CORTEL

Выполнение требований ФЗ без санкций регуляторов и закупок оборудования

Вероника Нечаева
Директор по Информационной Безопасности
Команды CORTEL

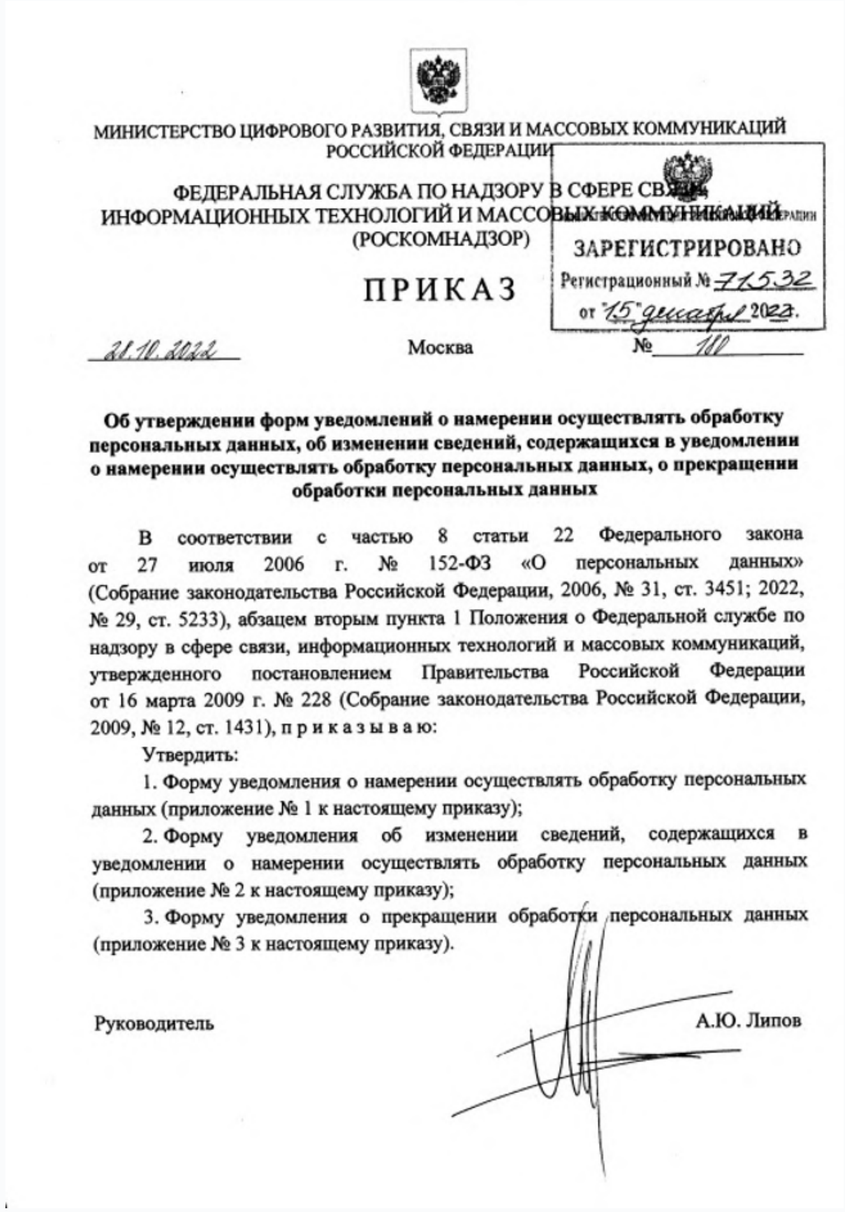
Что нового?

Федеральным законом 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»,
внесен ряд изменений в Федеральный закон от 27.07.2006 **№ 152-ФЗ** «О персональных данных».
Последние **поправки вступили в силу 1 марта 2023 г.**

Уведомление Роскомнадзора: право или обязанность.

Приказом Роскомнадзора от 28.10.2022 № 180 утверждены формы уведомлений:

- о намерении осуществлять обработку персональных данных;
- об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных;
- о прекращении обработки персональных данных.



МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ (РОСКОМНАДЗОР)

ЗАРЕГИСТРИРОВАНО
Регистрационный № 71532
от 15 декабря 2022.

ПРИКАЗ

28.10.2022 Москва № 180

Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных

В соответствии с частью 8 статьи 22 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2022, № 29, ст. 5233), абзацем вторым пункта 1 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденного постановлением Правительства Российской Федерации от 16 марта 2009 г. № 228 (Собрание законодательства Российской Федерации, 2009, № 12, ст. 1431), п р и к а з ы в а ю:

Утвердить:

1. Форму уведомления о намерении осуществлять обработку персональных данных (приложение № 1 к настоящему приказу);

2. Форму уведомления об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных (приложение № 2 к настоящему приказу);

3. Форму уведомления о прекращении обработки персональных данных (приложение № 3 к настоящему приказу).

Руководитель А.Ю. Липов

Коротко про изменения по уведомлению:

- **Если уведомление подано до вступления в силу изменений**, то есть, до 1 сентября 2022 года, необходимо переподать уведомление о внесение изменений в ранее поданное Уведомление в порядке и форме, установленных новым Приказом РКН (даже если нет изменений в текущей деятельности).
- **Нет жестких сроков** переподачи Уведомления в новой форме.
- **По обработке ПДн в ГИС**, Уведомление подавать должен государственный орган – владелец ГИС.
- **Нет разграничения** между оператором и обработчиком в российском законодательстве , поэтому обработчики по ч. 3 ст. 6 152-ФЗ тоже должны подавать Уведомления.
- **Самозанятые**, нотариусы, адвокаты тоже должны подавать Уведомления.
- **Когда работников в организации нет**, уведомление нужно подавать, если деятельность предполагает обработку ПДн и организация не попадает под исключение.
- **Если ранее деятельность попадала под исключения**, а теперь – нет (например, если обработка осуществляется только в отношении обработки ПДн работников), уведомление нужно подавать, .
- **Если во внутренних приказах** организации цели обработки указаны конкретно, в Уведомлении также указываются более конкретные цели, они должны соответствовать (на портале РКН – через поле «иное»).
- **Если ЦОД арендуется** и не принадлежит Оператору, в Уведомлении указывается адрес ЦОДа.
- Исключения, когда уведомление в РКН можно не подавать, содержатся во втором пункте статьи 22 закона 152-ФЗ.

Что такое трансграничная передача?

Трансграничная передача персональных данных (ТППД) — это передача личной информации гражданина на территорию иностранного государства органу власти иностранного государства, иностранному юрлицу или физлицу (ст. 3 152-ФЗ).

№ 152-ФЗ делит все иностранные государства на две категории

Страны, обеспечивающие адекватную защиту прав субъектов ПДн («адекватные страны»).

К ним относятся стороны Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и прочие государства, входящие в утвержденный Роскомнадзором список (Конвенция от 28.01.81; приказ Роскомнадзора от 05.08.2022 № 128 — действует с 1 марта 2023 года; приказ Роскомнадзора от 15.03.2013 № 274 — действует до 1.03.2023 года). Например, это Грузия, Азербайджан, Турция, Казахстан, Беларусь, КНР.

Страны, не обеспечивающие адекватную защиту прав субъекта ПДн («неадекватные страны»).

К ним относятся все государства, которых нет в перечисленных выше списках Роскомнадзора. Например, ЦАР.

** до 1 марта 2023 года в «адекватные страны» можно свободно передавать ПДн, при условии соблюдения № 152-ФЗ.*
Но субъект персональных данных имеет право знать, что оператор поручает кому-то обработку его личной информации (п. 8 ч. 7 ст. 14 Закона № 152-ФЗ).

