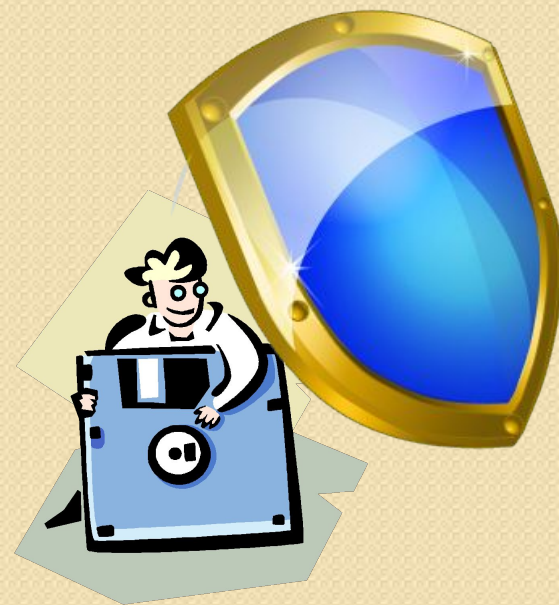


ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ СВОИМИ СИЛАМИ

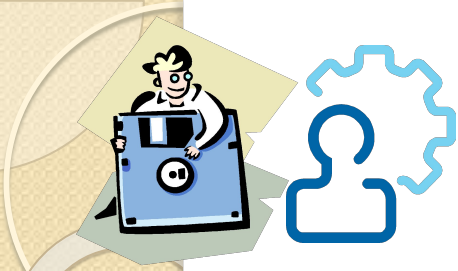


ДОКУМЕНТ

кадровое делопроизводство

- аудит
- восстановление
- обучение

2015 г.



Основные понятия

Персональные данные (ПДн) — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Оператор персональных данных — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн (ст.3, № 152-ФЗ).



- Иванов
- Иван Иванович

- ООО «Люттик»
- Иванова
- Мария Ивановна

- Паспортные данные





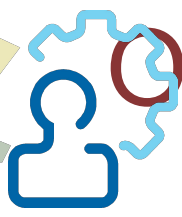
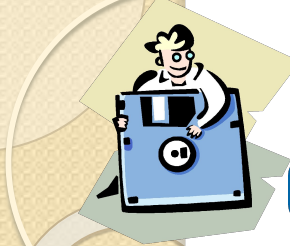
Дата рождения



Номер телефона



ФИО, место работы,
размер з/п



ОСНОВНЫЕ ПОНЯТИЯ

- **Общедоступные данные (ПДн)** — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности

- **Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
(ст.3, № 152-ФЗ).

Данные о человеке, обрабатываемые только с отдельного письменного разрешения



- национальная принадлежность
- политические взгляды
- религиозные убеждения



РИСКИ ПРИ РАЗГЛАШЕНИИ ПНД



Утрата паспорта (копии)

- Непредвиденные кредиты
- Регистрация СИМ карт и оплата счетов за разговоры



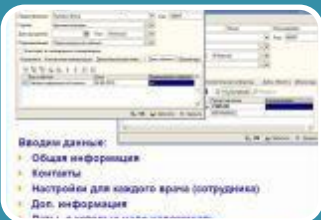
Утрата банковской карты или данных

- Оплата покупок через интернет
- Перевод денег на электронные кошельки



Разглашение данных об истории болезни

- Продажа БАД по телефону
- Шантаж и размещение в СМИ

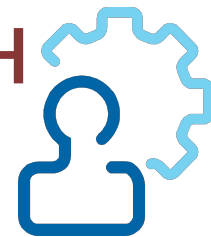


Разглашение данных о работнике

- Различные виды мошенничества
- Рассылка каталогов, буклетов, рекламы



Обязанности операторов ПДн



знать принципы обработки персональных данных

Принимать меры для защиты персональных данных

не раскрывать и не распространять данные без согласия



Принципы обработки ПДн





Как работать с персональными данными?

Начинать следует с выполнения требований Роскомнадзора по юридическому оформлению обработки персональных данных.

Действовать будем по алгоритму.



Этапы по внедрению системы защиты ПДн

1

- Создание приказа о начале работ по созданию системы защиты персональных данных

2

- Сбор и анализ информации

3

- Направление уведомления в Роскомнадзор

4

- Разработка документов для субъектов ПДн

5

- Внедрение системы защиты ПДн

6

- Определение технических средств защиты ПДн

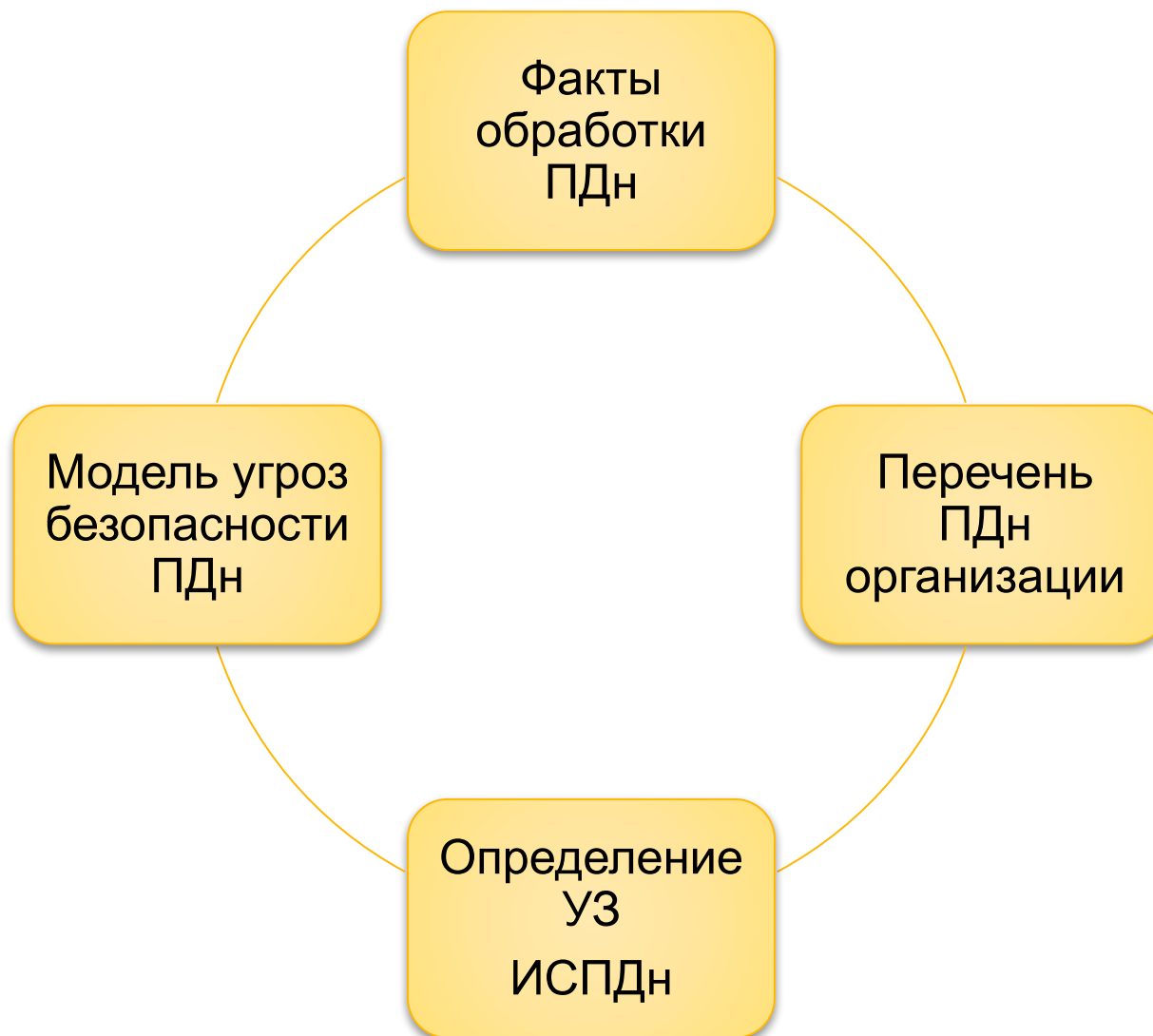
1 Этап. Создание приказа о начале работ по созданию системы защиты персональных данных

