CORTEL

КАК ВЫЖИТЬ В НОВОЙ СИСТЕМЕ ШТРАФОВ ЗА ПЕРСОНАЛЬНЫЕ ДАННЫЕ

ВЕРОНИКА НЕЧАЕВА
ДИРЕКТОР ПО ИБ КОМПАНИИ CORTEL

ВЕРОНИКА НЕЧАЕВА

CISO CORTEL

Опыт работы:
Органы аттестации

Лицензиаты
ФСТЭК/ФСБ

Региональные
органы власти

Компании-интеграторы

Член ассоциации
руководителей служб ИБ

Сертифицированный аудитор ЦБ РФ

Эксперт
в области защиты ПДн, ГИС, КИИ

Data Protection Officer

Центробанка (сертификат АБИСС)

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)

8-800-775-9990

Нормативные акты в сфере защиты Пдн

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными ли муниципальными органами»;
- Трудовой кодекс Российской Федерации (глава 14 «Защита персональных данных работника»).

Требования к локальным документам оператора

Изменения в п. 2 ч. 1, ч. 2 ст. 18.1
Федерального закона «О персональных данных»:

- Установлены требования к содержанию политики и локальных актов оператора применительно к каждой цели обработки ПДн
- Доступ к политике – на каждой странице, посредством которой осуществляется сбор ПДн

НЕВЫПОЛНЕНИЕ ОБЯЗАННОСТИ ПО ОПУБЛИКОВАНИЮ ИЛИ ОБЕСПЕЧЕНИЮ ИНЫМ ОБРАЗОМ НЕОГРАНИЧЕННОГО ДОСТУПА К ПОЛИТИКЕ, СВЕДЕНИЯМ О РЕАЛИЗУЕМЫХ ТРЕБОВАНИЯХ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ → Ч. 3 СТ.13.11 КОАП РФ

Типовые ошибки обработки ПДн в интернете

- ✕ 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.

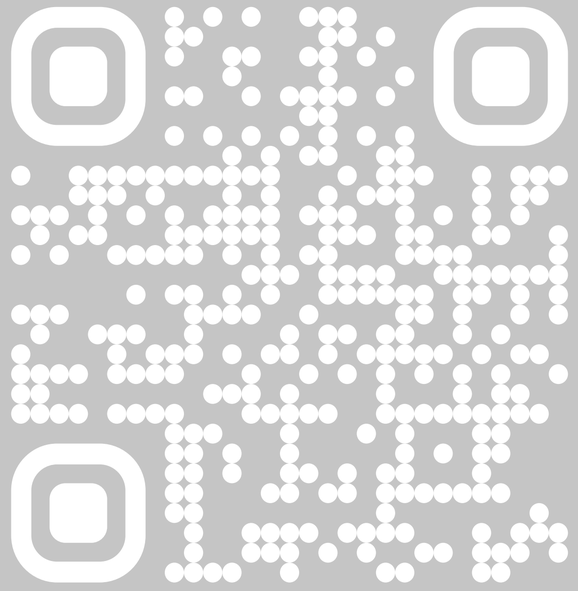
Рекомендуемые подходы к обработке ПДн

- **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
- **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
- **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)
- **Обеспечение раздельного хранения** ПДн различных категорий субъектов (клиенты, работники, соискатели и т. д.), в том числе несовместимых между собой по целям обработки

