РЕФОРМА 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ». РАЗБОР ПРОБЛЕМНЫХ СИТУАЦИЙ И СПОСОБОВ ИХ РЕШЕНИЯ.

Илья Романов
Руководитель Отдела консалтинга

ДиалОгНаука

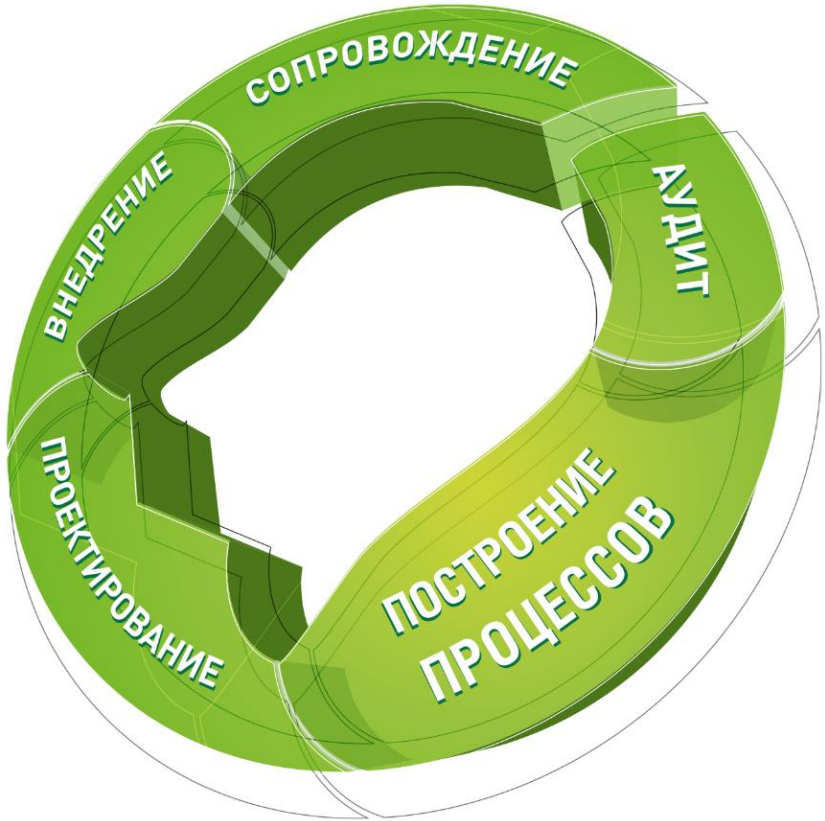
О компании

ДиалогНаука

- Создана в 1992 году СП «Диалог» и Вычислительным центром РАН.
- Первые продукты – ревизор ADinf, антивирусы Aidstest и Dr. WEB.
- В настоящее время – системный интегратор в области информационной безопасности.

Направления деятельности

- 152-ФЗ и GDPR
- Объекты КИИ (187-ФЗ)
- Положения Банка России
- ГОСТ 57580
- PCI DSS
- ISO 27001
- АСУ ТП
- Коммерческая тайна
- Сведения ДСП
- Защита ГИС



О компании «ДиалогНаука»: ключевые Заказчики

Разбор правоприменительной практики

План вебинара:

- Контрольные мероприятия в области ПДн.
- Интернет-сайты и 152-ФЗ (политика, согласия).
- Оценка вреда – как и зачем?
- Состав ПДн, особенности «кадровых» ПДн.
- Уничтожение ПДн.
- Уведомление об инцидентах.
- Уведомление об обработке и трансграничной передаче ПДн.

Основа вебинара – опыт реализации проектов по тематике ПДн, публичные мероприятия с участием Операторов ПДн и регуляторов, информация из СМИ

Разбор правоприменительной практики

План вебинара:

- **Контрольные мероприятия в области ПДн.**
- Интернет-сайты и 152-ФЗ (политика, согласия).
- Оценка вреда – как и зачем?
- Состав ПДн, особенности «кадровых» ПДн.
- Уничтожение ПДн.
- Уведомление об инцидентах.
- Уведомление об обработке и трансграничной передаче ПДн.