«Об организации работ по обеспечению безопасности ПДн»



комиссия по организации работы по защите ПДн

2 Этап. Обследование организации



Примеры использования ПДн

ФИО и
Организация
или должность

Указание на сайте
компании

Указание на двери
кабинета

Для публичного
поздравления с
днем рождения

Указание на пропуске

Паспорт

Кадровые документы

Внесение в бухгалтерские
информационные
системы

Ближайшие
родственники

Для возможной связи в
чрезвычайных случаях

Для предоставления
льгот и гарантий

Адрес

Для отправки
официальных
уведомлений

Знание
языков

Для включения в
кадровый резерв



2 Этап. Обследование организации



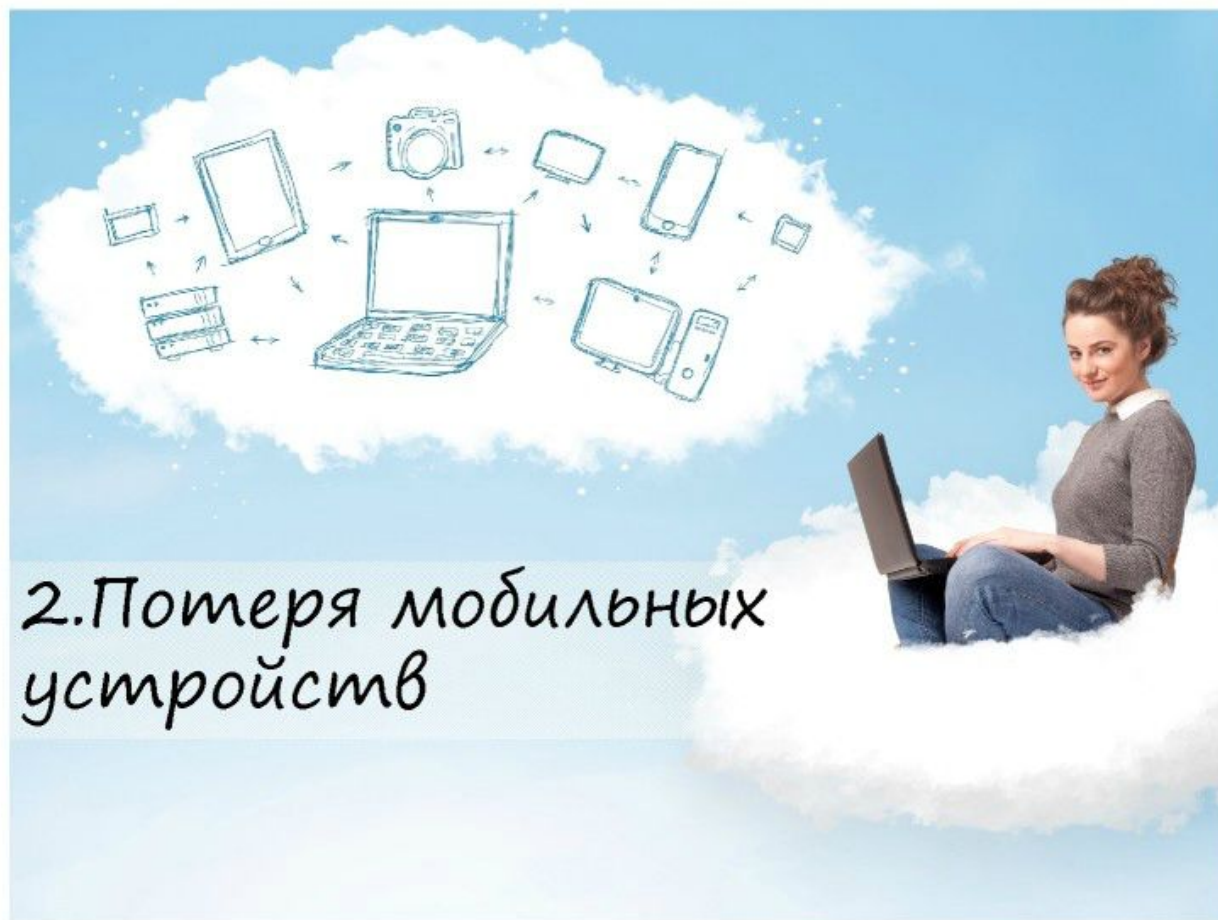
2 Этап. Обследование организации (10 самых распространённых ошибок)