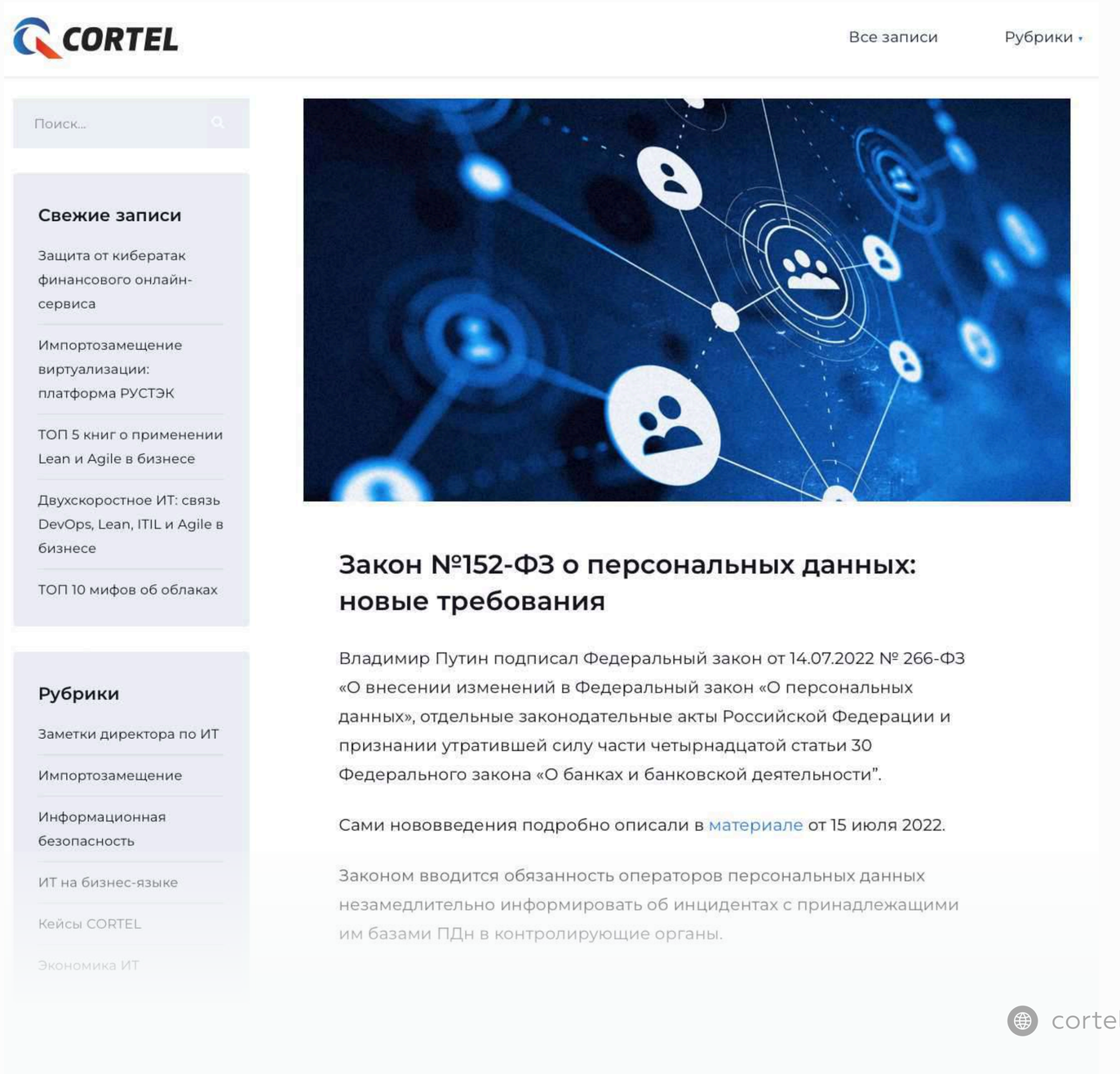
Рекомендуемые подходы к обработке ПДн

- **Назначение ответственного** за защиту ПДн, наделение его необходимыми полномочиями
- **Минимизация перечня** собираемых и обрабатываемых ПДн. Использование лишь тех данных, которые действительно необходимы для оказания услуг, продажи товаров и иной деятельности организации
- **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.

Как выполнить требования?



8-800-775-9990



Что такое ОРД

Организационно-распорядительная документация

Комплект документов,
который описывает порядок
защиты ПДн и работу с ПДн.

Содержит:

- приказы
- распоряжения
- постановления
- инструкции
- журналы
- регламенты
- формы уведомлений

Когда нужны документы ОРД

1 Стабильная работа компании

ОРД описывает порядок поступления, хранения и уничтожения ПДн в компании. С помощью ОРД устанавливаются уровни ответственности сотрудников

2 Проверки ФСБ, ФСТЭК, Роскомнадзора

ОРД - часть мер защиты ПДн, Именно с пакета ОРД начинается любая проверка

3 Подключение к ГИС, ФИС, РИС ...

Регламенты подключения большинства ИС, содержат требование о наличие ОРД, без них держатель ИС не допустит к работе

Требования к документам ОРД

Содержатся в 152-ФЗ, сайт Роскомнадзора

1 Актуальные формы	необходимо отслеживать изменения форм документов, вносить изменения по ответственным сотрудникам, если меняются цели сбора, категории ПДн
2 Соответствование требованиям к оформлению документов	соответствовать ГОСТ 7.0.97-2016. Должна быть - четкой, краткой, однозначно понятной
3 Доступ для сотрудников	все сотрудники задействованные в работе с ПДн должны иметь доступ к документам, должны быть ознакомлены с документами под роспись и быть в курсе изменений

Что проверяет РКН

1 Хостинг сайта

Должен находиться на территории РФ

2 Наличие политики ПДН и согласия на обработку

Формы изменились с 1 марта 2023 года. РКН проверяет, чтобы ссылки под формами обратной связи вели на верные документы

3 Наличие cookie баннеров, Яндекс и Google метрики

Не должны собирать избыточные данные (штрафы от 15 000 и выше) Google Analitics - отказаться от использования, так как собирает данные и передает через границу

Основные нарушения в ходе проверок РКН

- Компания отсутствует в реестре РКН
- Сбор данных без согласия субъекта ПДн
- Отсутствие актуальной Политики по обработке ПДн
- Сбор избыточных ПДн (то есть собираются данные, которые не требуется для работы с физическим лицом)
- Трансграничная передача данных

Данные публикуются в открытом доступе на сайте Роскомнадзора

Неуведомление об обработке:

на юрлиц до 100к до 300к рублей

Приказом Роскомнадзора от 28.10.2022 № 180 утверждены формы уведомлений:

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

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).

