

15 октября 2025



вебинар

Что делать?

Проверки

Как адаптироваться?

152-ФЗ

ПДн

Ответственность за персональные данные в 2025: реалии операторов

Опыт команды ИБ

Опыт работы:

- Органы аттестации
- Лицензиаты ФСТЭК/ФСБ
- Компании-интеграторы
- Региональные органы власти

Участвовала в проектах по:

Аудиту, построению и сопровождению системы защиты информации: Севэнергосбыт (ИСПДн, КИИ), Барнаулэнерго (КИИ), Алтайэнерго (КИИ), комитетах жилищно-коммунального хозяйства (ПДн, ГИС), Министерствах жилищно-коммунального хозяйства (ПДн, ГИС, КИИ), водоканалы (КИИ), ТОСы/УК/ТСЖ (ПДн)

- Белокурихинской ГЭС
- Барнаулэнерго
- Севастопольского морского порта
- Министерства здравоохранения Республики Алтай



CISO CORTEL

Вероника Нечаева

- Член ассоциации руководителей служб ИБ
- Сертифицированный аудитор ЦБ РФ
- Эксперт в области защиты ПДн, ГИС, КИИ
- Data Protection Officer



Проверки Роскомнадзора

В марте 2022 года Правительством РФ был введен мораторий на плановые проверки операторов персональных данных

И теперь подавляющая часть операторов ПДн до 2030 года не столкнутся с плановыми проверками.

Но вот уже несколько лет РКН проводит контрольные мероприятия без взаимодействия с контролируемым лицом в рамках которых проверяет сайты и мобильные приложения операторов.

Дистанционные проверки Роскомнадзора

Особый вид работы РКН - проведение контрольных мероприятий без взаимодействия: они могут коснуться всех, у кого есть сайты.

В рамках контрольных мероприятий без взаимодействия проверяют:

- ✓ локализацию баз данных, где хранятся данные, собранные с помощью сервисов сайта. Сервера, хранящие сведения о россиянах (в том числе данные, собираемые метрическими программами), должны находиться в РФ;
- ✓ размещение политики обработки персональных данных на сайте;
- ✓ наличие правовых оснований обработки ПД (пользовательское соглашение/договор оферты, согласие на обработку ПД и т.д.);
- ✓ соответствие объема обрабатываемых ПД целям обработки (не нужно собирать фамилию и отчество, если нужно связаться по заявке).



Если РКН выявил нарушения, то он отправляет письмо с перечнем нарушений и требованием дать информацию о соблюдении закона. Такие проверки выполняются с помощью автоматизированных алгоритмов, без участия человека.

Какие нарушения можно найти?

 ч.10 ст.13.11, ст. 19.7. КоАП РФ

отсутствие уведомления
об обработке ПДн.

 ч. 1, ч.1.1. ст.13.11 КоАП РФ

отсутствие согласий под формами
сбора ПДн.

 ч.2., ч.2.1. ст.13.11 КоАП РФ

сбор специальных категорий ПДн, в
отсутствие иных оснований, через сайт,
мессенджер, социальные сети.

 ч.3. ст.13.11. КоАП РФ

неопубликование Политики по
обработке ПДн на сайте

 ч.8., ч.9. ст.13.11 КоАП РФ

иностранный хостинг сайта,
использование Google Forms

Как выявляют нарушения?

 п. 10 ПП РФ №336 от 10.03.23г., пп.58-60 ПП РФ №1046 от 29.06.2023г.

Мероприятия по контролю без взаимодействия с контролируруемыми лицами не требует согласования с органами прокуратуры и без уведомления оператора проводятся в целях предупреждения, выявления, прогнозирования и пресечения нарушений требований 152-ФЗ



По итогам проведения проверки территориальное управление РКН публикует на своем сайте отчет, в котором фиксирует выявленные нарушения (с наименованием операторов, в отношении которых проводились мероприятия) и результаты устранения/неустранения нарушений операторами.