1. Потеря съёмных
носителей



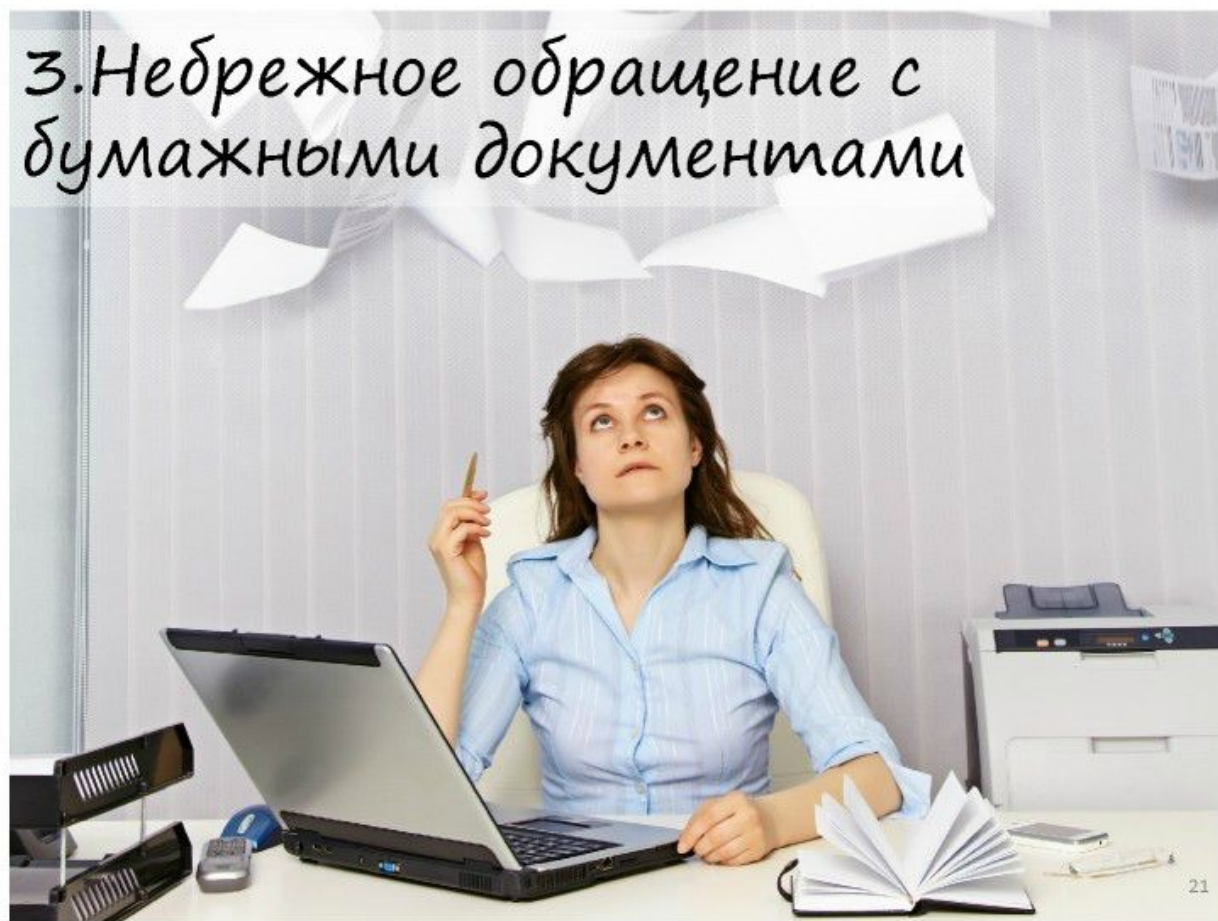
2 Этап. Обследование организации (10 самых распространённых ошибок)



2. Потеря мобильных устройств



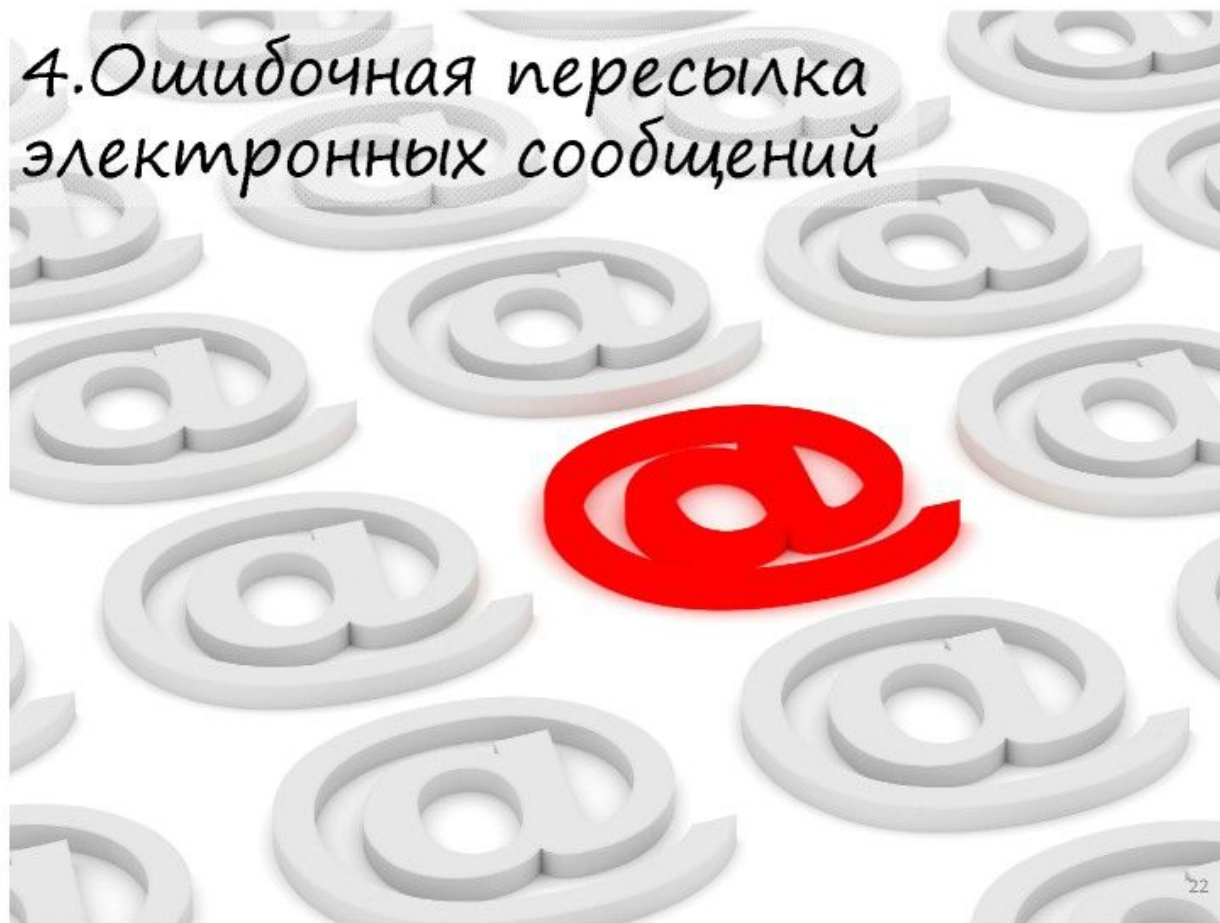
2 Этап. Обследование организации (10 самых распространённых ошибок)