Контрольные мероприятия в области ПДн

- Внеплановые проверки
  - например, в случае утечек.
- Запросы РКН
  - операторы обязаны ответить в течение 10 рабочих дней (формально в соответствии с 152-ФЗ это не надзорное мероприятие);
  - допустимо получение запросов и требований со стороны территориальных управлений, которые находятся в другом регионе, поскольку возможно нарушение прав гражданина, который проживает на территории данного региона.

Разбор правоприменительной практики

План вебинара:

- Контрольные мероприятия в области ПДн.
- **Интернет-сайты и 152-ФЗ (политика, согласия).**
- Оценка вреда – как и зачем?
- Состав ПДн, особенности «кадровых» ПДн.
- Уничтожение ПДн.
- Уведомление об инцидентах.
- Уведомление об обработке и трансграничной передаче ПДн.

Интернет-сайты и 152-ФЗ

Основные проблемные аспекты, связанные с Интернет-сайтами:

- Политика в отношении обработки ПДн:
  - требования к содержанию;
  - требования к размещению.

- Согласия на обработку ПДн с использованием сайта:
  - с использованием метрических программ;
  - с использованием типовых форм, размещенных на сайте.

Требования к локальным актам и Политике

Оператор обязан издать:

- ✓ политику в отношении обработки ПДн;
- ✓ локальные акты по вопросам обработки ПДн,
- ✓ локальные акты, направленные на предотвращение, выявление и устранение последствий нарушений законодательства РФ

Требования к локальным актам и Политике

Оператор обязан издать:

- ✓ политику в отношении обработки ПДн;
- ✓ локальные акты по вопросам обработки ПДн,
- ✓ локальные акты, направленные на предотвращение, выявление и устранение последствий нарушений законодательства РФ

Должны определять **для каждой** цели обработки ПДн:
- ✓категории и перечень ПДн;
- ✓категории субъектов ПДн;
- ✓способы обработки;
- ✓сроки обработки и хранения;
- ✓порядок уничтожения.

Требования к локальным актам и Политике

Оператор обязан издать:

- ✓ политику в отношении обработки ПДн;
- ✓ локальные акты по вопросам обработки ПДн,
- ✓ локальные акты, направленные на предотвращение, выявление и устранение последствий нарушений законодательства РФ

Политика оператора в отношении обработки ПДн должна быть доступна **на всех страницах** Интернет-сайтов, которые используются для сбора ПДн.

Согласия на сайте

- ✓ **Согласие на сбор технической информации о пользователе и cookie-файлов:**
  - жестких требований нет, рекомендуемый вариант – всплывающее окно;
  - обработка cookie-файлов должна быть учтена в Политике (в большинстве случаев это отдельная цель);
  - необходимо отразить использование сторонних метрических программ;
  - иностранные метрические программы = трансграничная передача ПДн (позиция РКН).

Согласия на сайте

✓ **Согласие на обработку ПДн в иных случаях**

- рекомендуется включать как минимум: наименование Оператора, цель обработки, сведения о составе ПДн, о передаче третьим лицам;

- указывать ссылку на политику в отношении обработки ПДн

Разбор правоприменительной практики

План вебинара:

- Контрольные мероприятия в области ПДн.
- Интернет-сайты и 152-ФЗ (политика, согласия).
- **Оценка вреда – как и зачем?**
- Состав ПДн, особенности «кадровых» ПДн.
- Уничтожение ПДн.
- Уведомление об инцидентах.
- Уведомление об обработке и трансграничной передаче ПДн.

Оценка вреда субъектам ПДн

- ✓ Приказ Роскомнадзора от 27 октября 2022 г. № 178 "Об утверждении Требований к оценке вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона "О персональных данных"

- ✓ Примеры критериев определения степени вреда:
  - обработка биометрии, или спецкатегорий;
  - обработка ПДн несовершеннолетних;
  - обезличивание с целью скоринга и оказания услуг по прогнозированию;
  - поручение обработки иностранному лицу;
  - ведение общедоступных источников;
  - и др. критерии, **касающиеся состава, целей и особенностей обработки ПДн**.

Оценка вреда субъектам ПДн

Пример 1.