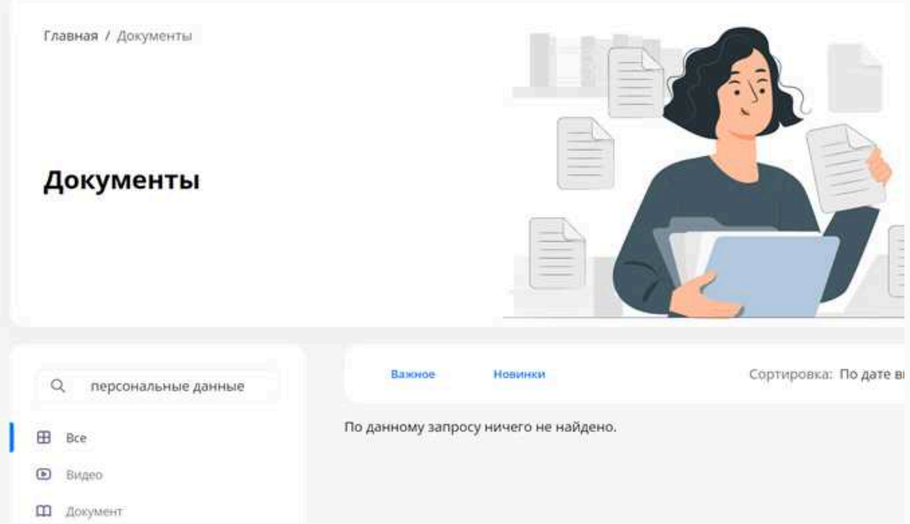
Руководитель А.Ю. Липов

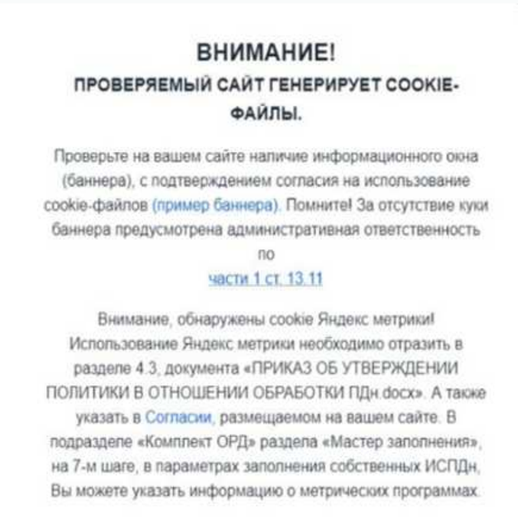
Коротко про изменения по уведомлению:

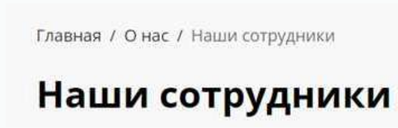
- **Если уведомление подано до вступления в силу изменений**, то есть, до 1 сентября 2022 года, необходимо переподать уведомление о внесение изменений в ранее поданное Уведомление в порядке и форме, установленных новым Приказом РКН (даже если нет изменений в текущей деятельности).
- **По обработке ПДн 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.