21

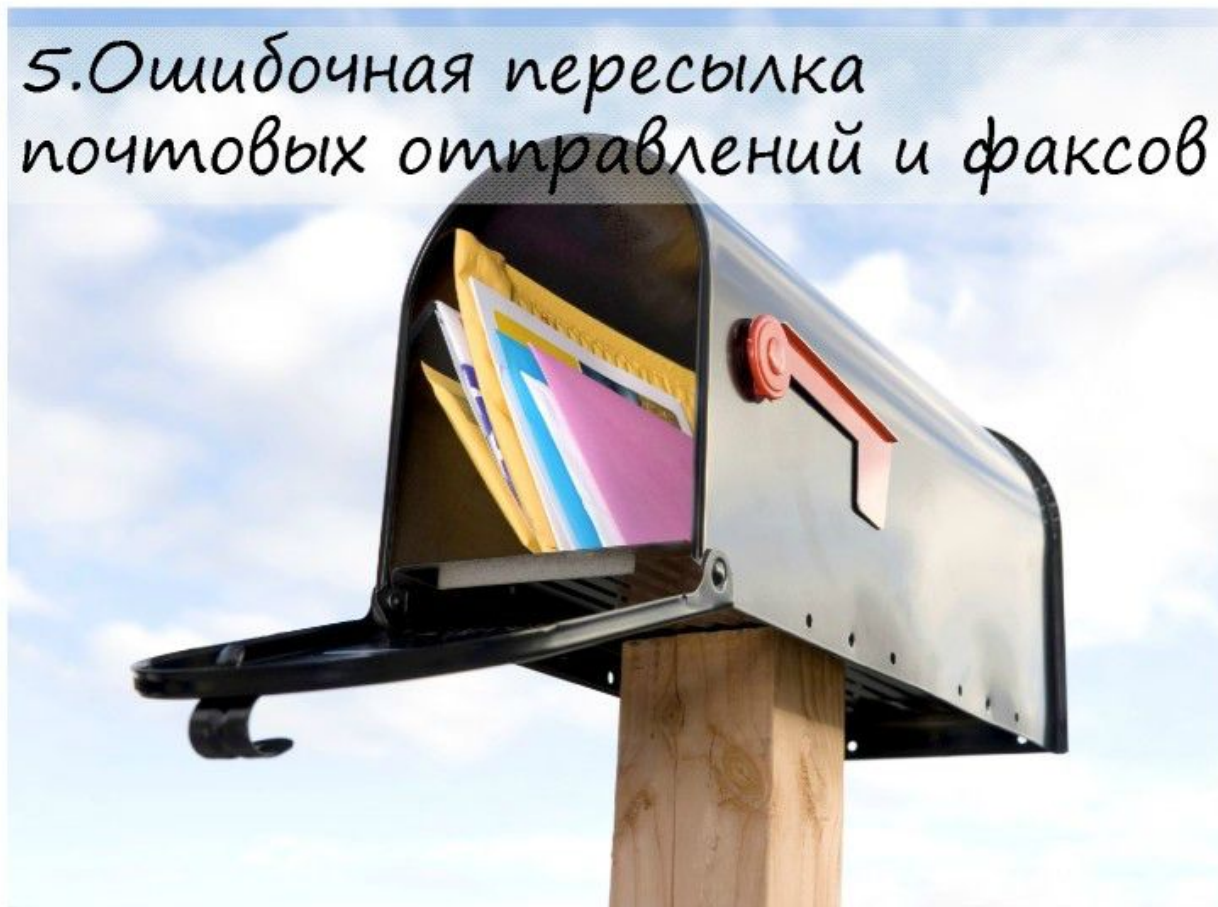


2 Этап. Обследование организации (10 самых распространённых ошибок)



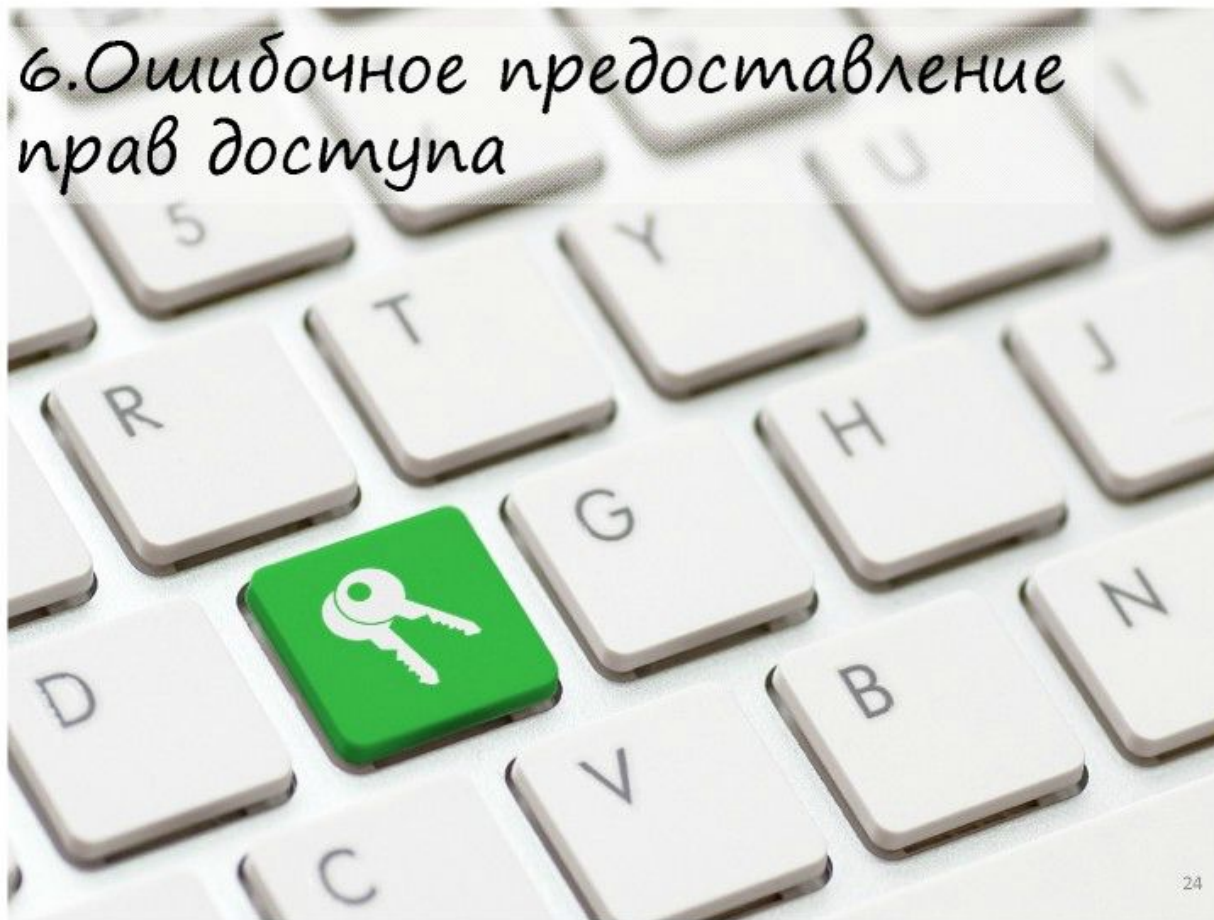
2 Этап. Обследование организации (10 самых распространённых ошибок)

5. Ошибочная пересылка
почтовых отправлений и факсов



2 Этап. Обследование организации (10 самых распространённых ошибок)

*6. Ошибочное предоставление
прав доступа*



24



2 Этап. Обследование организации (10 самых распространённых ошибок)



2 Этап. Обследование организации (10 самых распространённых ошибок)

8. Небрежная утилизация оборудования



26



2 Этап. Обследование организации (10 самых распространённых ошибок)

9. Передача на техническое обслуживание 3М лицам



27



2 Этап. Обследование организации (10 самых распространённых ошибок)

10. Нарушение политики ИБ
по чужой просьбе или указанию



2 Этап. Обследование организации Где содержатся ПДн

Использование данных о
сотруднике при кадровом
учете



Командировки
сотрудников



Перевод заработной
платы работников через
банк



Визитные карточки



2 Этап. Обследование организации. Обработка ПДн без использования средств автоматизации Обработка типовых форм

Издательство

Получатель: ООО "Газпром межрегионгаз Кострома" 157940, г.Красное, ул.Советская, д.20, 4431017834 р/с 4070201053001214111 в Костромском ОДБ №40 БИК: 04380923 к/с 3070181030000000023

ООО "Газпром межрегионгаз Кострома"
Лицевой счет Плательщик

Адрес:
К оплате за **Август 2011г.** **59 руб. 84 коп.**
Показание по счетчику **1.948** новые _____

Квитанция

ООО "Газпром межрегионгаз Кострома"
Красновольский пункт, 157940, г.Красное, ул.Советская, д.20
Лицевой счет Плательщик

Адрес:
К оплате за **Август 2011г.** **59 руб. 84 коп.**

Вид потребления Цена Норматив Характеристики абонента:
Плата 4,07 руб/м³ - Зарегистрировано: 2 чел.
Размер общей площади: 44,5 м² Плата

Последняя дата оплаты 22.09.2011

Наименование	Долг на 01.08.2011	Наислано	Перерасчет	Плата	Оплачено	К оплате
01 за природный газ	44,77	48,84	0,00	0,00	44,77	48,84
15 Техническое обслуживание БДГО	11,00	11,00	-	-	11,00	11,00
Итого	-	59,84	0,00	0,00	55,77	59,84

Оплату произведите в срок до 25.09.2011г.