Критерий:

- ✓ обработка сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПДн) и которые используются оператором для установления личности субъекта ПДн, **за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки биометрических ПДн.**

Комментарий:

- ✓ В случае обработки ПДн в ЕБС критерий неприменим.

Оценка вреда субъектам ПДн

Пример 2.

Критерии:

- ✓ сбор ПДн с использованием баз данных, находящихся за пределами РФ;
- ✓ обработка ПДн в дополнительных целях, отличных от первоначальной цели сбора

Комментарий:

- ✓ Если эти критерии применимы, то нарушаются требования 152-ФЗ

Оценка вреда субъектам ПДн

Пример 3.

✓ А что, если ни один из критериев не применим?

Комментарий:
~~Вариант 1 – Субъектам не может быть причинен вред~~
Вариант 2 – Не может быть причинена ни одна из степеней вреда, согласно Приказу РКН

Оценка вреда субъектам ПДн

- ✓ На степень возможного вреда **НЕ** влияет:
  - объем обрабатываемых сведений;
  - оценка последствий в случае возможных инцидентов с ПДн;
  - реализуемые меры по защите.

- ✓ Согласно ПП-1119 определение типа угроз безопасности ПДн производится **с учетом оценки возможного вреда**, но каким образом учитывать такую оценку нормативные документы не поясняют.

Разбор правоприменительной практики

План вебинара:

- Контрольные мероприятия в области ПДн.
- Интернет-сайты и 152-ФЗ (политика, согласия).
- Оценка вреда – как и зачем?
- **Состав ПДн, особенности «кадровых» ПДн.**
- Уничтожение ПДн.
- Уведомление об инцидентах.
- Уведомление об обработке и трансграничной передаче ПДн.

Состав и категории ПДн. Правоприменение

Персональными данными являются следующие сведения (примеры из практики РКН):

- ✓ Номер телефона и любая дополнительная информация, включая MAC, IMEI и др.;
- ✓ Различные идентификаторы (СНИЛС, ИНН и др.);
- ✓ Личный корпоративный e-mail;
- ✓ Реквизиты банковских карт и платежная информация.

Состав и категории ПДн. Правоприменение

К специальным категориям персональных данных относятся в том числе (правоприменительная практика):

- ✓ сведения о нетрудоспособности (больничные);
- ✓ медицинские книжки;
- ✓ сведения в военных билетах;
- ✓ сведения об инвалидности.

ПРИМЕЧАНИЕ: кстати, согласно 323-ФЗ к врачебной тайне относят в том числе сведения о факте обращения за медицинской помощью, сведения, полученные при мед. обследовании и лечении.

Состав и категории ПДн. Правоприменение

Рекомендуемый подход в отношении обработки «кадровых» спецкатегорий ПДн (больничные, военники, сведения об инвалидности и несчастных случаях):

- ✓ В большинстве случаев правовые основания обработки – это требования законодательства.
- ✓ В отдельных случаях – может потребоваться согласие (например, при обработке ПДн родственников)
- ✓ Выделяем в отдельные ИСПДн с кол-вом субъектов менее 100 000 (это позволит ограничится 3-уровнем защищенности)

Разбор правоприменительной практики

План вебинара:

- Контрольные мероприятия в области ПДн.
- Интернет-сайты и 152-ФЗ (политика, согласия).
- Оценка вреда – как и зачем?
- Состав ПДн, особенности «кадровых» ПДн.
- **Уничтожение ПДн.**
- Уведомление об инцидентах.
- Уведомление об обработке и трансграничной передаче ПДн.