Уголовная ответственность за незаконную обработку

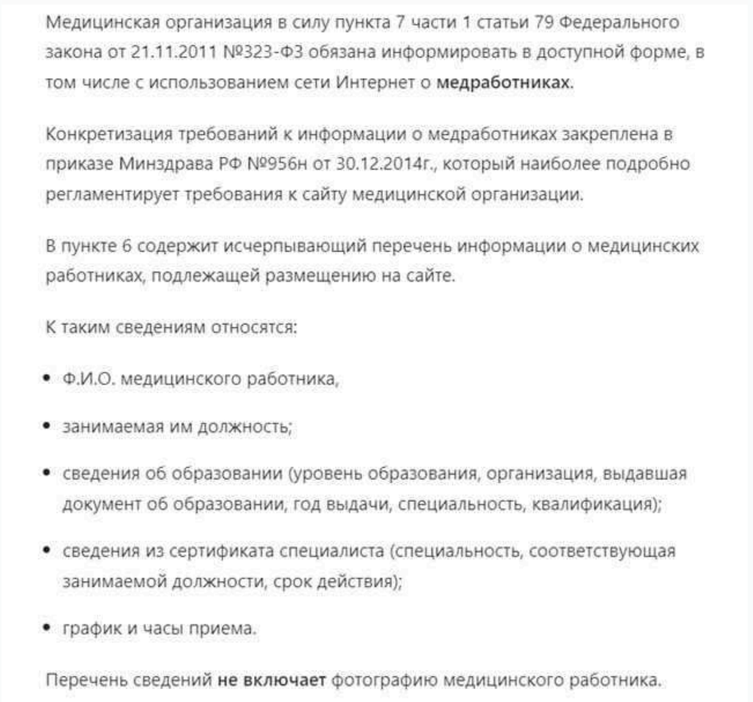
Николай и его ГБУЗ



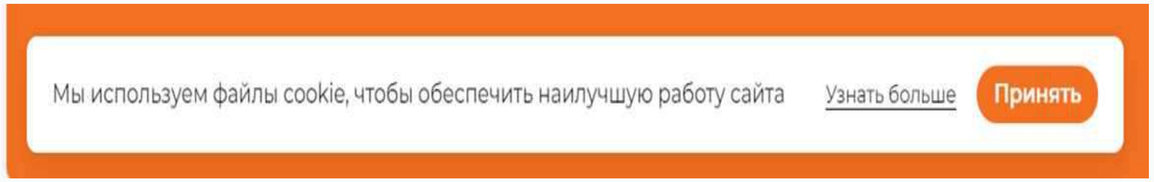


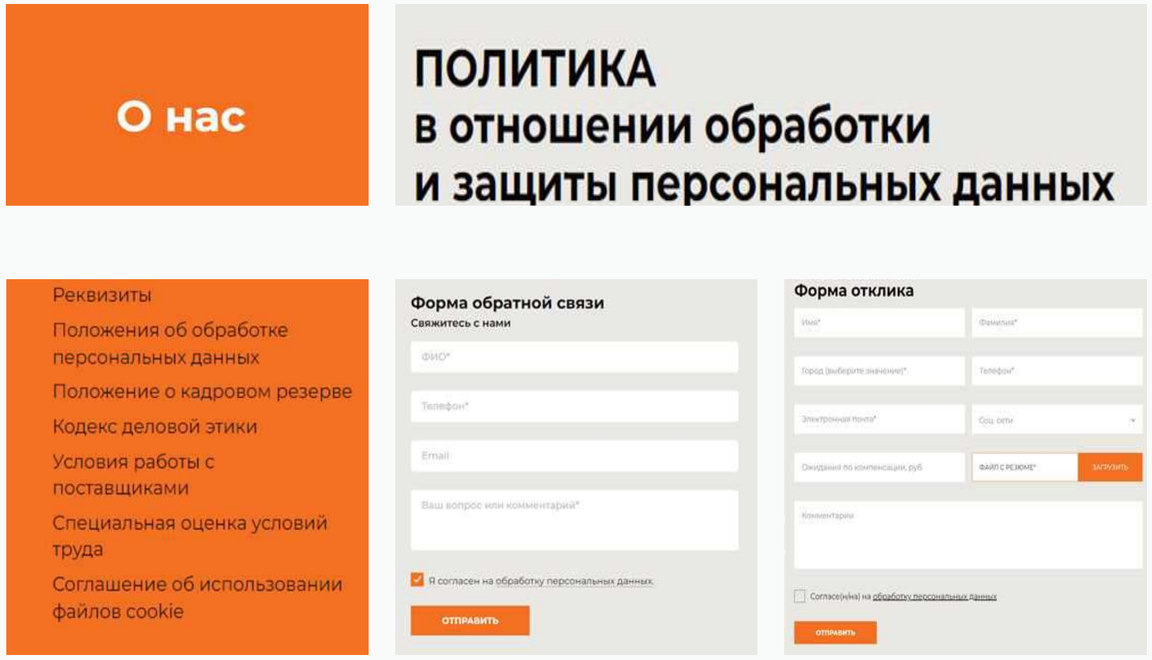


Присылайте резюме на почту:
Почтовый_ящик@домен.ru



