

Трансформация подхода по защите ПДн в 2025 году



Екатерина Алипова

Эксперт по консалтингу в организационно-правовой сфере департамента ИБ

Ужесточение наказаний за нарушения порядка обработки персональных данных

04.12.2023

Внесение законопроектов в ГД РФ №502104-8 О внесении изменений в КОАП РФ и № 502113-8 о внесении изменений в УК РФ

30.11.2024

Утверждение ФЗ от 30.11.2024 г. № 420-ФЗ о внесении изменений в КОАП РФ и ФЗ от 30.11.2024 г. №421-ФЗ о внесении изменений в УК РФ

30.05.2025

Окончание отсрочки в 180 дней бизнесу и вступление законов в силу. Уголовная ответственность уже действует!

Новые штрафы

- за несвоевременное уведомление РКН о намерении осуществлять обработку ПДн: до **300К**
- обработка ПДн без согласия субъекта либо с нарушением установленных требований: до **700К** для ЮЛ, до **300К** для должностных лиц
- за несвоевременное уведомление РКН в случае утечки ПДн: **до 3М**
- за «утечку» ПДн субъектов: **до 15М** для ЮЛ, **до 600К** для должностных лиц
- за невыполнение обязанности по локализации баз данных ПДн на территории РФ: до **6М** для ЮЛ, до **200К** для должностных лиц
- за «утечку» биометрических данных **до 20М** для ЮЛ , **до 1,5М** для должностных лиц
- за «утечку» специальных данных **до 15М** для ЮЛ, **до 1,3М** для должностных лиц
- за повторные «утечки» ПДн оборотные штрафы от 1% до 3% от выручки, **но не менее 20М и не более 500М**
- **за действие (бездействие)**, повлекшее неправомерную передачу ПДн, если оно содержит признаки уголовно наказуемого деяния: **наказывается штрафом либо лишением свободы в зависимости от тяжести последствия**

Судебная практика по ПДн

1. Использование систем аналитики



Применение на сайте сервисов **Google Analytics** и «**Яндекс.Метрика**» приравнивается к трансграничной передаче ПДн с нарушением требований о локализации баз с персональными данными

2. Биометрические ПДн



Применение **СКУД** с функцией **распознавания лица** без предоставления сведений, подтверждающих наличие согласия в письменной форме субъектов ПДн на обработку биометрических ПДн.

3. Передача ПДн 3-м лицам



В ходе проверки выявлено, что у лиц, собирается согласие на обработку ПДн **без уведомления о дальнейшей передачи**, в т.ч. третьим лицам - в г. Мюнхене (Германия).

4. Использование иностранных сервисов



Иностранным сервисам, прямо не направленным на российскую аудиторию, придется использовать дополнительные организационные и технические меры.

1.



2.



3.



4.



Судебная практика. Бытовые кейсы

Решение Московского районного суда (Город Санкт-Петербург) от 14.06.2023 по делу № 12-790/2023:

Бывший сотрудник пожаловался на неправомерную обработку ПДн в рамках расчета выплаты. Он сообщил, что были сделаны скан-копии всех страниц трудовой книжки, а не только последней страницы, которая содержала сведения о последнем месте работы (что и нужно было для этой выплаты). Заявитель указал, что не давал на то согласия, а в трудовой книжке находятся его ПДн. Управление Роскомнадзора не выявило нарушения, ссылаясь на дачу согласия на обработку ПДн при начале работы в организации. Однако суд не согласился с такой логикой, отменил решение РКН и направил дело на новое рассмотрение.

Определение Первого кассационного суда общей юрисдикции от 28.03.2022 по делу N 88-6426/2022:

ООО «Вайлдберриз» как работодатель привлечен к ответственности за разглашение ПДн бывшего сотрудника. Без его ведома и согласия общество выдало его бывшей сожительнице справку по форме 2-НДФЛ, которую она представила в суд вместе с иском о взыскании алиментов на ребенка.

