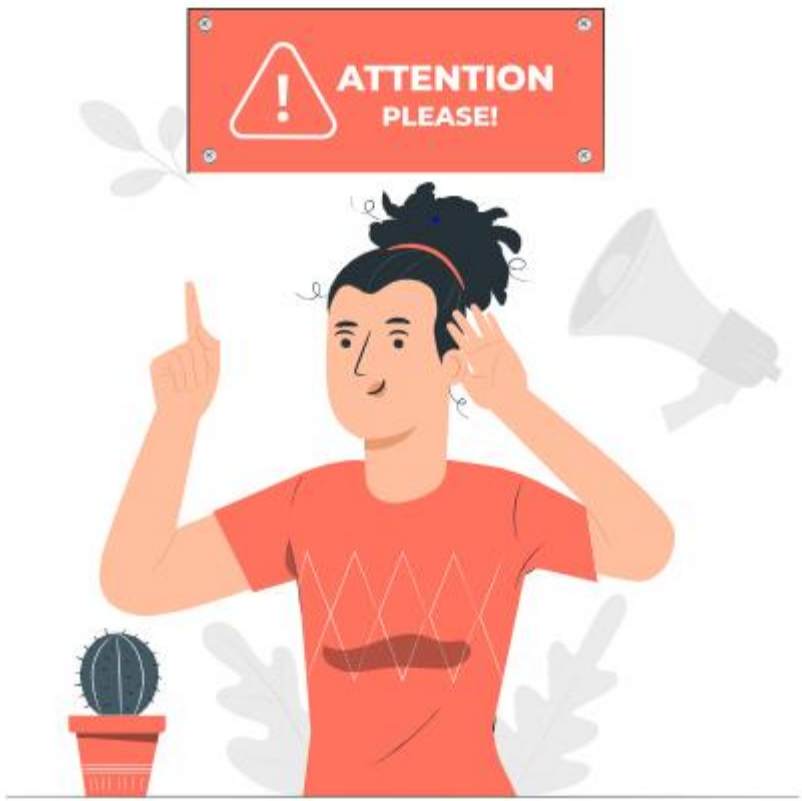
Особенности обработки персональных данных (хранения и передачи) при осуществлении электронного документооборота

Ирина Ахмедова

Руководитель практики интеллектуальной собственности
и персональных данных юридической фирмы Клифф

CLIFF

Что важно учитывать при использовании ЭДО в разрезе ПДн



1. ЭДО – это всегда участие 3-го лица (владельца системы) в обработке ПДн.
2. Статус владельца системы ЭДО в отношении обработки ПДн оператором и его оформление.
3. Различие ПДн, непосредственно вносимых в систему ЭДО, и ПДн, содержащихся в документах, загружаемых в систему.
4. Оформление согласий на передачу ПДн.
5. Защита ПДн при передаче посредством ЭДО.
6. Разграничение ответственности между оператором и владельцем системы ЭДО. Оценка рисков.

Понятие ИСПДн

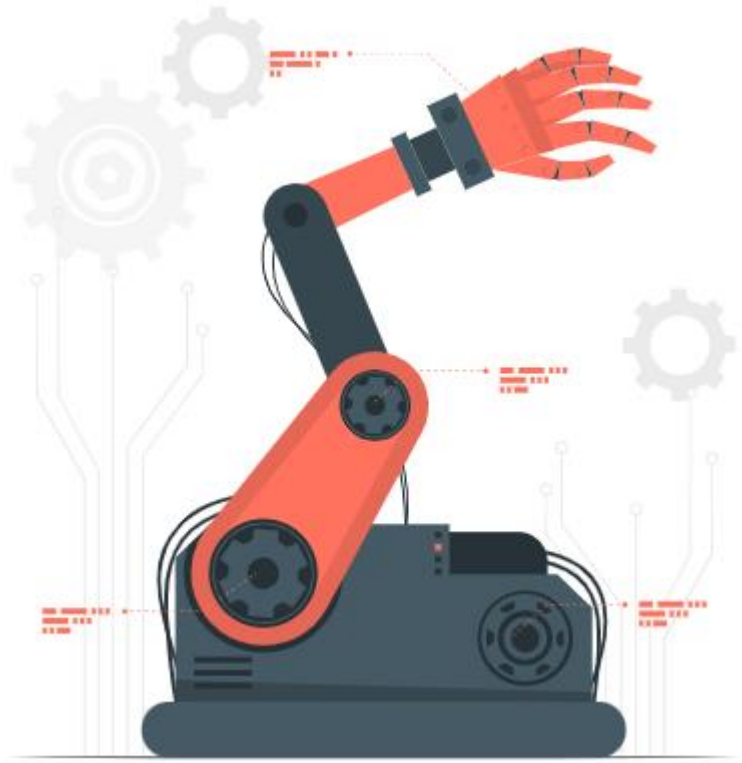
П. 10 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

Информационная система персональных данных (ИСПДн) – (1) совокупность содержащихся в базах данных ПДн и (2) обеспечивающих их обработку информационных технологий и (3) технических средств.