Трансграничная передача в «неадекватные страны» возможна только при выполнении одного из условий:

- С письменного согласия субъекта ПДн
- В случаях, предусмотренных международными договорами Российской Федерации
- Для исполнения условий договора с субъектом ПДн
- Для защиты жизни, здоровья, интересов самого гражданина и других лиц, когда невозможно получить письменное согласие на ТППД.
- Если это необходимо по закону для обеспечения конституционного строя, обороны и безопасности страны, транспортной защиты

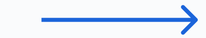
Коротко по теме ТГП:

- Трансграничная передача может быть включена в любое согласие, если указанная в нем цель предусматривает такую трансграничную передачу.
- Уведомление по ст. 6 266-ФЗ не предусматривало возможность запрета / ограничения, с 1 марта подается уведомление по ст. 12 152-ФЗ, РКН может наложить запреты / ограничения такой передачи.
- Если после 1 марта 2023 года никаких изменений не происходит (в части целей, объема ПДн, перечня стран), дополнительное уведомление не подается, но в случае изменений подается уведомление по ст. 12 152-ФЗ в изменившейся части, а не полностью заново.
- Уведомление о ТГП не заменяет правовые основания для ТГП, то есть, независимо от подачи уведомления, необходимо обеспечить правомерность (взять согласие и т. д.)
- Информация о запретах / ограничениях будет направлена на e-mail, указанный в уведомлении, а также указана на сайте РКН в разделе «статус уведомления» (доступен по ключу).
- Если уведомление не было подано до 1 марта 2023 года, но ТГП есть, надо подавать уведомление по ст. 12 152-ФЗ, возможны запреты / ограничения, если деятельность не попадает под исключения.
- Если уведомление по ст. 6 266-ФЗ подано на бумажном носителе, ориентироваться РКН будет на почтовый штемпель, уведомления, de facto отправленные до 1 марта 2023 года, будут приняты.

К имевшимся требованиям, предъявляемым к поручению, законодатель добавил следующие:

- Перечень персональных данных.
- Требования по локализации.
- Соблюдение положений ст. 18.1 закона о персональных данных.
- Необходимость обработчика уведомлять оператора о произошедших утечках.
- Предоставление по запросу заказчика сведений и документов по выполнению поручения.
- Перечень персональных данных.
- Требования по локализации.
- Соблюдение положений ст. 18.1 закона о персональных данных.
- Необходимость обработчика уведомлять оператора о произошедших утечках.
- Предоставление по запросу заказчика сведений и документов по выполнению поручения.

- Перечень персональных данных.
- Требования по локализации.
- Соблюдение положений ст. 18.1 закона о персональных данных.
- Необходимость обработчика уведомлять оператора о произошедших утечках.
- Предоставление по запросу заказчика сведений и документов по выполнению поручения.

Что нужно сделать 

В реестр третьих лиц, которым поручается обработка персональных данных, внести информацию по каждому поставщику услуг:

- Наименование, адрес и контакты
- Цели обработки ПДн
- Категории субъектов, данные которых передаются
- Действия с данными в каждой цели
- Сроки или условия прекращения обработки в каждой цели
- Способ передачи персональных данных
- Способ передачи персональных данных
- Описание процессов и ИСПДн, посредством которых передаются данные
- Проверить, уведомлен ли обработчик о сроках и реализации права физического лица по запросу оператора

- Внести в шаблон требования о соблюдения обработчиком положения п. 5 ст. 18.1 закона о персональных данных
- Включить в шаблон пункт о подтверждении обработчиком данных с предоставлением соответствующего акта об уничтожении
- Проверить наличие актуальных требований о сроках уничтожения данных (лучше установить за девять рабочих дней, чтобы уложиться в срок предоставления ответа заявителю).
- Подробно и последовательно расписать процесс проверки обработчиком требований поручения.
- Обязательно внести сведения об уведомлении об инциденте в срок не более 12 часов.

Из последних разъяснений РКН по Поручению обработки ПДн

1

Обработчик может привлекать суб-обработчика, если это предусмотрено поручением оператора, иначе нельзя.

2

Множественность на стороне обработчиков в договоре не допускается, один обработчик – одно поручение (термины в ч. 3 ст. 6 152-ФЗ – единственном числе), а в согласии указать несколько обработчиков можно (если совпадают все атрибуты поручаемой обработки ПДн).