Основные нарушения, выявленные в ходе мероприятий

- 1 Хостинг сайта
(проверяется с использованием сервисов Whois)
- 2 Сбор cookie и использование сервисов веб-аналитики
(Яндекс.Метрика/Google.Analytics)
- 3 Политика обработки ПДн
- 4 Формы сбора ПДн на сайте



Хостинг сайта и веб-аналитика на сайте

Размещение сайта на иностранном хостинге может привести к нарушениям требований о локализации.

 ч.8., ч.9. ст.13.11 КоАП РФ: от 1 до 6 млн.руб. за первичное нарушение и от 6 до 18 млн.руб. – повторное

Использование Google.Analytics может привести к нарушениям требований о локализации и нарушениям требований к трансграничной передаче.

При размещении сайта на зарубежном хостинге могут нарушаться требования ст.12 152-ФЗ о трансграничной передаче. Трансграничная передача без уведомления может быть квалифицирована как нарушение.

 ст.19.7. КоАП РФ

При сборе ПДн с использованием веб-аналитики (cookie) оператор должен получить согласие на обработку таких данных (cookie-баннер) и описать процесс в Политике обработки ПДн.

Политика обработки и формы сбора ПДн на сайте



Где про про Политику на сайте?
В ч.2 ст.18.1 152-ФЗ.



Если используются сервисы веб-аналитики, то это нужно
указать в Политике.



Требования к содержанию Политики
п.2. ч.1. ст.18.1. 152-ФЗ (изменены с 1 сентября 2022 г.)



Политика не может быть основанием для обработки ПДн!

Под формами сбора ПДн должно быть размещено согласие на
обработку ПДн (гиперссылка, которая ведет к полному тексту
согласия, составленного в соответствии с ч.1. ст.9 152-ФЗ)

Best Practice – размещение чек-бокса (без предустановленной
галочки) с текстом «Согласен на обработку ПДн, где
«Согласен» - гиперссылка, ведущая на полный текст согласия».