Справки по заключению договора БДГО чел. (49432) 2-21-39; (4942) 49-11-29, 49-11-71, по техническому обслуживанию оборудования чел. (49432) 2-21-39, по заключению ремонту чел. (49432) 2-21-39.

Уважаемый абонент! В целях исполнения договора поставки природного газа для обеспечения коммунально-бытовых нужд и организации взаимодействия ООО «Газпром межрегионгаз Кострома» с органами социальной защиты населения по вопросу предоставления гражданам мер социальной поддержки по оплате газа убедительно просим Вас дать Согласие на обработку персональных данных в соответствии с Федеральным Законом от 27.07.2006 №152-ФЗ «О персональных данных», обращая Ваше внимание на обязательность заполнения всех полей Согласия на обработку персональных данных.

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

г. _____ « _____ 20__ г.

Я, _____ (фамилия, имя, отчество полностью) _____ серия _____ № _____ выдан _____ (вид документа, удостоверяющий личность, кем и когда выдан)

проживающий(ая) по адресу _____

даю свое согласие ООО «Газпром межрегионгаз Кострома» (далее-Поставщик), юридический адрес: г. Кострома, ул. Лесная, д. 37, на обработку в период действия договора поставки газа для обеспечения коммунально-бытовых нужд граждан (далее - договор), включая сбор, систематизацию, накопление, хранение, передачу, уточнение (обновление, изменение), использование моих персональных данных (фамилия, имени, отчества, пола, даты и места рождения, места жительства/регистрации, паспортных данных, номера лицевого счета (договора), права собственности/закладения жилая поквартирная, объема газопотребления, сведений об оплате и задолженности за потребленный природный газ, мер социальной поддержки (дата, серия и номер документа на право получения), общей суммы начислений и размера льготной скидки, количества совместно проживающих членов семьи, параметров заоснащения жилого помещения и иной информации с целью использования моих персональных данных для исполнения договора поставки газа для обеспечения коммунально-бытовых нужд граждан (в том числе предоставления мер социальной поддержки по оплате природного газа), а также передачи силами поставщика, либо оператора почтовой связи, либо кредитных и иных организаций, с которыми Поставщиком заключены соответствующие договоры, квитанций на оплату природного газа, претензий и уведомлений в открытом виде, а равно при привлечении третьих лиц к организации и осуществлению налогового, бухгалтерского, управленческого, абонентского и иных видов учета Поставщика в указанных целях.

Настоящее Согласие может быть отозвано мною в любое время, путем уведомления об этом оператора персональных данных ООО «Газпром межрегионгаз Кострома» в письменном виде. Срок действия согласия в данном случае считается окончанным с момента получения данного уведомления оператором персональных данных ООО «Газпром межрегионгаз Кострома».

С момента подписания настоящего Согласия оно считается данным в соответствии со ст.9 Федерального Закона от 27.07.2006 №152-ФЗ «О персональных данных»

Подпись: _____

Типовая форма
должна
предусматривать
поле, в котором
субъект ПДн
может поставить
отметку о своём
согласии на
обработку ПДн,
осуществляемую
без использования
средств
автоматизации



Этап 2. Обследование организации. Разработка модели угроз безопасности ПДн

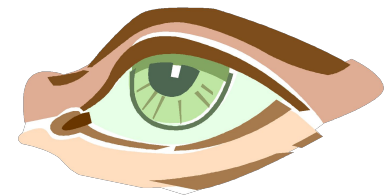


Категории ПДн

Биометрические персональные данные – физиологические и биологические особенности человека, на основании которых можно установить его личность

и используются оператором для установления личности.

Примеры: Фото, отпечатки пальцев, изображение сетчатки глаза



Соответствуют классу 3 классификации по постановлению правительства РФ 781 от 17.11.07

Категории ПДн

Специальные персональные данные – закрытый перечень приведённый в статье 10 содержащий:

- расу,
- национальность,
- политические взгляды,
- религию,
- философию,
- состояние здоровья,
- интимную жизнь



Соответствуют классу 1 классификации по постановлению правительства РФ 781 от 17.11.07

Категории ПДн

Персональные данные, сделанные **общедоступными** субъектом персональных данных

- Список ФИО на сайте
- Доска почёта
- Статистические данные



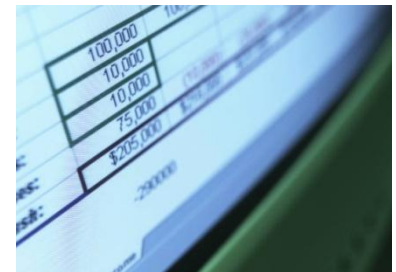
Соответствуют классу 4 классификации по постановлению правительства РФ 781 от 17.11.07



Категории ПДн

Иные персональные данные – не вошедшие в первые три категории

- Паспортные данные (кроме фото)
- Размер зарплаты
- Занимаемая должность
- Бухгалтерские \ кадровые информационные системы
- Системы по учету услуг (информационная система автомойки, салона красоты и тд)



Соответствуют классу 2 классификации по постановлению правительства РФ 781 от 17.11.07

Уровни защищенности ИСПДн. Обработываемые ПДн принадлежат сотрудникам компании оператора

Тип угрозы / тип ПДн	1 тип угроз	2 тип угроз	3 тип угроз
Биометрические ПДн (фото,отпечатки пальцев)	УЗ 1	УЗ 2	УЗ 3
Специальные ПДн (состояние здоровья)	УЗ 1	УЗ 2	УЗ 3
Иные ПДн (паспорт, должность)	УЗ 1	УЗ 3	УЗ 4
Общедоступные ПДн (сайт, доска почёта)	УЗ 2	УЗ 3	УЗ 4