3

Если сайт компании хостится на мощностях другой компании, это является поручением обработки ПДн, как и хранение данных в облаке.

Типовые ошибки при обработке ПДн в сети интернет

- Документ, определяющий политику ПДн отсутствует или размещен не на всех страницах сайта, на которых осуществляется сбор ПДн
- Размещена ссылка или другой документ, не имеющий отношения к политике в отношении обработки ПДн
- Размещена политика в отношении обработки ПДн другой организации (оператора)
- В документе отсутствуют обязательные сведения, предусмотренные п. 2 ч. 1 ст. 18.1 Федерального закона «О персональных данных», или указанные сведения не соответствуют фактической деятельности оператора
- Полное дублирование положений Федерального закона «О персональных данных», а не отражение сведений, соответствующих фактической обработке ПДн

при использовании на сайте метрических программ

- проинформировать об этом пользователей при входе на сайт и получить согласие на обработку пдн, собираемых посредством метрических программ
- указать какие именно метрические программы используются
- включить в политику в отношении обработки пдн информацию об использовании метрических программ

ОСНОВНЫЕ НАРУШЕНИЯ, ВЫЯВЛЕННЫЕ В ХОДЕ ПРОВЕРОК РКН

- Организация отсутствует в реестре РКН
- Сбор данных без согласия субъекта ПдН
- Отсутствие актуальной Политики по обработке Персональных данных
- Сбор избыточных ПДн (например данные, которые не требуются для работы с физическим лицом)
- Трансграничная передача данных

ДАННЫЕ
В ОТКРЫТОМ ДОСТУПЕ
НА САЙТЕ
РОСКОМНАДЗОРА

Административная ответственность

КоАП РФ	Событие правонарушения	Штраф
Ч.1 ст. 13.11 КоАП РФ	Обработка ПДн в случаях, не предусмотренных законодательством РФ в области ПДн, либо обработка ПДн, несовместимая с целями их сбора	на дл. лиц - от 10 тыс. до 20 тыс. руб. на юр. лиц - от 60 тыс. до 100 тыс. руб.
Ч. 2 ст. 13.11 КоАП РФ	Обработка ПДн без согласия в письменной форме субъекта ПДн на обработку его ПДн в случаях, когда такое согласие должно быть получено в соответствии с законодательством РФ в области ПДн, , либо обработка ПДн с нарушением установленных законодательством РФ в области ПДн требований к составу сведений, включаемых в согласие в письменной форме субъекта ПДн на обработку его ПДн	на дл. лиц - от 20 тыс. до 40 тыс. руб. на юр. лиц - от 30 тыс. до 150 тыс. руб.
Ч.3 ст. 13.11 КоАП РФ	Невыполнение оператором предусмотренной законодательством РФ в области ПДн обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки ПДн, или сведениям о реализуемых требованиях к защите ПДн	на дл. лиц - от 6 тыс. до 12 тыс. руб. на ИП - от 10 тыс. до 20 тыс. руб. на юр. лиц - от 30 тыс. до 60 тыс. руб.
Ч.4 ст. 13.11 КоАП РФ	Невыполнение оператором предусмотренной законодательством РФ в области ПДн обязанности по предоставлению субъекту ПДн информации, касающейся обработки его ПДн	на дл. лиц - от 8 до 12 тыс. руб. на ИП от 20 до 30 тыс. руб. на юр. лиц - от 40 до 80 тыс. руб.
Ч.5 ст. 13.11 КоАП РФ	Невыполнение оператором в сроки, установленные законодательством РФ в области ПДн, требования субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн об уточнении ПДн, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки	на дл. лиц - от 8 до 20 тыс. руб. на ИП - от 20 до 40 тыс. руб. на юр. лиц - от 50 до 90 тыс. руб.
Ч.6 ст. 13.11 КоАП РФ	Невыполнение оператором при обработке ПДн без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством РФ в области ПДн сохранность ПДн при хранении материальных носителей ПДн и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении ПДн, при отсутствии признаков уголовно наказуемого деяния	на дл. лиц - от 8 до 20 тыс. руб. на ИП от 20 до 40 тыс. руб. на юр. лиц - от 50 до 100 тыс. руб.
Ч.7 ст. 13.11 КоАП РФ	Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством РФ в области ПДн обязанности по обезличиванию ПДн либо несоблюдение установленных требований или методов по обезличиванию ПДн	на дл. лиц от 6 до 12 тыс. руб.
Ч.8 ст. 13.11 КоАП РФ	Невыполнение оператором при сборе ПДн, в том числе посредством информационно-телекоммуникационной сети "Интернет", предусмотренной законодательством РФ в области ПДн обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения ПДн граждан РФ с использованием баз данных, находящихся на территории РФ	на дл. лиц - от 100 тыс. до 200 тыс.руб. на юр. лиц - от 1 млн. до 6 млн. руб.