Уничтожение ПДн

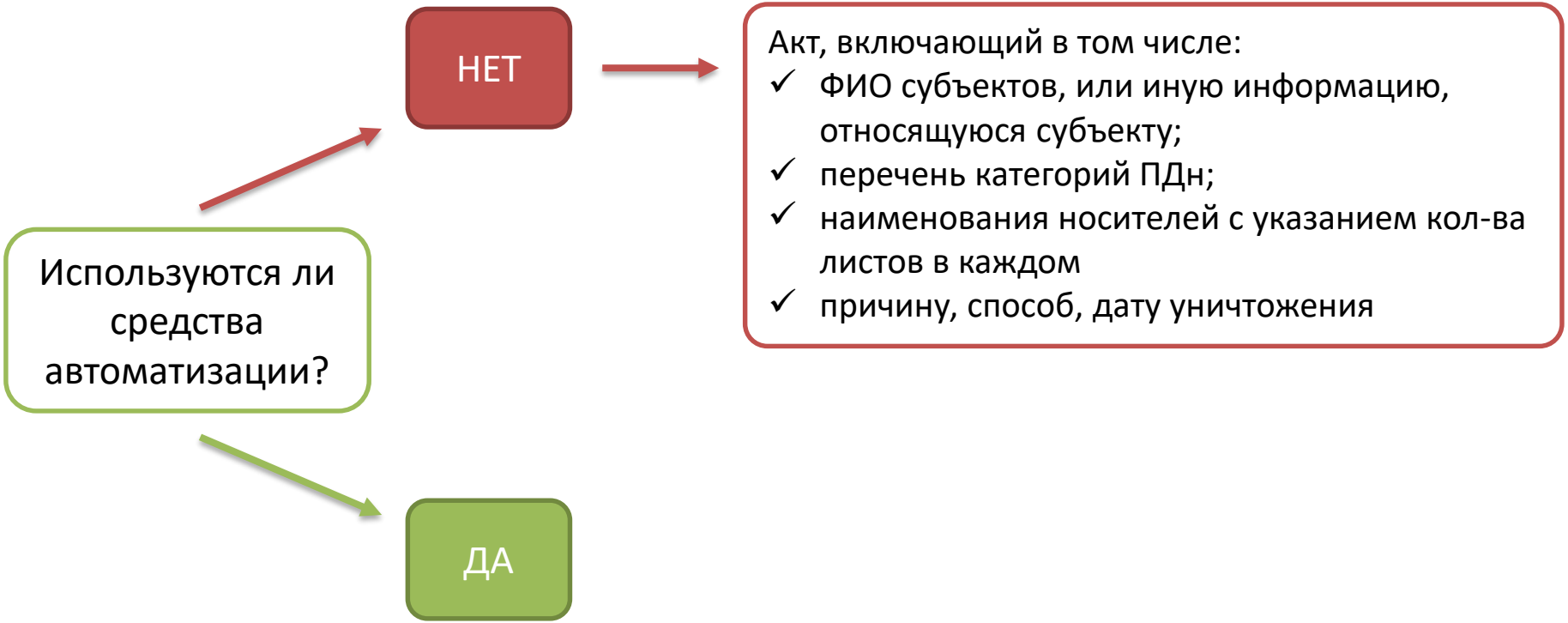
Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 г. № 179 «Об утверждении Требований к **подтверждению уничтожения** персональных данных»

Требования применяются в случаях :