Дмитрий и его консалтинг стратегии эффективной цифровизации



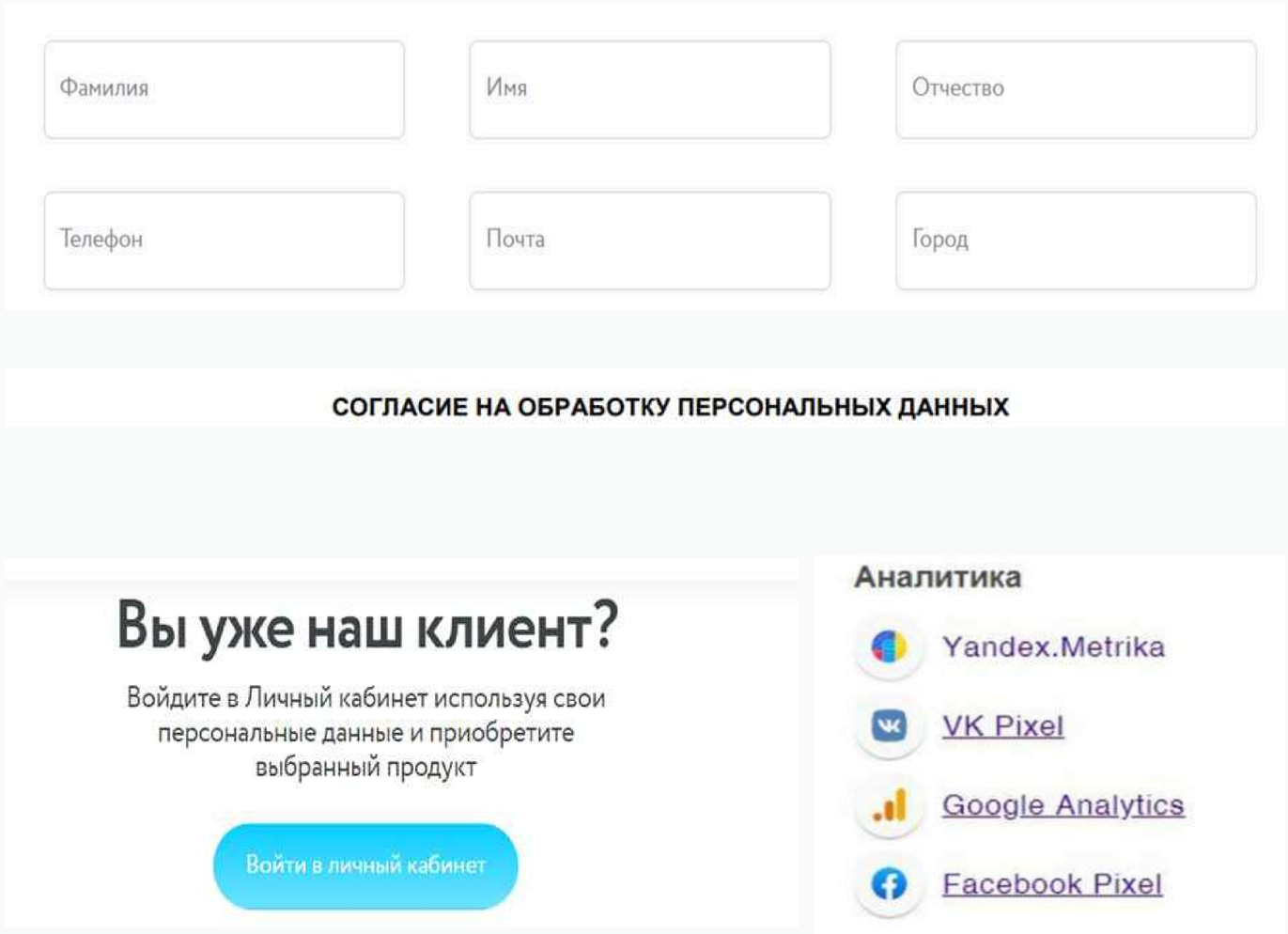


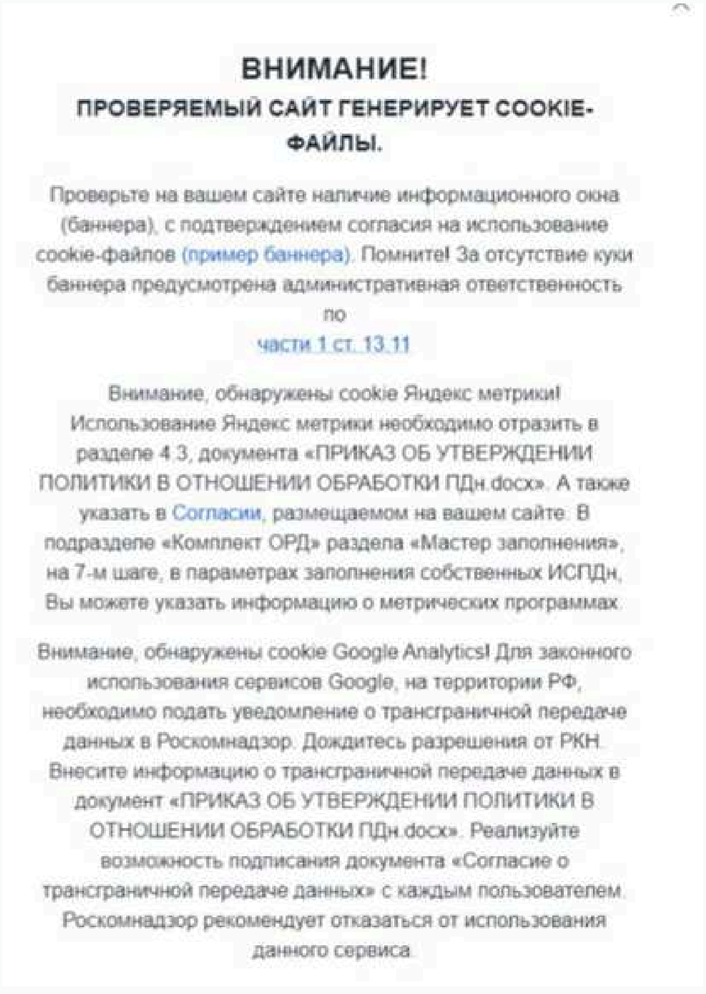
3.3 Основанием для обработки данных кандидатов является согласие субъекта на обработку персональных данных