ПРАВИТЕЛЬСТВО ОДОБРИЛО ПРОЕКТ ЗАКОНА

от 3 до 5 млн руб. штраф для юрлиц за утечку от 1 до 10 тыс. записей персональных данных.
от 5 до 10 млн руб. за утечку от 10 до 100 тыс. записей
от 10 до 15 млн руб. за утечку более 100 тыс. записей

Оборотные штрафы вводятся за повторное нарушение.
В зависимости от масштаба:
от 0,1% совокупной выручки за предыдущий год
до 3%, но не менее 15 млн и не более 500млн руб.

Со всеми штрафами в области невыполнения требований законодательства или нарушений в обработке ПДн вы можете ознакомиться в закрытом Telegram-канале, все полезные материалы уже там.

8-800-775-9990
cortel.cloud

Рекомендуемые подходы к обработке ПДн

- Хранение идентификаторов, указывающих на человека (ФИО, e-mail, телефон, адрес) и данные о взаимодействии с ним (оказанные услуги, проданные товары, переписка, договора и т. д.) в разных, не связанных друг с другом непосредственно, базах данных. Использование для указанных баз синтетических идентификаторов, не позволяющих без дополнительной информации и алгоритмов отнести информацию в этих базах к конкретному субъекту персональных данных, и хранение таких идентификаторов отдельно от предыдущих двух баз
- Использование технических и программных средств, принадлежащих оператору, для обеспечения необходимого уровня безопасности данных. Поручение обработки данных третьим лицам не снимает с оператора ответственности, но снижает контроль со стороны оператора за принимаемыми мерами безопасности
- Отказ от практики накопления ПДн «на всякий случай», от формирования профилей клиента, если это не жизненно нужно для организации. Своевременное уничтожение ПДн при достижении цели их обработки (например, после оказания услуги)
- Минимизация перечня собираемых и обрабатываемых ПДн. Использование лишь тех данных, которые действительно необходимы для оказания услуг, продажи товаров и иной деятельности организации
- Обеспечение раздельного хранения ПДн различных категорий субъектов (клиенты, работники, соискатели и т. д.), в том числе несовместимых между собой по целям обработки
- Своевременное информирование Роскомнадзора о признаках и (или) наступивших инцидентах, повлекших (возможно повлекших) распространение ПДн субъектов
- Принятие мер физического контроля доступа к данным во избежание компрометации данных внутренними нарушителями.
- Назначение ответственного за защиту персональных данных, наделение его необходимыми полномочиями

ПРОБЛЕМА

Штрафы и ответственность

Регуляторы применяют штрафы и санкции, вплоть до уголовной ответственности за невыполнение организационных и технических мер защиты данных и отсутствие аттестации.

Импортозамещение

Западное ПО и оборудование запрещены к использованию, а отечественные решения им существенно уступают.

Стоимость решения

Высокая стоимость самостоятельного построения защищенной импортозамещённой инфраструктуры.

Компетенции

Нехватка экспертизы для гарантированного сокращения рисков получения штрафа и уголовной ответственности.

Как выполнить требования?

8-800-775-9990

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
- ИТ на бизнес-языке
- Кейсы CORTEL
- Экономика ИТ

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.