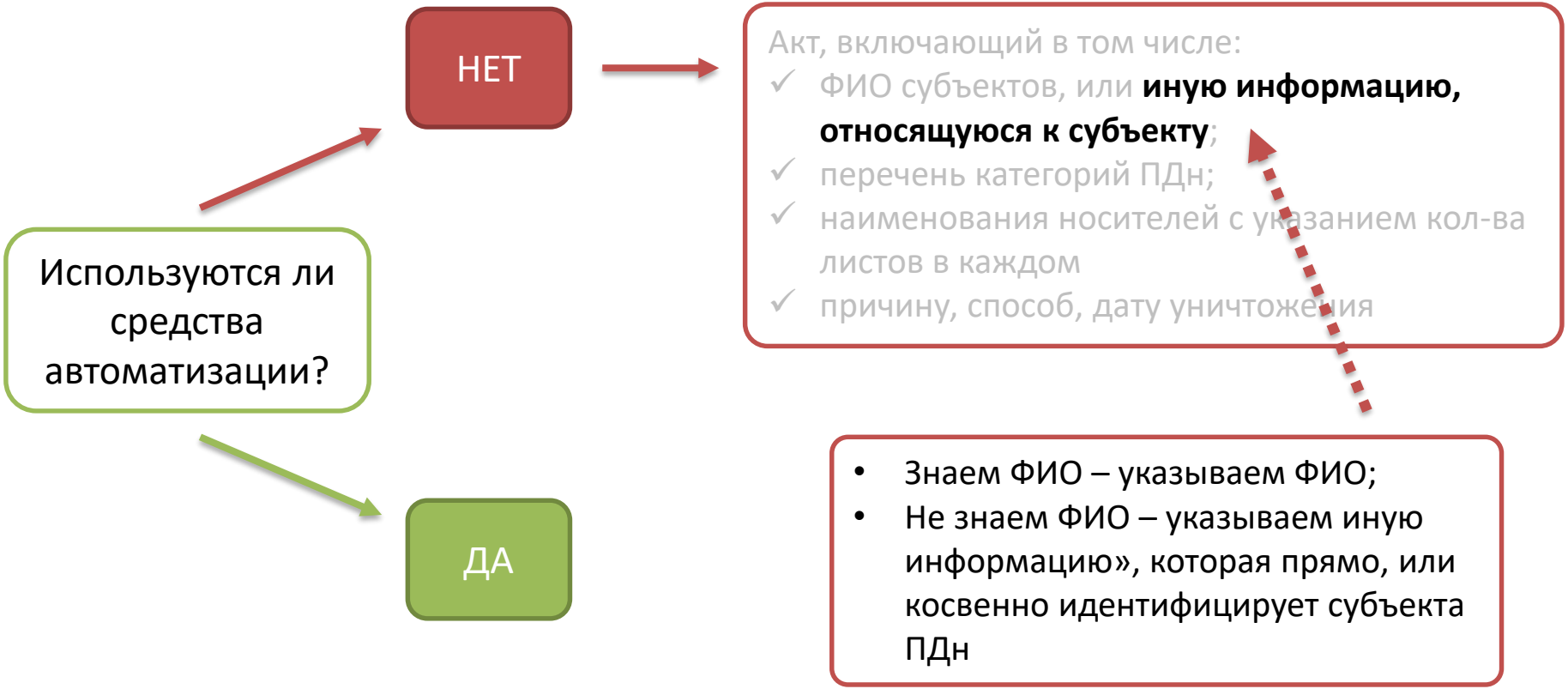
- ✓ выявления неправомерной обработки ПДн;
- ✓ достижения цели обработки ПДн;
- ✓ отзыва субъектом ПДн согласия на обработку ПДн.
- ✓ при отсутствии иных правовых оснований для продолжения обработки.

Уничтожение ПДн

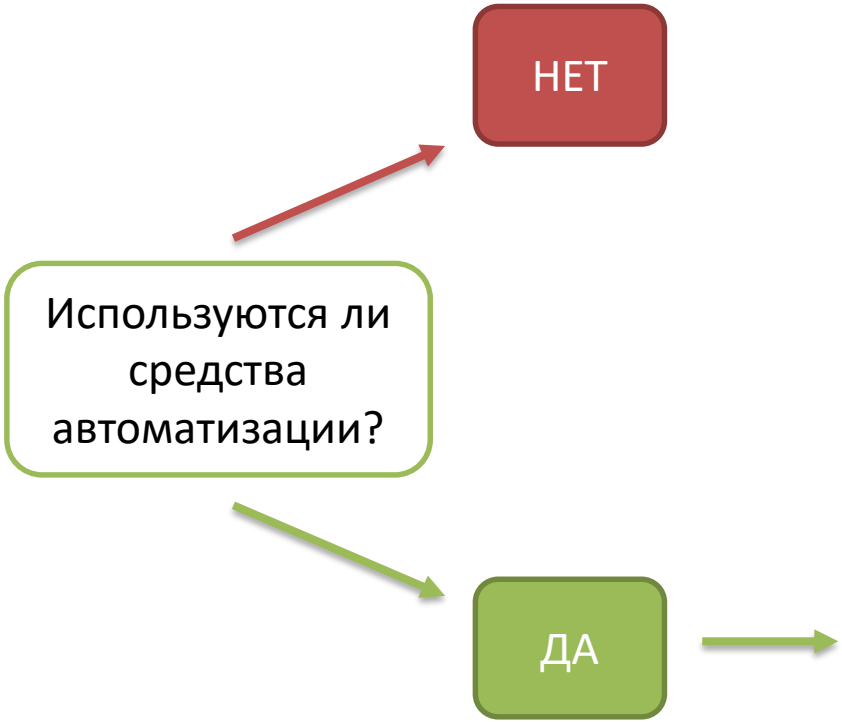
Уничтожение ПДн



Уничтожение ПДн



Уничтожение ПДн



Акт, включающий в том числе:

- ✓ ФИО субъектов, или иную информацию, относящуюся субъекту);
- ✓ перечень категорий ПДн;
- ✓ наименования носителей с указанием кол-ва листов в каждом
- ✓ причину, способ, дату уничтожения

Выгрузка из журнала ИСПДн, включающая:

- ✓ ФИО субъектов, или иную информацию, относящуюся субъекту);
- ✓ перечень категорий ПДн;
- ✓ наименование ИСПДн;
- ✓ причину и дату уничтожения

Уничтожение ПДн

- ✓ Если выгрузка из журнала не позволяет указать отдельные сведения, недостающие сведения вносятся в акт.
  - Вопрос: А можно ли вообще не делать выгрузку?

- ✓ Акт и выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения ПДн.

Разбор правоприменительной практики

План вебинара:

- Контрольные мероприятия в области ПДн.
- Интернет-сайты и 152-ФЗ (политика, согласия).
- Оценка вреда – как и зачем?
- Состав ПДн, особенности «кадровых» ПДн.
- Уничтожение ПДн.
- **Уведомление об инцидентах.**
- Уведомление об обработке и трансграничной передаче ПДн.

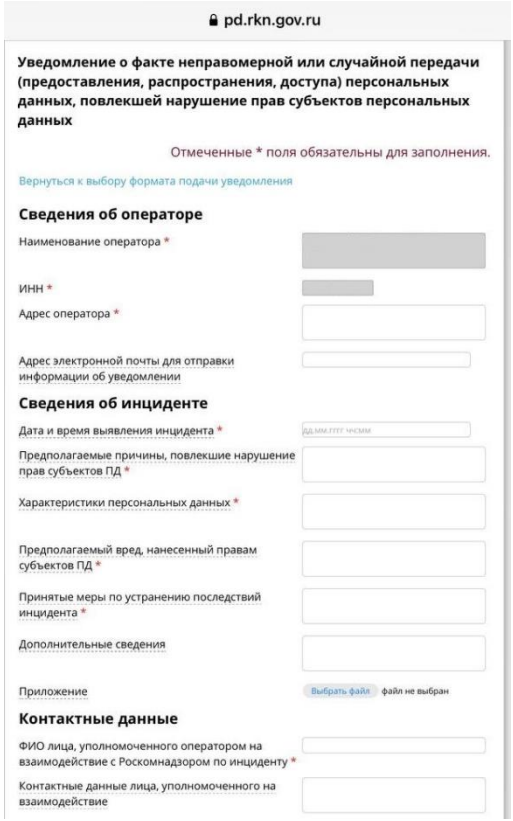
Уведомление об инцидентах

Ст. 19 – Обязанность обеспечения взаимодействия с ГосСОПКА, включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПДн.

Ст. 21 – Обязанность информирования о факте неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, **повлекшей нарушение прав субъектов ПДн**, а также о результатах внутреннего расследования.

Уведомление об инцидентах

Уведомление РКН об инцидентах - форма


pd.rkn.gov.ru

Уведомление о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных

Отмеченные * поля обязательны для заполнения.