Меры защиты

Уровень защищенности	Необходимый состав применяемых мер для обеспечения уровня защищенности
УЗ 4	<ul style="list-style-type: none">• Ограничен доступ в помещения, из которых можно подключиться к ИСПДн;• Контролируются носители ПДн;• При необходимости применяются сертифицированные средства защиты информации;• Документально утвержден перечень лиц, имеющих доступ к ИСПДн
УЗ 3	<ul style="list-style-type: none">• Включает требования 4 уровня защищенности;• Назначен работник, ответственный за обеспечение безопасности ПДн
УЗ 2	<ul style="list-style-type: none">• Включает требования 3 и 4 уровней защищенности;• Ограничен доступ к электронному журналу сообщений
УЗ 1	<ul style="list-style-type: none">• Включает требования остальных уровней;• В электронном журнале безопасности автоматически фиксируется изменение прав доступа к ИСПДн;• Безопасность ПДн в ИСПДн контролирует структурное подразделение (НЕ отдельный сотрудник)



Этап 3. Направление уведомления в Роскомнадзор

Можно обрабатывать без уведомления:

данные сотрудников

данные по договорным отношениям с юр. лицами

данные , которые являются общедоступными

данные, которые обрабатываются без использования средств автоматизации



Этап 3. Направление уведомления в Роскомнадзор



Внимание! Уведомления в электронном виде недостаточно, обязательна отправка бумажного варианта по почте

Всем, кто отправил уведомление до 2011 г. Необходимо отправить повторно



Этап 4. Разработка документов по субъектам ПДн. Общие локальные нормативные акты

1. Общий документ, определяющий политику в отношении обработки ПДн (положение о персональных данных).
2. Список лиц, обрабатывающие ПДн.
3. Приказ о назначении сотрудника, ответственного за организацию обработки ПДн.
4. Положение о правовых, организационных и технических мерах защиты ПДн.
5. Локальный акт, устанавливающий процедуры, направленные на предотвращение и выявление нарушения законодательства в сфере защиты ПДн.



Этап 4. Разработка документов по субъектам ПДн



«Согласие на обработку ПДн»



«Отзыв согласия на обработку ПДн»



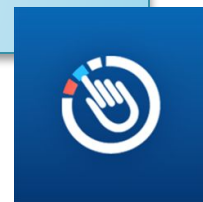
Этап 4. Согласие на обработку ПДн



Не требуется получать согласие на обработку ПДн, если обработка необходима (152-ФЗ, статья 6.1)



Предоставление госуслуг



Для осуществления законной деятельности журналиста или СМИ

Исполнение законодательства, международных договоров РФ и решений суда

Случаи обработки ПДн без согласия

ПДн общедоступны или подлежат обязательному раскрытию

В статистических целях (ПДн обезличены)

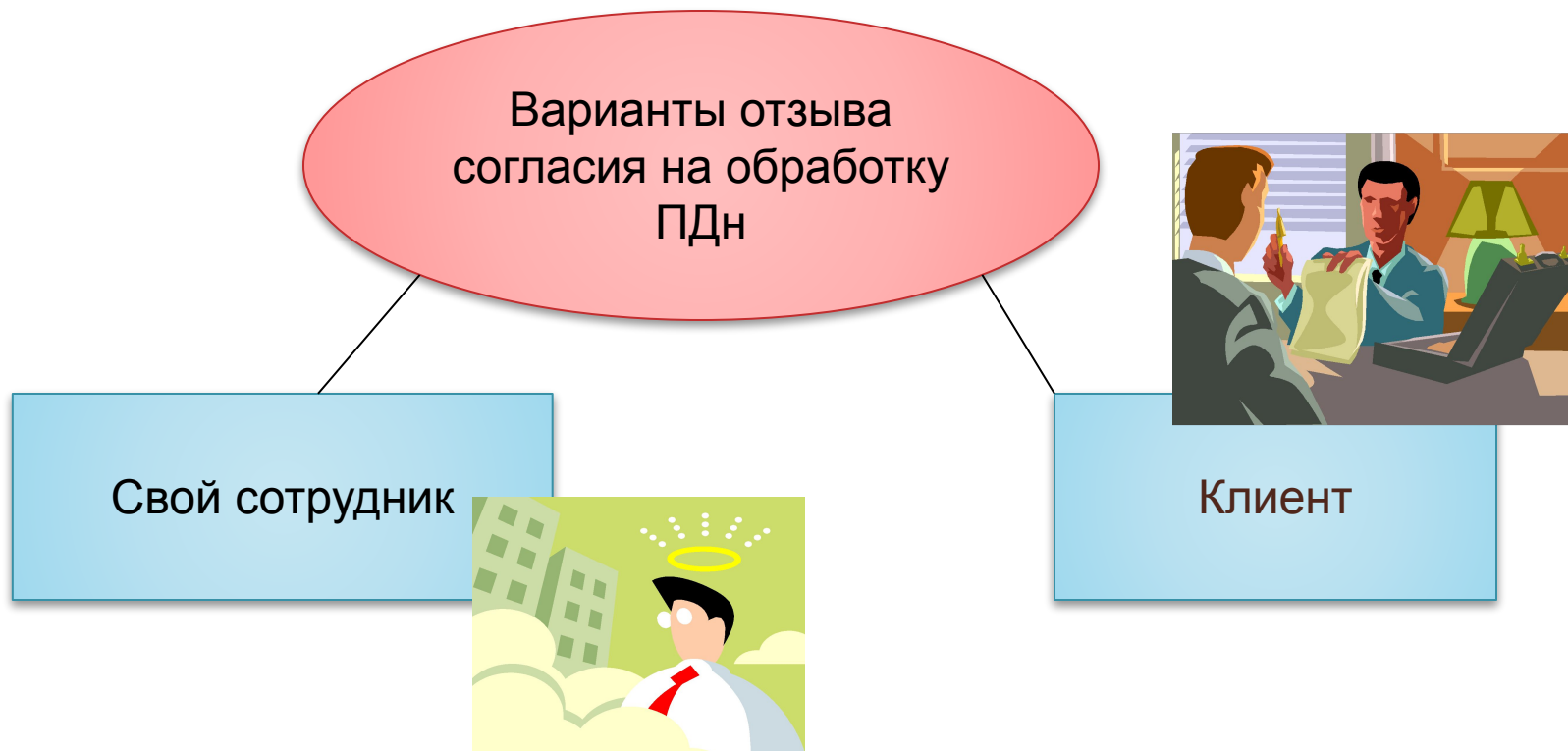
Исполнение договоров



Защита жизни и здоровья (если согласие получить невозможно)



Этап 4. Отзыв согласия на обработку ПДн



Допускается продолжение обработки персональных данных, если это требуется для исполнения Федерального законодательства.