ИСПДн представляет собой совокупность следующих компонентов:

- ПДн;
- базы данных, в которых обрабатываются ПДн;
- серверы, на которых хранятся базы данных;
- программы, с помощью которых обрабатываются ПДн;
- компьютеры, на которых работники обрабатывают ПДн;
- защитные программы: антивирусы, межсетевые экраны и другое подобное ПО.

Понятие ИСПДн



Постановление Правительства Российской Федерации 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.

Методика ФСТЭК России от 05.02.2021.

Ключевой признак ИСПДн – наличие автоматизированной обработки, поиск ПДн в соответствии с заданным алгоритмом.

Ст. 2 Конвенции о защите физических лиц при автоматизированной обработке персональных данных (г. Страсбург 28.01.1981): автоматизированная обработка включает в себя операции, осуществляемые полностью или частично **с помощью автоматизированных средств**.

П. 4 ст. 3 Закона о ПДн автоматизированная обработка ПДн – обработка ПДн **с помощью средств вычислительной техники.**

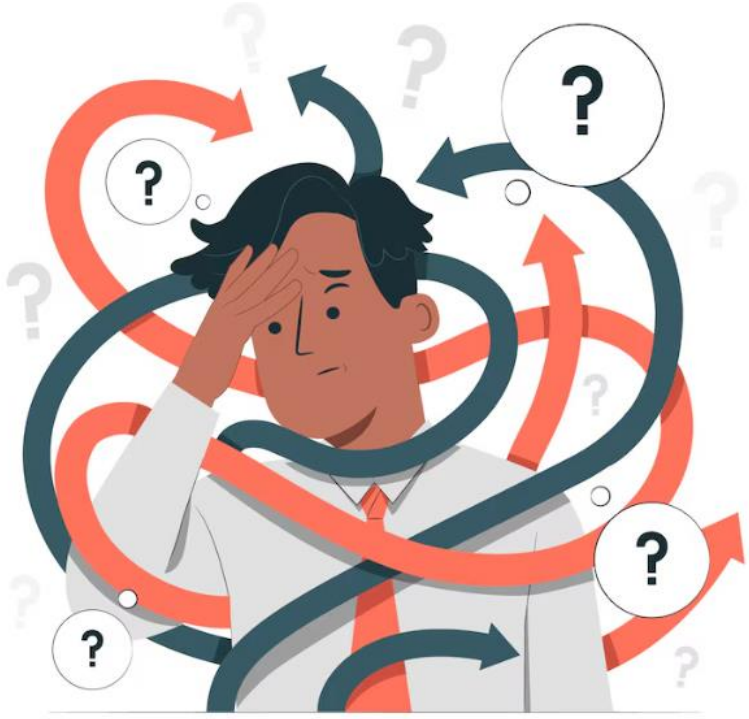
Проблемы выделения системы ЭДО в качестве ИСПДн

Исходя из структуры **система ЭДО может быть признана ИСПДн**.

Ч. 1 ст.19 Закона о ПДн:

Оператор при обработке ПДн обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

Главная проблема – как реализовывать эти меры в ситуации, когда система ЭДО контролируется владельцем системы ЭДО и возможности вмешательства оператора ограничены.



Меры по защите ПДн при обработке в ИСПДн

Ч. 2 ст. 19 Закона о ПДн возлагает на оператора ПДн **обязанности по принятию ряда мер в отношении ИСПДн, направленных на обеспечение безопасности ПДн:**

1) определение угроз безопасности ПДн;
2) применение организационных и технических мер по обеспечению безопасности ПДн;
3) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
4) применение для уничтожения ПДн средств защиты информации, в составе которых реализована функция уничтожения информации;
5) оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
6) обнаружение фактов несанкционированного доступа к ПДн и принятие необходимых мер;
7) восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
8) установлением правил доступа к ПДн;
9) контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

Статус провайдера системы ЭДО

Оператор ПДн и Обработчик ПДн

Квалификация в качестве обработчика ПДн зависит от того:

(1) **является ли система автономной** (т.е. представляет собой ПО, установленное на серверах оператора, при этом представители других компаний (в том числе поставщика такого ПО) не имеют к нему доступ), или

(2) **система функционирует как облачный сервис**, и доступ к ней имеют иные лица (в том числе в связи с обновлением ПО, осуществлением технической поддержки).