Законом вводится обязанность операторов персональных данных незамедлительно информировать об инцидентах с принадлежащими им базами ПДн в контролирующие органы.

cortel.cloud

SAFE CLOUD

Готовый сервис, реализующий требования безопасности для защиты и размещения ГИС, ИСПДН и КИИ.

CORTEL 2023 г.

ОДНО РЕШЕНИЕ
ДЛЯ ВСЕХ ЗАДАЧ

Мы исследовали и проанализировали лучшие практики для защиты ГИС, ИСПДН и КИИ и разработали сервис, который обеспечивает решение самых сложных задач в работе с чувствительными данными.

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

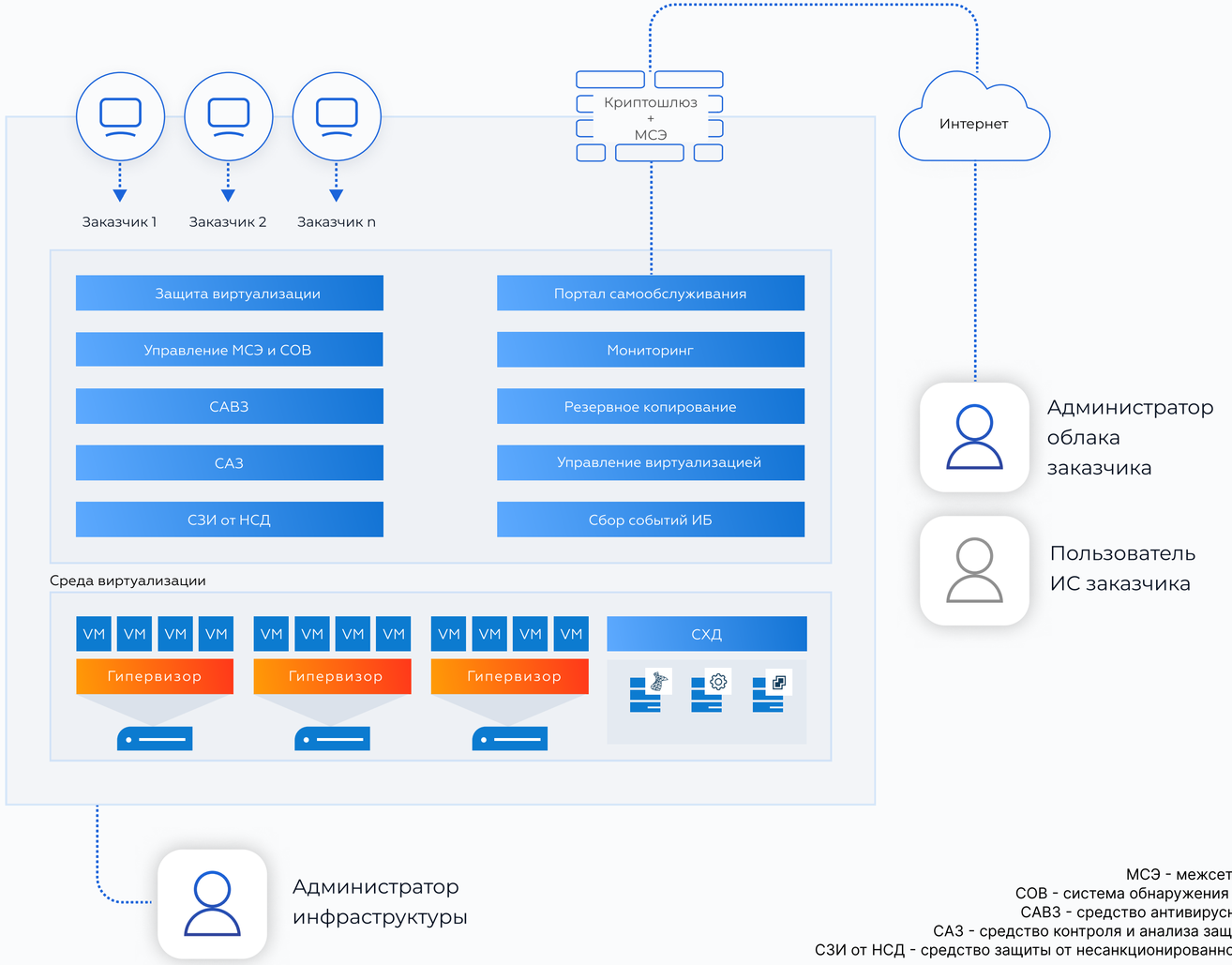
1. Организационные и технические меры защиты ГИС, ИСПДН и КИИ уже применены в решении
2. Сервис уже готов к работе в облаке и не требует процедур закупок
3. Делегирование ответственности за утечку чувствительных данных в CORTEL
4. Экспертная команда в вашем распоряжении предоставляет непрерывный сервис под строгий SLA
5. Легкая бесшовная миграция
6. Есть возможность построения частной закрытой защищённой инфраструктуры на вашем оборудовании
7. Гарантируем самую низкую полную стоимость владения с гибкой системой оплат
8. Регистрация всех событий безопасности