4.1 При обращении в Компанию через способы обратной связи, представленные на веб-сайте, могут обрабатываться следующие персональные данные для ответа на запрос или для целей подбора персонала:

- Фамилия, имя, отчество;
- Номер телефона;
- Адрес электронной почты;
- А также другие данные, указываемые в соответствующей форме или приложенных документах.

Сергей и его банк





ОДНО РЕШЕНИЕ
ДЛЯ ВСЕХ ЗАДАЧ

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

152DOC поможет минимизировать риски получения штрафов от Роскомнадзора.

152DOC

1. Оперативно сформировать весь пакет документов ОРД (РКН дает 10 дней на устранение недочетов)
2. В сервисе формируются такие документы как Политика по обработке персональных данных, все формы Согласий – вам останется их утвердить и опубликовать на вашем сайте
3. В сервисе быстро и удобно менять данные и актуализировать информацию
4. После формирования документов сможете быстро подать уведомление в РКН

8-800-775-9990

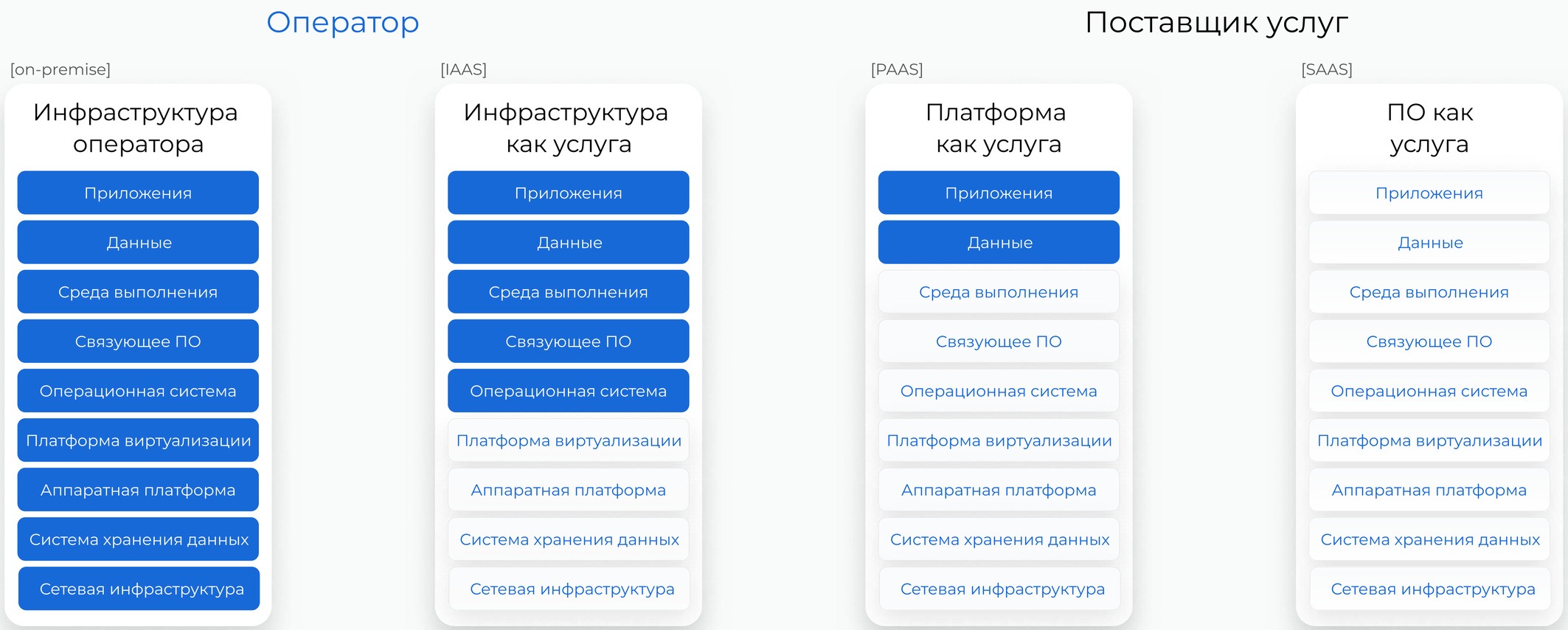
Где конкретно про “технические меры” сз ПДн?