Вернуться к выбору формата подачи уведомления

Сведения об операторе

Наименование оператора *

ИНН *

Адрес оператора *

Адрес электронной почты для отправки информации об уведомлении

Сведения об инциденте

Дата и время выявления инцидента *

Предполагаемые причины, повлекшие нарушение прав субъектов ПД *

Характеристики персональных данных *

Предполагаемый вред, нанесенный правам субъектов ПД *

Принятые меры по устранению последствий инцидента *

Дополнительные сведения

Приложение

Выбрать файл файл не выбран

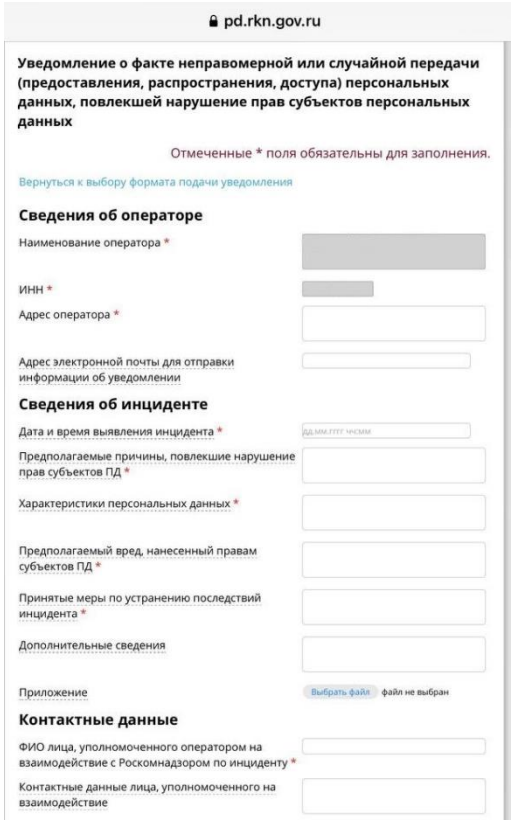
Контактные данные

ФИО лица, уполномоченного оператором на взаимодействие с Роскомнадзором по инциденту *

Контактные данные лица, уполномоченного на взаимодействие

- Дата и время выявления инцидента
- Причины, повлекшие нарушение прав субъектов ПДн
- Характеристики ПДн
- Предполагаемый вред правам субъектов ПДн
- Принятые меры по устранению последствий

Уведомление РКН об инцидентах - форма



pd.rkn.gov.ru

Уведомление о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных

Отмеченные * поля обязательны для заполнения.

Вернуться к выбору формата подачи уведомления

Сведения об операторе

Наименование оператора *

ИНН *

Адрес оператора *

Адрес электронной почты для отправки информации об уведомлении

Сведения об инциденте

Дата и время выявления инцидента *

Предполагаемые причины, повлекшие нарушение прав субъектов ПД *

Характеристики персональных данных *

Предполагаемый вред, нанесенный правам субъектов ПД *

Принятые меры по устранению последствий инцидента *

Дополнительные сведения

Приложение

Выбрать файл файл не выбран

Контактные данные

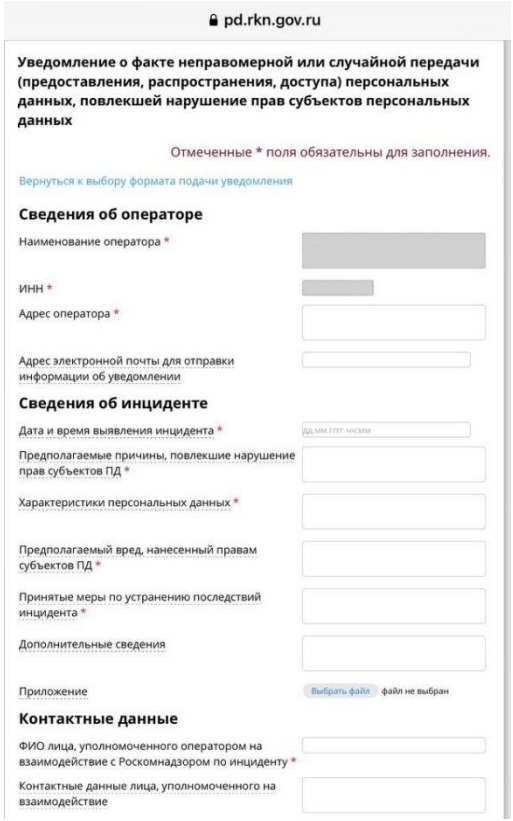
ФИО лица, уполномоченного оператором на взаимодействие с Роскомнадзором по инциденту *

Контактные данные лица, уполномоченного на взаимодействие

- Дата и время выявления инцидента
- Причины, повлекшие нарушение прав субъектов ПДн
- **Характеристики ПДн**
- Предполагаемый вред правам субъектов ПДн
- Принятые меры по устранению последствий

- ✓кол-во записей
- ✓категории субъектов
- ✓категории ПДн
- ✓актуальность БД
- ✓период сбора ПДн

Уведомление РКН об инцидентах - форма


pd.rkn.gov.ru

Уведомление о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных

Отмеченные * поля обязательны для заполнения.