Если система функционирует как облачный сервис – владелец системы ЭДО признается обработчиком ПДн.

Оформление отношений по обработке ПДн в системе ЭДО

Ч. 3 ст. 6 Закона о ПДн:

Оператор вправе поручить обработку ПДн другому лицу **с согласия субъекта ПДн**, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (**поручение оператора**).

Обработчик ПДн обязан:

- соблюдать принципы и правила обработки ПДн, предусмотренные Законом о ПДн,
- соблюдать конфиденциальность ПДн,
- принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о ПДн.

Поручение на обработку ПДн

С 01.09.2022 в поручения на обработку ПДн необходимо включать:

- Перечень обрабатываемых ПДн;
- Цели их обработки;
- Процедуру взаимодействия между оператором и обработчиком;
- Соблюдение требования о локализации ПДн;
- Описание реализации обработчиком правовых, организационных и технических мер;
- Процедуру реагирования на компьютерные инциденты.

На практике владельцы систем ЭДО часто отказываются от заключения поручений на обработку ПДн

Виды ПДн и согласие на обработку ПДн в системе ЭДО

ПДн, которые субъект ПДн непосредственно вносит в систему ЭДО – согласие не требуется (предоставляется субъектом ПДн владельцу системы ЭДО самостоятельно).

ПДн, которые оператор непосредственно вносит в систему ЭДО – требуется согласие на передачу ПДн.

Если вносятся ПДн работников согласие в письменном виде по правилам ч. 4 ст. 9 Закона о ПДн.

В согласии указывается (кроме прочего):

- ПДн будут обрабатываться в системе ЭДО
- волеизъявление на передачу ПДн владельцу системы ЭДО для целей использования ЭДО
- сведения о владельце системы ЭДО

ПДн, которые содержатся в документах, загружаемых в систему ЭДО – ситуация неоднозначная, можно говорить о неприменении Закона о ПДн к таким ситуациям.

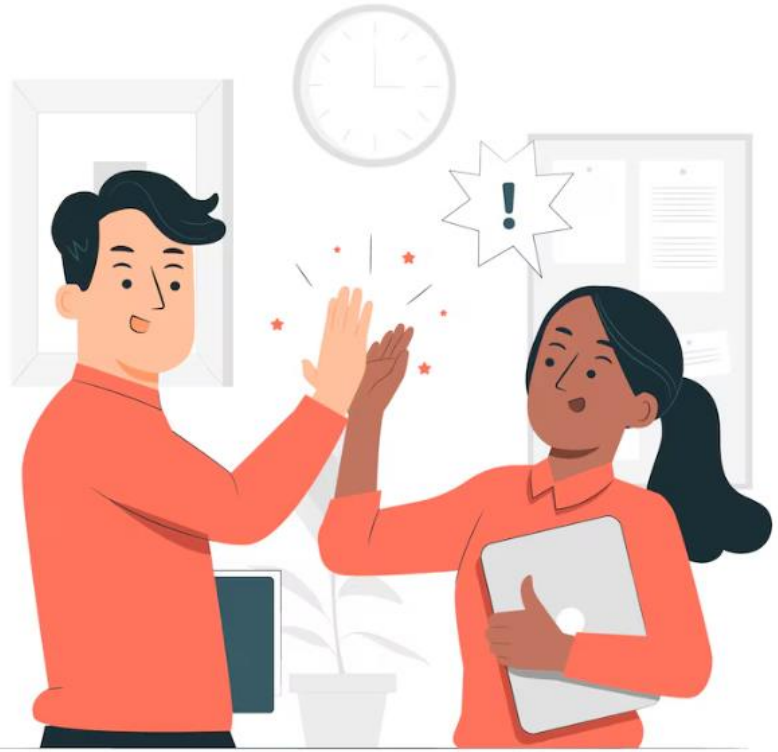
Взаимные обязательства. Разграничение ответственности

По общему правилу – вся ответственность на операторе, м.б. переложена на владельца системы ЭДО на основании договора/поручения.