SafeCloud

Все меры защиты уже
в готовом удобном сервисе.

Защищенный сегмент CORTEL сразу подходит для размещения ПДН, требующих 2 уровня защищенности и ГИС класса защищенности 2, включая размещение:

- медицинской тайны;
- специальных категорий ПДН;
- чувствительных данных;
- данных КИИ;
- биометрических данных.



МСЭ - межсетевой экран
СОВ - система обнаружения вторжений
САВЗ - средство антивирусной защиты
СА3 - средство контроля и анализа защищенности
СЗИ от НСД - средство защиты от несанкционированного доступа

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 защиту чувствительных данных делегируется в рамках договора CORTEL.

99,95%

Доступность сервиса

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

Договор SLA даёт финансовые гарантии.

Экспертиза

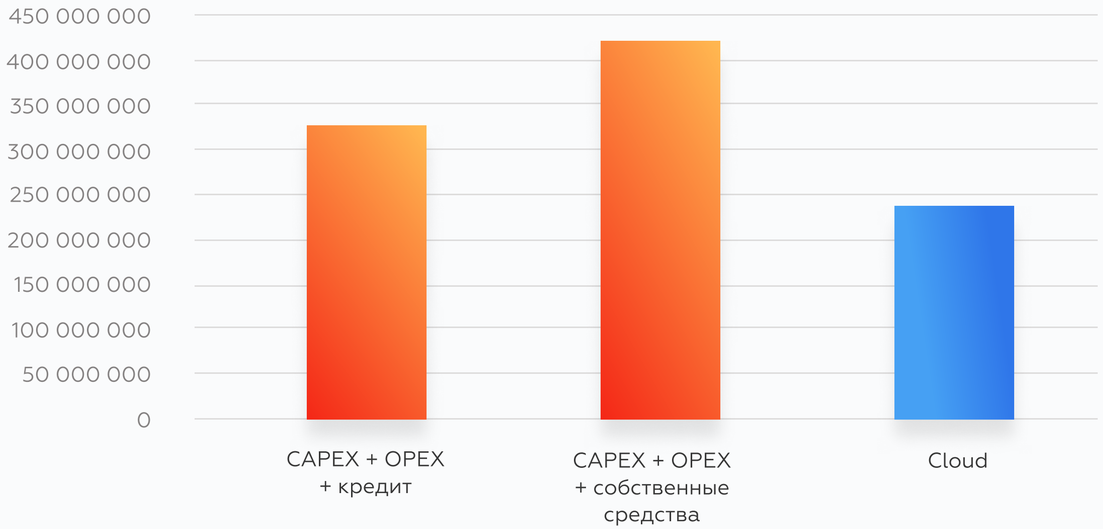
Экспертные рекомендации в части организации мер защиты, круглосуточное обслуживание и техническая поддержка 24/7/365.

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:

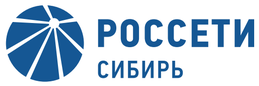
1. Риски потери оборудования
2. Моральное устаревание оборудования

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 мы организовали отзывчивую техподдержку системы защиты информации и инфраструктуры:

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

СРЕДИ НАШИХ КЛИЕНТОВ:



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