Согласен на обработку ПДн



8-800-775-9990

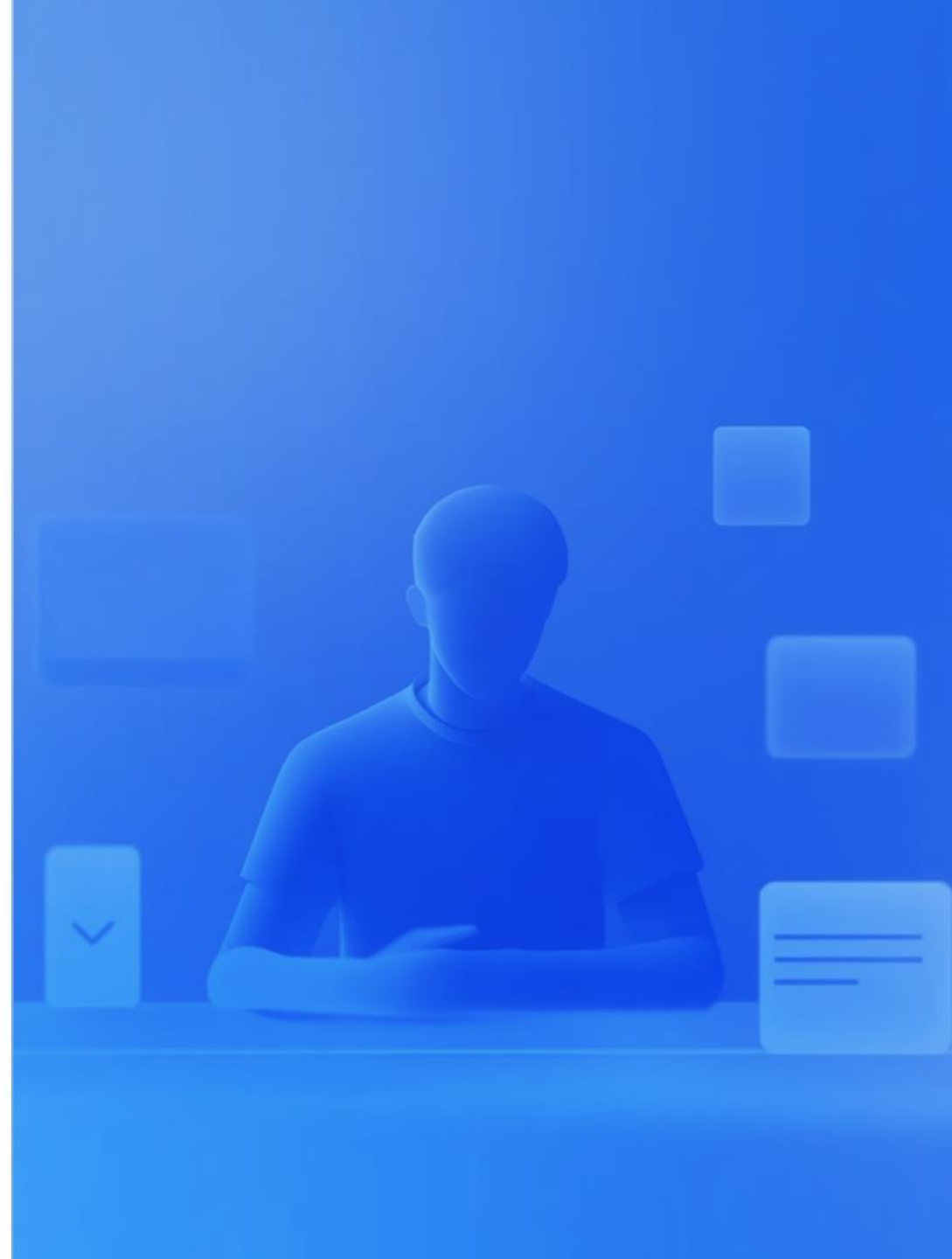


cortel.cloud

С чем пользователь должен согласиться в **обязательном порядке**

Заполняя любую форму на сайте пользователь должен дать согласие на:

- ☒ обработку персональных данных
- ☒ положения политики обработки персональных данных
- ☒ с передачей персональных данных третьей стороне (если вы пользуетесь услугами подрядчиков)
- ☒ оферту или пользовательское соглашение
- ☒ согласие на получение рекламных, информационных и иных материалов



Хотите присылать пользователю рассылки и уведомления на почту и телефон?

Позаботьтесь о том, чтобы иметь подтверждение согласия пользователя!

 Ст. 18 ФЗ-38 обязывает иметь доказательства согласия абонента (подписчика) на получение рекламы по сетям электросвязи (email, sms-рассылки и т.п.);

