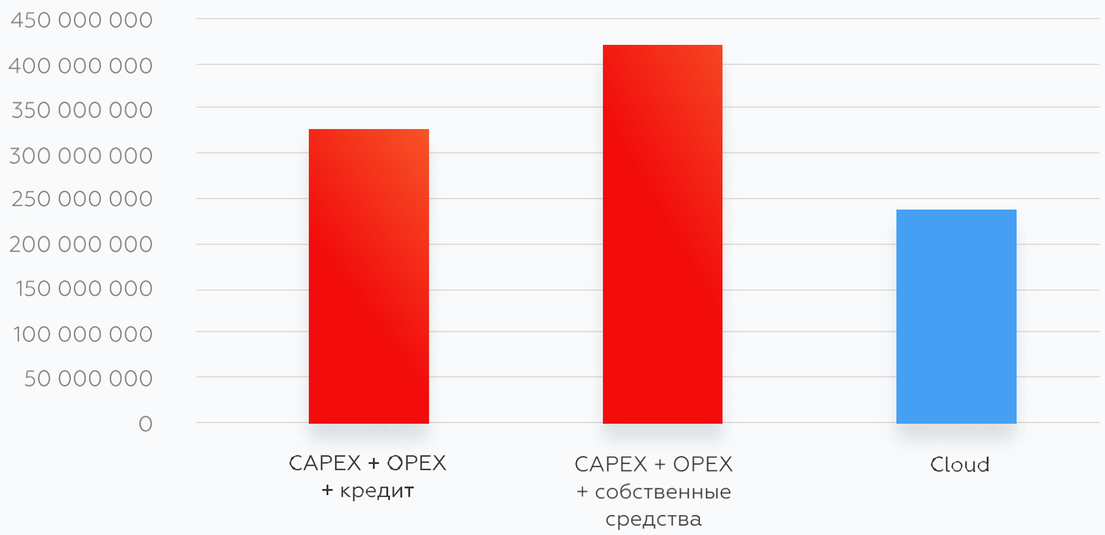
Экспертные рекомендации в части организации мер защиты, круглосуточное обслуживание и техническая поддержка 24/7/365.

# Документация

**Весь пакет документов*** для выполнения требований регуляторов со стороны облака уже входит в сервис и не требует дополнительной оплаты.

* CORTEL не оказывает услуги по подготовке документации без предоставления ИТ инфраструктуры

# ГАРАНТИРУЕМ ЛУЧШУЮ СТОИМОСТЬ ВЛАДЕНИЯ




| | |
|---|---|
| CAPEX | 189 299646,0 |
| OPEX | 84 758 352,0 |
| Стоимость % по кредиту | 52 023 836,54 |
| Стоимость собственных средств | 144 311 010,76 |

| | |
|---|---|
| **CAPEX + OPEX + кредит** | 326 081 835 |
| **CAPEX + OPEX + собственные средства** | 418 369 009 |
| **Cloud** | **238 794 737** |

| **Период амортизируемой эксплуатации мес.** | **60 мес** |
|---|---|
| Стоимость упущенной выгоды % (Расчитывается как годовая EBITDA в % 1 руб выручки) | 12,00% |
| Обслуживание заемных средств % | 10,00% |

**Косвенные затраты:**

1. Управление персоналом
2. Учёт ТМЦ ( бухгалтерия + склад)
3. Закупка (закупка + логистика)

**Риски:**

1. Риски потери оборудования
2. Моральное устаревание оборудования

# Техподдержка, которой не всё равно

За 7 лет работы мы научились строить системы поддержки так, чтобы клиенты решали задачи быстрее. Поэтому и для Safe Cloud 152 мы организовали отзывчивую техподдержку системы защиты информации и инфраструктуры:

- 24/7/365 на короткой связи
- время реагирования до 20 мин

# О КОМПАНИИ

CORTEL - эксперты в управлении и сопровождении высоконагруженных ИТ-инфраструктур с 2015 г.

Мы исследуем и анализируем информационные системы для подготовки каждого индивидуального решения.

Многие годы используем только лучшие проверенные технологии и практики, благодаря которым клиенты решили свои самые сложные технологические задачи.

**9**
лет компании

**100+**
проектов в России

**121**
эксперт

# СРЕДИ НАШИХ КЛИЕНТОВ:

СОВКОМБАНК

АТОМЭНЕРГОСБЫТ РОСАТОМ

Слата

vsemayki.ru

БАНК АКЦЕПТ

РОССЕТИ СИБИРЬ

КрасныйЯр

РОССЕТИ ТЮМЕНЬ

TION.

Angioline interventional device

КОМАНДОР

Новосибирскэнергосбыт
Наполняя жизнь энергией

Центральный офис нашей компании расположен в **Новосибирске.**
Офис также открыт в **Барнауле.**

## Контакты

8 (800) 775 99 90
sales@cortel.cloud

[ЦЕНТРАЛЬНЫЙ ОФИС]

**Новосибирск, Орджоникидзе 38,**
**БЦ Партнёр, 2 этаж.**

# Если вы заинтересовались или у вас остались вопросы, вот мои контакты:

**Вероника Нечаева**
CISO CORTEL
DPO, серт-й аудитор ЦБ РФ

Тел.: +7 905 925 45 68
e-mail: nvv@cortel-cloud.ru

CORTEL