1. **Меры по обеспечению безопасности** ПДн должны реализовываться оператором и владельцем системы ЭДО совместно. **Важны письменные запросы.**

2. **Для подготовки модели угроз** Заказчику рекомендуется:

   - запросить у владельца системы ЭДО результаты оценки угроз безопасности ПДн,
   - в случае непредставления – использовать информацию, размещенную в сети Интернет (например, Контрур.Диадок: https://kontur.ru/diadoc/spravka/21935-bezopasnost_elektronnogo_dokumentooborota),
   - в самой крайней ситуации – оценить систему ЭДО как скомпрометированное ПО.



Взаимные обязательства. Разграничение ответственности

3. **Средства защиты информации** должны определяться договором между оператором и владельцем системы ЭДО (условие о возможности приобретения оператором СКЗИ).
4. **Адрес ЦОД – допустимо Российская Федерация** со ссылкой на письменные отказы владельца системы ЭДО, независимое уведомление Роскомнадзора и гарантию локализации.
5. **Абсолютный характер права собственности и исключительного права** как основание для минимизации ответственности при непредставлении информации.
6. **Баланс исполнимости обязанностей оператора и обеспечения защиты ПДн.**

Ст. 4 ФЗ от 31.07.2020 № 247-ФЗ «Об обязательных требованиях в Российской Федерации»: принцип установления обязательных требований – **исполнимость обязательных требований.**

Ответственность и иные неблагоприятные последствия

Роскомнадзор не имеет полномочий по проверке реализации технических и организационных мер защиты ПДн в ИСПДн. Вправе только запрашивать документы и информацию*.

Ст. 19.7 КоАП: штраф за непредоставление сведений или предоставление неполных или недостоверных сведений – от 3 до 5 тысяч руб.

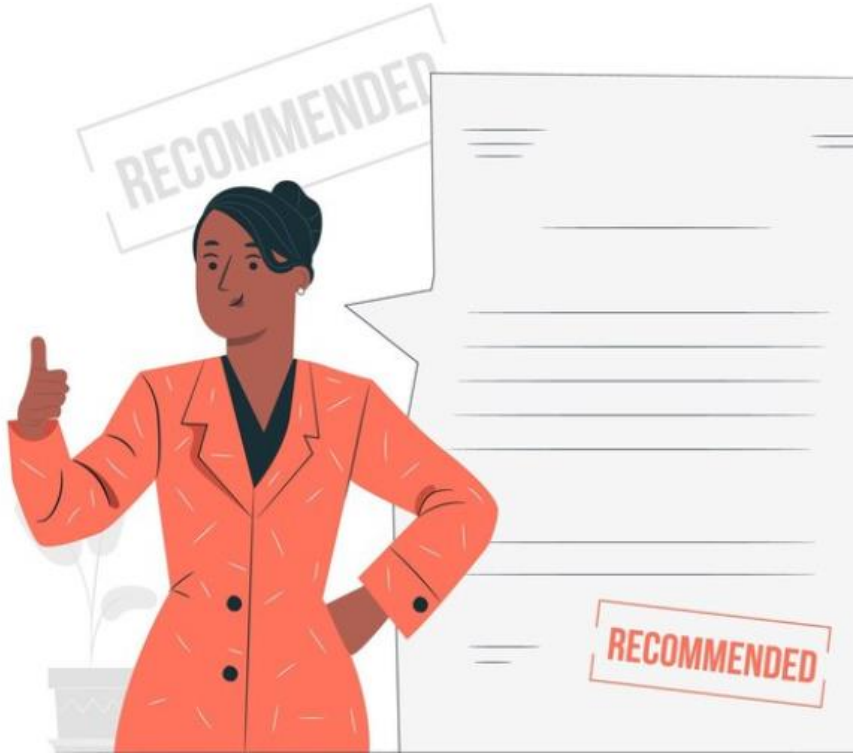
НО! Привлечение к ответственности повышает риски полной проверки.

Прокуратура вправе проверять все**.