Суд посчитал, что справка о доходах физического лица по форме 2-НДФЛ представляет собой документ, содержащий персональные данные физического лица, и могла быть выдана работодателем (налоговым агентом) только по заявлению этого лица или с его согласия. В связи с чем суд пришел к выводу о взыскании с ответчика в пользу истца компенсации морального вреда, определив сумму в 3000 рублей.

Определение Седьмого кассационного суда общей юрисдикции от 06.09.2022 по делу № 8Г-12644/2022 [88-13416/2022]:

Дело касалось пропуска сотрудником работы (работник электростанции). Работник утверждал, что он не давал согласия на обработку его биометрии для пропуска на территорию, поэтому не мог выйти на работу, где был пропускной пункт. Работодатель посчитал, что сотрудник допустил прогулы без уважительных причин. Сначала суд апелляционной инстанции удовлетворил требования работника и взыскал средний заработок за время вынужденного прогула в размере 1 451 357 рублей. Вышестоящий суд это решение отменил и вот почему.

По общему правилу для использования биометрической системы пропусков, как и для учета рабочего времени с ее помощью, необходимо получить письменное согласие на то работников и составить локальный нормативный акт организации, а также заключить дополнительные соглашения к трудовым договорам с работниками. Однако, если предприятие относится к объекту топливно-энергетического комплекса (и подобных объектов критически важной инфраструктуры) отдельного согласия на обработку биометрических ПДн не требуется в связи с необходимостью обеспечения безопасности. Там обработка биометрии осуществляется по закону.

Решение Арбитражного суда г. Москвы от 23.05.2023 по делу № А40-21074/2023:

Отдельное согласие должно быть получено и для рекламной рассылки. Само по себе принятие условий обработки персональных данных не свидетельствует о наличии согласия на получение рекламной информации.

Утечка ПДн

В Сеть попали данные желающих взять кредит в Совкомбанке

В интернете в свободном доступе опубликовали более 150 тыс. анкет с данными россиян, которые подавали онлайн-заявки на кредит в Совкомбанке.

 РИА НОВОСТИ

Сервису Skyeng грозит штраф за утечку данных пользователей

Онлайн-школе Skyeng грозит штраф до ста тысяч рублей за утечку данных пользователей



28 июня 2023, 15:44, обновлено 28 июня 2023, 18:39

Суд оштрафовал банк "Тинькофф" за утечку персональных данных

Сумма штрафа составила 70 тыс. рублей

Общество, 10 мая 2023, 21:42 | 5 508 | Поделиться

ВШЭ оштрафовали за утечку персональных данных студентов

Суд оштрафовал Высшую школу экономики на 960 тыс. за утечку персональных данных студентов

Общество, 06 авг 2022, 00:33 | 8 112 | Поделиться

СК возбудил уголовное дело после утечки данных пользователей «Яндекс.Еды»



12 декабря 2022, 16:55

Центр допобразования "Яндекса" оштрафовали за нарушение закона о персональных данных

В июле сообщалось о возможной утечке персональных данных пользователей платформы "Яндекс.Практикум"

Смягчающие обстоятельства



РАСХОДЫ ОПЕРАТОРА

Ежегодные расходы оператора за последние 3 года составляют не менее 0,1% от годовой выручки



ВЫПОЛНЕНИЕ ЗАКОНОДАТЕЛЬНЫХ ТРЕБОВАНИЙ

Выполнение требований к защите ПДн при их обработке в ИС за предшествующий год документально подтверждается



ОТСУТСТВИЕ НАРУШЕНИЙ

Отсутствуют нарушения в части сбора, обработки ПДн, своевременных оповещений Роскомнадзора, а также правил информирования граждан о политике оператора в отношении работы с ПДн

Что выгоднее?