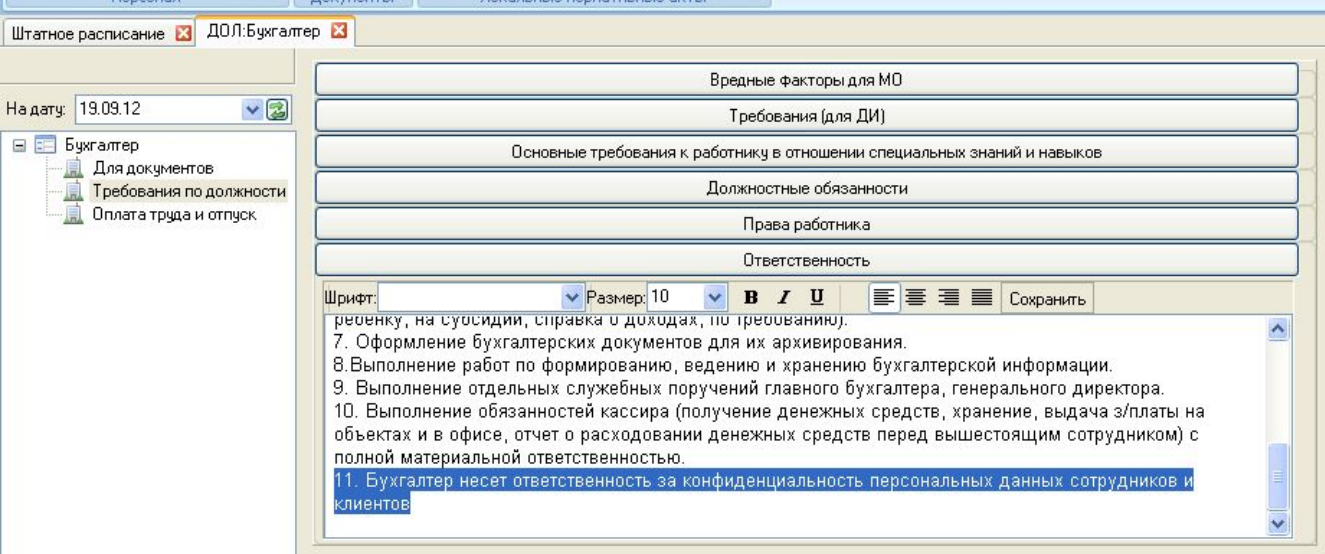
Этап 5. Внедрение системы защиты ПДн

составление, утверждение и уведомление перечня лиц, допускающихся к обработке ПДн

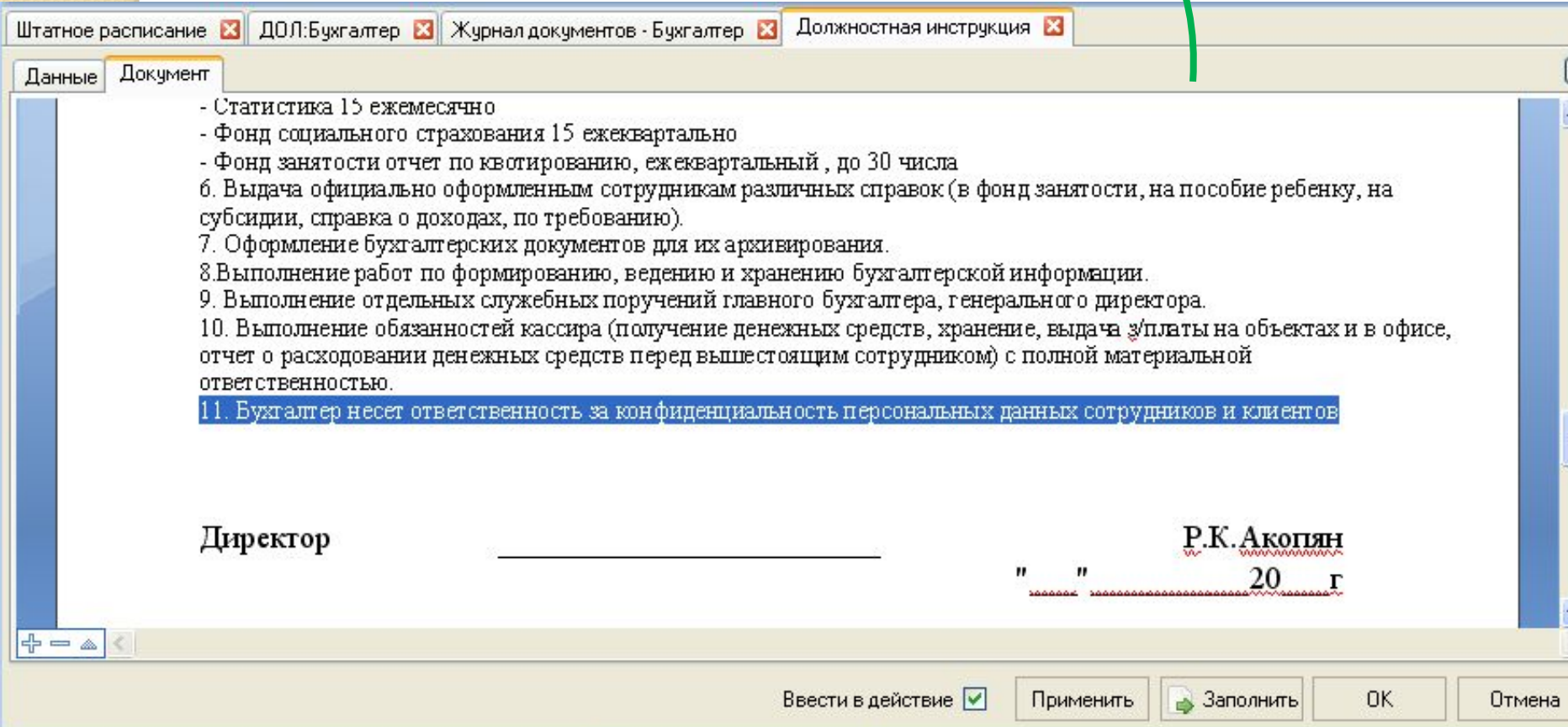
составление и утверждение перечня обрабатываемых ПДн

составление и утверждение положения об обработке и защите ПДн на предприятии, включающего лист ознакомления сотрудников с данным положением





Кадр.ИН



На дату: 19.09.12

- Селицкий Виталий Анварович
- Паспортные, общие данные
- Воинский учет
- Семья
- Документы
- Стаж
- Справки
- Характеристика
- Образование
- Звания, степени, награжде
- Квалификационная категор
- Переподготовка

- Удалить объект
- Обновить данные
- Документы
- Создать документ
- Создать документ по всем

Основная часть

Наименование: Селицкий Виталий Анварович

Должность: ЗАО Арктика\планово-технически

Наименование организации: ЗАО "Арктика"

Вид трудового договора: по основной работе

Ставка: Оклад

Активация

Активировать

Дата принятия: 05.07

Прием на работу

Просмотр

Просмотр

Просмотр

Лист ознакомления

Трудовой договор

Приказ о приеме на работу

Оформить документ

Дата документа: 19.09.12

- Активация ШР
- Документы по организации
- Акты, распоряжения, отстранения
- Договор ГПХ
- Документы мед. осмотры, мед. заключения
- Документы по воинскому учету
- Должностные инструкции
 - Должностная инструкция (сотрудник)
 - Уведомление - изменение должн. инстр.
- Командировка
- Приказы, акты по организации
- Справки
- Уведомления, требования
- Ученический договор
- Документы по работникам

УВЕДОМЛЕНИЕ

ОБ ИЗМЕНЕНИИ ОПРЕДЕЛЕННЫХ СТОРОНАМИ УСЛОВИЙ ТРУДОВОГО ДОГОВОРА

Уважаемая(ый) **Виталий Анварович!**

Уведомляем вас, что в связи с внесением изменений в законодательных условий... (текст уведомления)

УВЕДОМЛЕНИЕ

18.09.12 г.