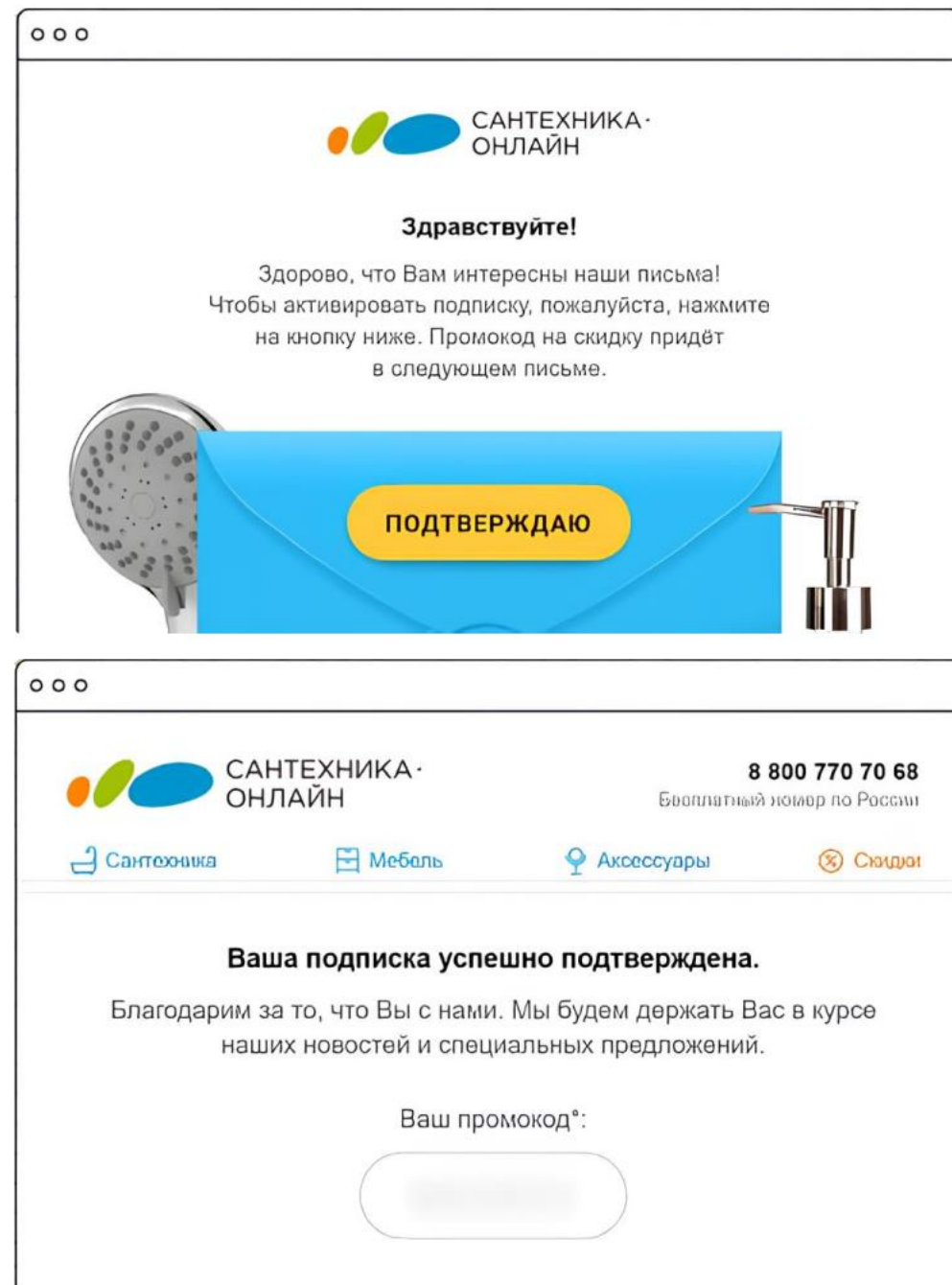
Самый удобный формат такого доказательства в случае email-маркетинга - письмо с **Double opt-in** подтверждением.

Double Opt-In — это двухэтапная подписка на рассылку. Контакт пользователя попадает в базу в два этапа:

Компания собирает email-адреса через форму на сайте.

- 2 Пользователь даёт своё согласие на получение рассылки, переходя по ссылке из письма.
Только после этого email-адрес подписчика попадает в базу рассылки.

 8-800-775-9990



Какие же документы должны быть на сайте?



Политика обработки
персональных данных



Согласие на обработку
персональных данных



Согласие с передачей персональных
данных третьей стороне
(если вы пользуетесь услугами подрядчиков)



Договор оферты
или Пользовательское соглашение.

Как выполнить требования?

Сканируйте QR-код, чтобы узнать, как легко соблюдать требования 152-ФЗ с поддержкой **CORTEL**



☰ cortel.cloud

CORTEL

Все записи

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



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».

☎ 8-800-775-9990

 cortel.cloud

Если вы заинтересовались
или у вас остались вопросы,
ВОТ МОИ КОНТАКТЫ  



**Вероника
Нечаева**

Директор по информационной
безопасности CORTEL

+7 905 925 45 68
nvv@cortel-cloud.ru