Трансформация подхода по защите персональных данных

1. Изменение бизнес-процессов



Оптимизация бизнес-процессов с целью минимизации перечня и количества собираемых ПДн позволит снизить риски штрафных санкций

2. Повышение культуры ИБ



Знание правил обработки ПДн и понимание необходимости их выполнения формируют у сотрудников навыки противодействия киберугрозам

3. Предотвращение кибератак



Выбор технических решений должен основываться не на типовом наборе мер ФСТЭК России, а на анализе прямых и косвенных рисков

4. Тестирование на проникновение



Тестирование на проникновение является способом проверки внедренной системы защиты на надежность

5. Регулярное выполнения требований по защите ПДн



Ежедневное соблюдение требований по защите ПДн с последующей фиксацией свидетельств позволит повысить защищенность ПДн

6. Аудит ИБ



Ежегодное подтверждение выполнения требований законодательства лицензиатом ФСТЭК является смягчающим обстоятельством при утечке ПДн

Оценка рисков утечки



Этапы работ (если система защиты не внедрена)

ОБСЛЕДОВАНИЕ



1-2 месяца

Результат

1. Изучим документы и ИТ-инфраструктуру, проведем интервью с сотрудниками и изучим процесс обработки ПДн
2. Разработаем отчет

РАЗРАБОТКА ДОКУМЕНТАЦИИ



1-2 месяца

Результат

1. Разработаем Модель угроз, Акты определения УЗ
2. Разработаем ТЗ и ТП на систему защиты
3. Комплект ОРД

ВНЕДРЕНИЕ СЗПДн



3-6 месяца

Результат

1. Внедренные средства защиты
2. Пакет эксплуатационной документации

ОЦЕНКА СООТВЕТСТВИЯ



1 месяц

Результат

1. Запущенная в эксплуатацию система защиты
2. Заключение о соответствии требованиям

КОНСУЛЬТАЦИИ И СОПРОВОЖДЕНИЕ



Результат

1. Техническая поддержка и консультации
2. Сопровождение при проверках и инцидентах

DPO-as-a-service

Сторонний эксперт, ответственный за организацию обработки ПДн

Этапы работ (если система защиты внедрена)

ОБСЛЕДОВАНИЕ



Около 1 месяца

Результат

1. Изучим документы и ИТ-инфраструктуру, проведем интервью с сотрудниками и изучим процесс обработки ПДн
2. Разработаем отчет

АКТУАЛИЗАЦИЯ ДОКУМЕНТАЦИИ



1-2 месяца

Результат

1. Модель угроз, Акты определения УЗ
2. ТЗ и ТП на систему защиты
3. Комплект ОРД

ВНЕДРЕНИЕ НЕДОСТАЮЩИХ СЗИ



3-6 месяца

Результат

1. Внедренные средства защиты
2. Пакет эксплуатационной документации

ОЦЕНКА СООТВЕТСТВИЯ



1 месяц

Результат

1. Подтверждение выполнения требований по защите ПДн

КОНСУЛЬТАЦИИ И СОПРОВОЖДЕНИЕ



Результат

1. Техническая поддержка и консультации
2. Сопровождение при проверках и инцидентах

DPO-as-a-service

Сторонний эксперт, ответственный за организацию обработки ПДн

vDPO – кому актуально?

vDPO (Virtual Data Protection Officer) –
внешний специалист или компания, выполняющие функции
ответственного за обработку персональных данных

Ответственного за
обработку ПДн нет,
функции распределены
между юристами и ИТ, или
не реализованы

Критичный бизнес-процесс
завязан на обработку
клиентских ПДн

Комплект документов
разработан, но процессы не
работают, что создает риск
санкций со стороны
регуляторов

Большое количество
процессов обработки ПДн
и передачи третьим лицам

Необходимо быть готовым
к успешному прохождению
проверок регуляторов

DPO-as-a-service или virtual DPO

Реагирование на изменения законодательства

- Подготовка новостных отчетов по теме обработки ПДн
- Оперативное планирование действий по доработке ОРД и корректировке процессов
- Актуализация ОРД

Внедрение процессов

- Разработка комплекта документов
- Назначение ответственных лиц
- Получение свидетельств