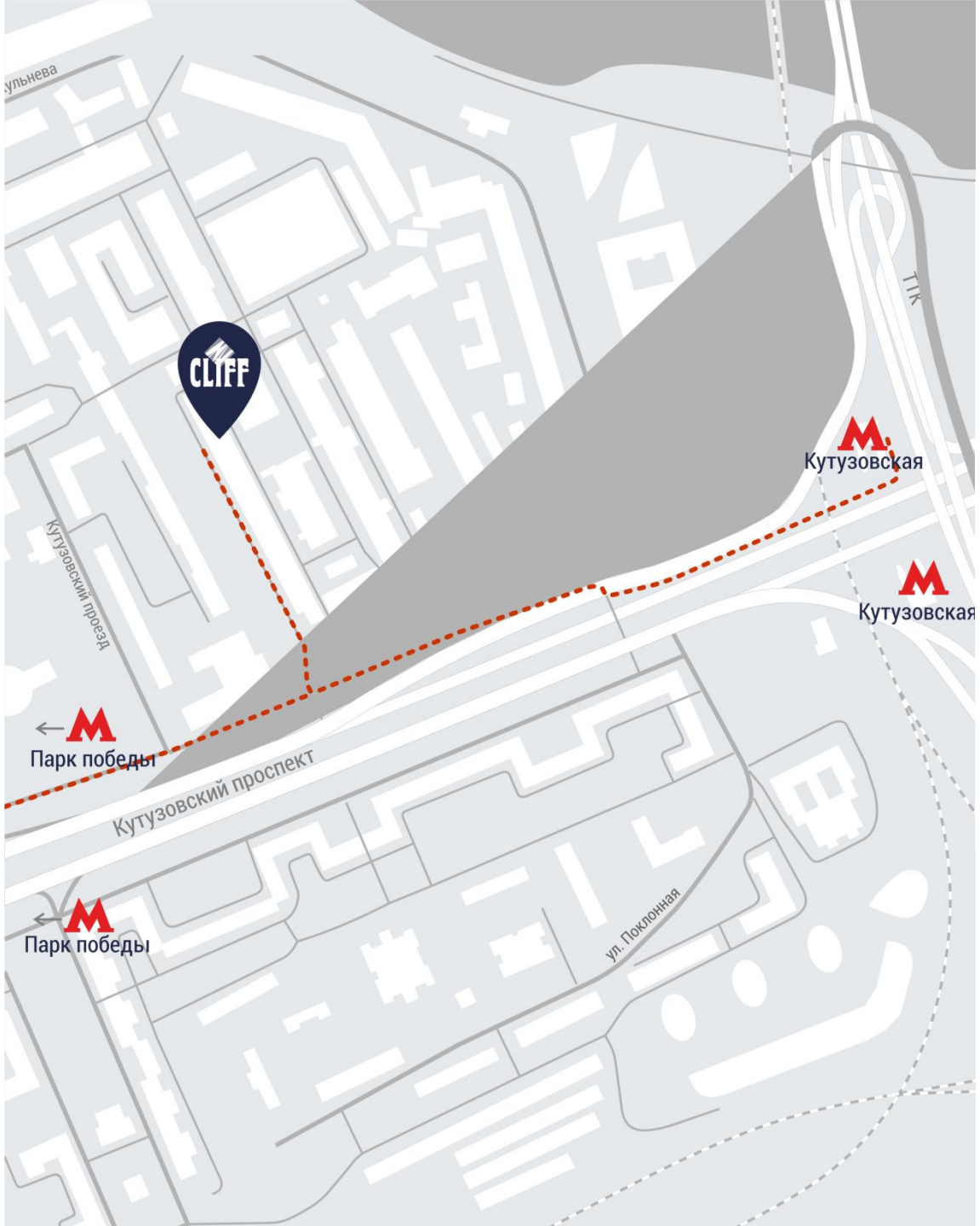
*Положение о федеральном государственном контроле (надзоре) за обработкой персональных данных, утв. Постановлением Правительства РФ от 29.06.2021 № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных»
**п. 1 ст. 21 ФЗ от 17.01.1992 № 2202-1 «О прокуратуре Российской Федерации»

Рекомендации операторам, использующим системы ЭДО

1) Заключить с владельцем системы ЭДО поручение на обработку ПДн / соглашение об обработке ПДн / урегулировать вопросы защиты ПДн в договоре;
2) Направить владельцу системы ЭДО письменный запрос о предоставлении информации о реализуемых мерах безопасности и защите ПДн;
3) Направить владельцу системы ЭДО письменный запрос об адресах нахождения серверов;
4) Не выделять систему ЭДО в качестве ИСПДн, включить ее в состав более широкой ИСПДн «Документооборот»;
5) Реализовать все возможные и необходимые меры в отношении обработки ПДн в системе ЭДО;
6) Подписывать у субъектов ПДн согласия на обработку ПДн в системе ЭДО.



Спасибо за внимание!



Контакты:

Адрес:
121170
г. Москва, Кутузовский проспект,
дом 36, строение 3, вход №8
офис 232

Телефоны:
+7 (495) 504-34-61

E-mail:
contact@cliff.ru

Сайт:
www.cliff.legal

akhmedova.i@cliff.ru

В презентации использованы картинки (векторы) по бесплатной лицензии с сайта https://ru.freepik.com/ автора @storyset