- **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"

Границы при оценке угроз в информационной инфраструктуре поставщика услуг



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.

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)	Средтво 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:

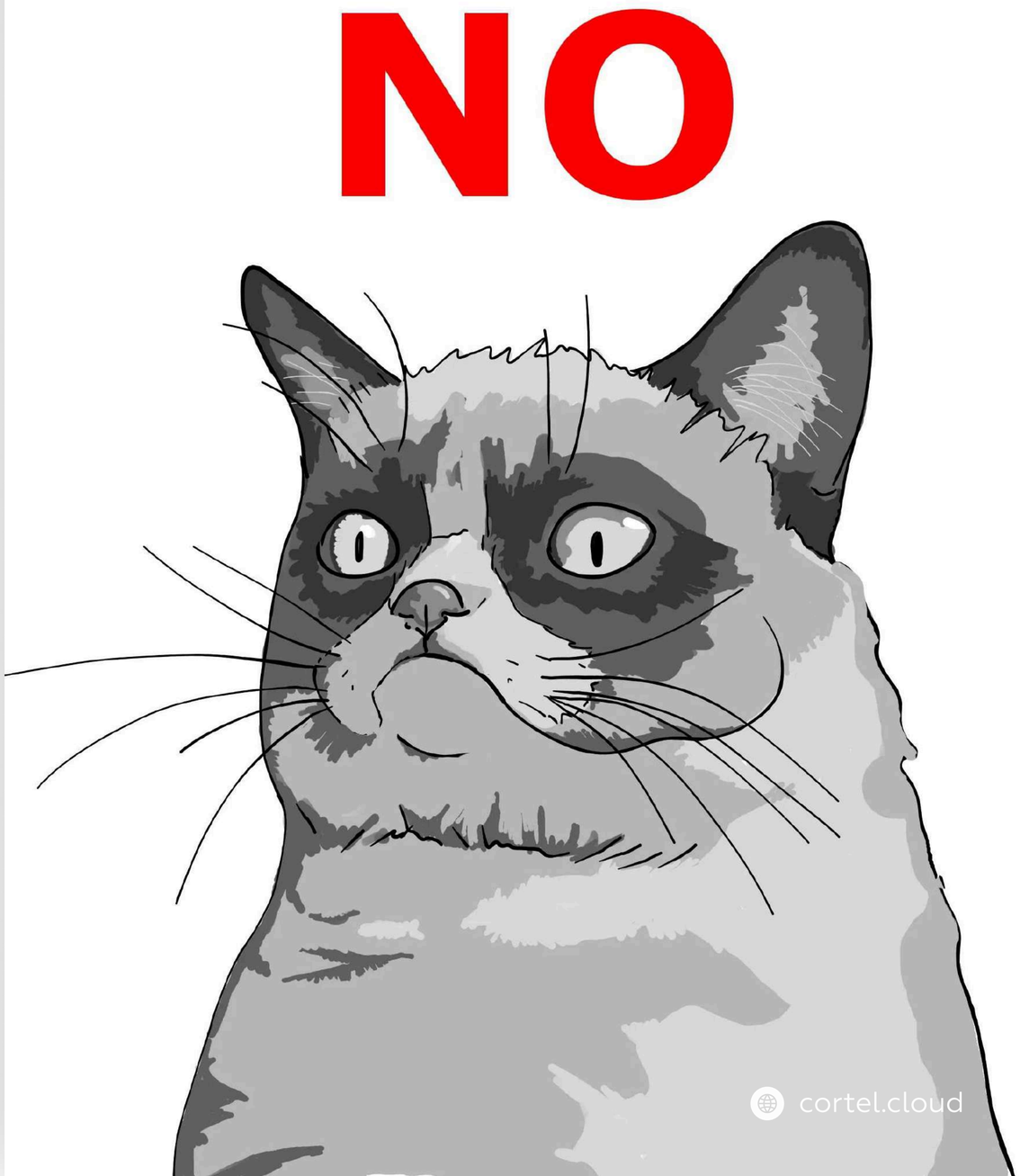
Для обеспечения... уровня защищенности ПДн при их обработке в ИС необходимо выполнение следующих требований:...
г) использование СЗИ, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких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