Вернуться к выбору формата подачи уведомления

Сведения об операторе

Наименование оператора *

ИНН *

Адрес оператора *

Адрес электронной почты для отправки информации об уведомлении

Сведения об инциденте

Дата и время выявления инцидента *

Предполагаемые причины, повлекшие нарушение прав субъектов ПД *

Характеристики персональных данных *

Предполагаемый вред, нанесенный правам субъектов ПД *

Принятые меры по устранению последствий инцидента *

Дополнительные сведения

Приложение

Выбрать файл файл не выбран

Контактные данные

ФИО лица, уполномоченного оператором на взаимодействие с Роскомнадзором по инциденту *

Контактные данные лица, уполномоченного на взаимодействие

- Дата и время выявления инцидента
- Причины, повлекшие нарушение прав субъектов ПДн
- Характеристики ПДн
- Предполагаемый вред правам субъектов ПДн
- **Принятые меры по устранению последствий**

В соответствии со статьями 18.1 и 19

Уведомление РКН о расследовании - форма

- ✓ Результаты расследования, в том числе информация о
  - причинах инцидента;
  - вреде, нанесенном правам субъектов;
  - информационной системе;
  - мерах, принятых по результатам расследования.

- ✓ Сведения о лицах, действия которых стали причиной инцидента:
  - ФИО, должность (в отношении работника);
  - ФИО, наименование, IP-адрес, предполагаемое местонахождение и иные сведения (в отношении посторонних лиц)

Разбор правоприменительной практики

План вебинара:

- Контрольные мероприятия в области ПДн.
- Интернет-сайты и 152-ФЗ (политика, согласия).
- Оценка вреда – как и зачем?
- Состав ПДн, особенности «кадровых» ПДн.
- Уничтожение ПДн.
- Уведомление об инцидентах.
- **Уведомление об обработке и трансграничной передаче ПДн.**

Уведомление об обработке ПДн

Ст. 22, ч. 2 – Сокращено количество случаев, освобождающих от необходимости уведомлять Роскомнадзор об обработке ПДн.

Больше **не являются** исключением случаи:

- ✓ Обработки ПДн в соответствии с трудовым законодательством;
- ✓ Обработки ПДн для исполнения договора.

Уведомление **не требуется** в случаях:

- ✓ Обработки в ГИС, созданных в целях защиты безопасности государства и общественного порядка;
- ✓ Обработки исключительно без использования средств автоматизации;
- ✓ Обработки, согласно законодательству о транспортной безопасности.

Состав уведомления об обработке ПДн

Ст. 22, ч. 2

Оператор **для каждой цели обработки ПДн** указывает

- ✓ категории ПДн;
- ✓ категории субъектов ПДн;
- ✓ правовое основание обработки ПДн;
- ✓ перечень действий с ПДн;
- ✓ способы обработки ПДн.

Трансграничная передача - уведомление

- ✓ Больше нельзя подать уведомление **об осуществляемой** трансграничной передаче ПДн.

- ✓ Перед началом трансграничной передачи ПДн – нужно подать уведомление о таком намерении.
  - *Исключения – ПП-2526, например для почтовой связи*

- ✓ Если поданные ранее сведения о трансграничной передаче изменились – нужно также подать уведомление.

- ✓ Роскомнадзор, рассмотрев уведомление, может ограничить или запретить трансграничную передачу (ПП-24).
  - *Исключения – ПП-2526, например, использование платежных систем*

Вопросы?

117105, г. Москва, ул. Нагатинская, д. 1

Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: info@DialogNauka.ru