Обучение работников

- Адаптация обучающих материалов под контекст компании
- Проведение онлайн-обучения
- Инструктаж новых работников 1 раз в месяц
- Контроль знаний через полгода
- Повторное обучение

Мониторинг

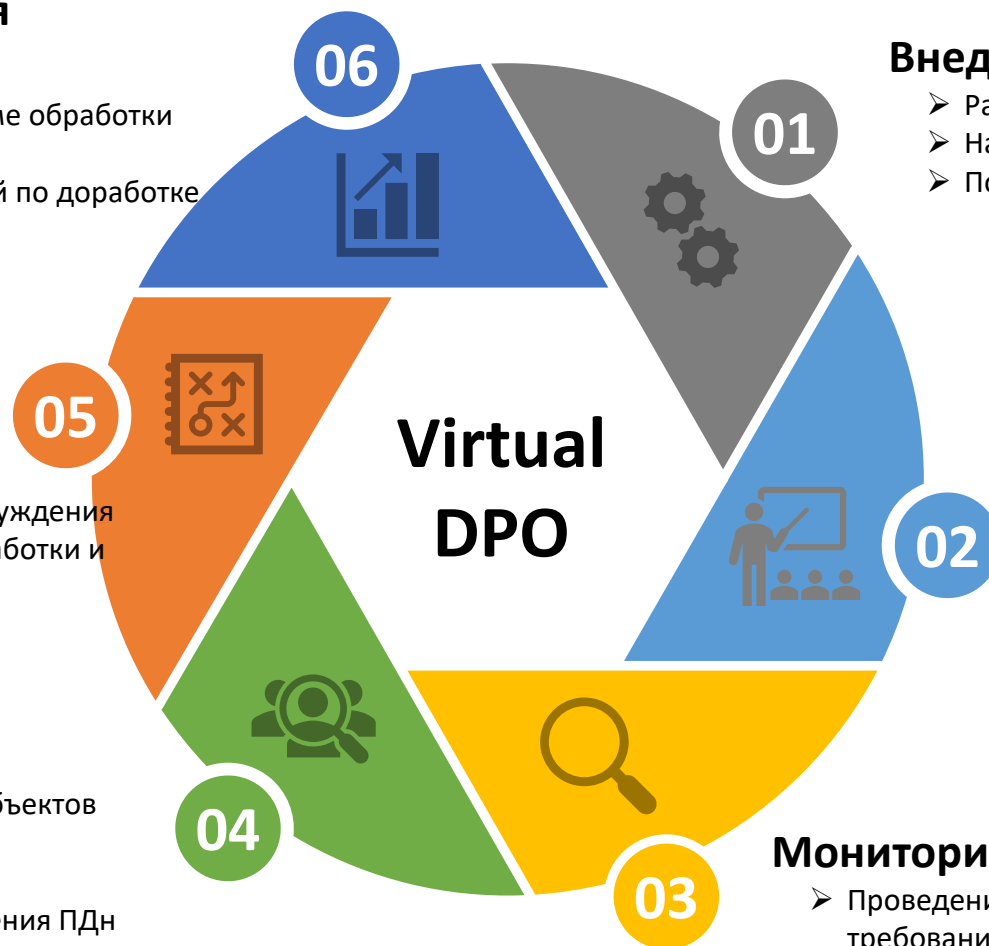
- Проведение внутреннего аудита выполнения требований по защите ПДн
- Контроль выполнения политик и регламентов
- Реагирование на инциденты

Консультирование

- Регулярные онлайн-встречи для обсуждения всех текущих вопросов по теме обработки и защиты ПДн

Ответы на запросы

- Подготовка ответов на запросы субъектов ПДн/регуляторов/партнеров
- Регистрация запросов
- Организация уничтожения/изменения ПДн



Екатерина Алипова

Эксперт по консалтингу ИБ

М +7 961 227 40 27

Ekaterina.Alipova@softline.com