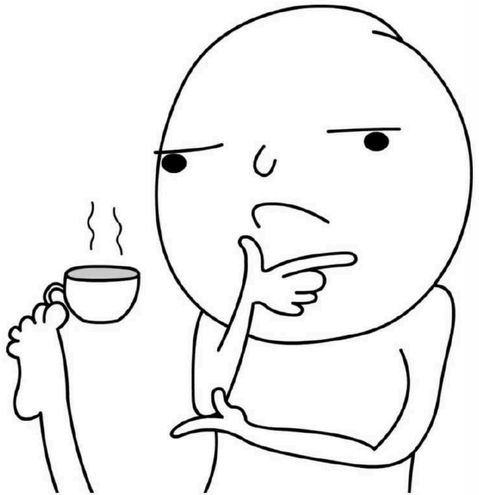
- Снижение репутационных рисков
(обоснование принятия мер защиты)

- 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 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.

Закрытый чат в Telegram

8-800-775-9990

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.

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 2025 г.

Проблемы

Штрафы
Оборотные штрафы на компанию
от 1 до 3% за утечку персональных данных.

Ответственность
Персональные санкции руководителям
за неисполнение 152-ФЗ от штрафов до уголовной
ответственности.

Стоимость решения
Высокая стоимость самостоятельного
построения защищенной инфраструктуры
для обработки и защиты ПДн.

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

Гарантии

Соответствует 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

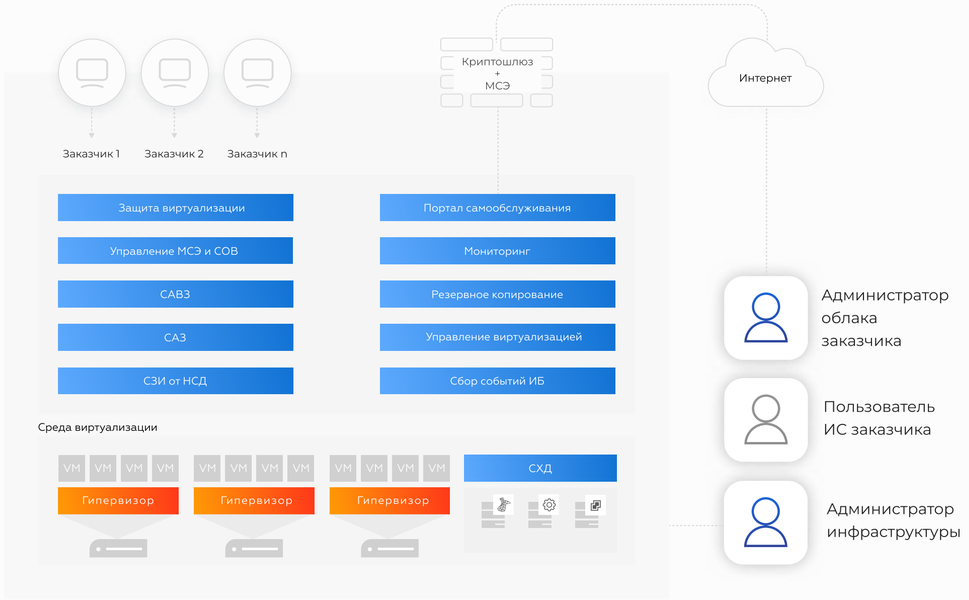
SLA 99,95 %
Договор SLA даёт финансовые гарантии.
Safe Cloud 152 может быть
недоступен не более 5 часов в год.

Внимательная техподдержка
Экспертные рекомендации,
круглосуточное обслуживание
и техническая поддержка 24/7/365
удобным для заказчика способом.

Решение SafeCloud 152:

Все меры защиты
уже в готовом удобном сервисе.
Защищенный сегмент CORTEL сразу подходит для развёртывания среды разработки ПО, ИС, размещения ПДН, требующих УЗ-2 и ГИС К2, включая размещение:

- медицинской тайны
- специальных категорий ПДН
- чувствительных данных
- данных КИИ
- 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

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.

10
лет компании

100+
проектов в России

121
эксперт

НАМ ДОВЕРЯЮТ

TION.

СОВКОМБАНК

АТОМЭНЕРГОСБЫТ
РОСАТОМ

Слата

РОССЕТИ
ТЮМЕНЬ

муниципальная новосибирская
аптечная сеть

МИНИСТЕРСТВО
ОБРАЗОВАНИЯ И НАУКИ
АЛТАЙСКОГО КРАЯ

Angioline

КОМАНДОР

Новосибирскэнергосбыт

РОССЕТИ
СИБИРЬ

СТОПДОЛГ®
юридическая компания

КрасныйЯр

БАНК АКЦЕПТ

ELTEX

VSEMAYKI.RU

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

Нечаева Вероника
Директор информационной безопасности CORTEL

Телефон:
+7 913 251 49 32

Почта:
nvv@cortel-cloud.ru