Архангельск

об изменении определенных сторонами условий трудового договора

Уважаемая(ый) **Виталий Анварович!**

В связи с внесением изменений в Федеральный закон № 152-ФЗ от 25.07.2011 и необходимостью приведения локальных нормативных актов в соответствие с действующим законодательством, уведомляем Вас, что IV "Ответственность работника" раздел должностной инструкции бухгалтера от 01.03.2000 № 11 будет дополнен пунктом следующего содержания:

" - нести ответственность за персональные данные сотрудников и клиентов".

В случае не согласия работать в новых условиях, Вам будет предложена другая имеющаяся работа. В случае отказа от предложенной работы, либо отсутствия вакансий, трудовой договор с Вами будет расторгнут в соответствии с пунктом 7 части первой статьи 77 Трудового Кодекса Российской Федерации.

С уведомлением ознакомлена, экземпляр получила. _____ выполнять должностные обязанности в соответствии с новой должностной инструкцией **11-ДИ**, утвержденной **19.11.12**

Оформить документ

ПРЕДСТАВИТЕЛЬ РАБОДАТЕЛЯ

ПОДПИСЬ

ОК

Отмена



ПРАВОНАРУШЕНИЯ СВЯЗАННЫХ С ПДН

1

- обработка ПДн с нарушением требований к составу сведений, включаемых в письменное согласие субъекта ПДн на обработку его персональных данных

2

- обработка ПДн без согласия их субъекта

3

- обработка ПДн, входящих в специальные категории, в случаях, которые не предусмотрены законодательством

4

- невыполнение оператором обязанности опубликования его политики в отношении обработки ПДн и сведений о реализуемых требованиях к защите ПДн

ПРАВОНАРУШЕНИЯ СВЯЗАННЫХ С ПДН

5

- невыполнение оператором обязанности предоставления субъекту ПДн информации, касающейся обработки его ПДн

6

- невыполнение оператором требований субъекта ПДн или уполномоченного органа по защите прав субъектов ПДн об уточнении ПДн, их блокировании либо уничтожении

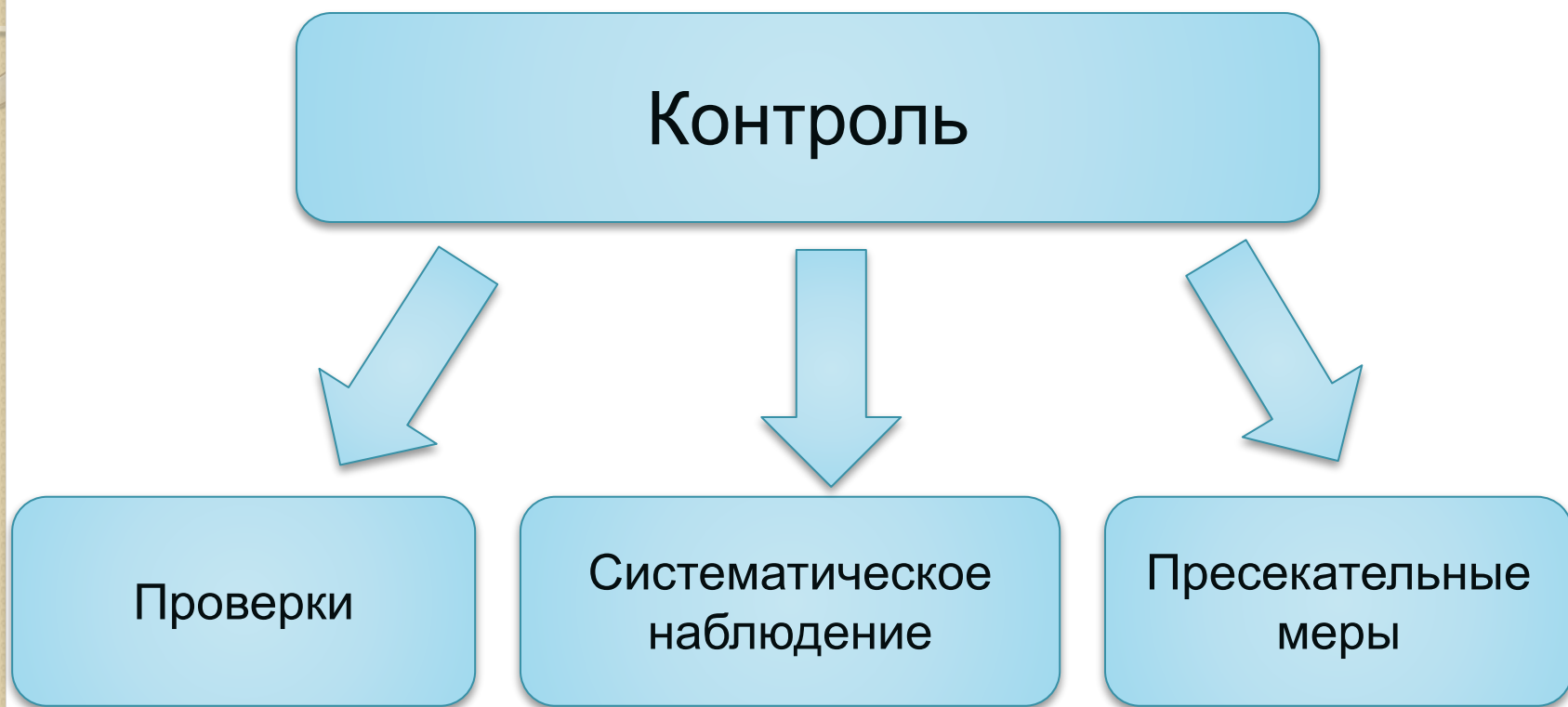
7

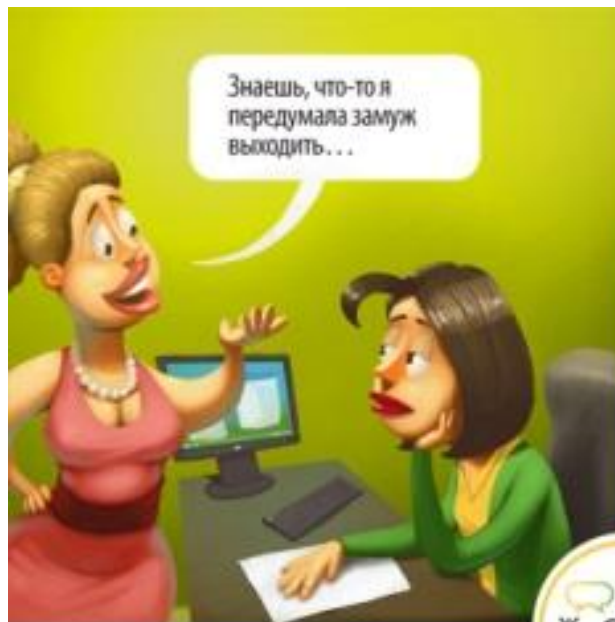
- при обработке ПДн без использования средств автоматизации невыполнение оператором обязанности обеспечения сохранности ПДн

8

- невыполнение оператором, являющимся государственным или муниципальным органом, обязанности обезличивания ПДн, несоблюдение установленных требований и методов обезличивания ПДн

Контроль Роскомнадзора





Х Система
Кадры

