softline®
Мы всё сможем
30 лет в ИТ

Трансформация.
Успешная. Цифровая. Защищенная.

Самостоятельное выполнение требований 152-ФЗ. Первые шаги

Гострый Максим

Системный архитектор
направления безопасности
промышленных предприятий

Что такое Закон № 152-ФЗ и зачем это нужно?

Вступил в силу с 1 июля 2011 и все ещё актуален, нормативно-правовая база постоянно совершенствуется

Является обязательным требованием для всех Операторов ПДн

Основной регулятор – Роскомнадзор (РКН)

Оператор обязан обеспечить реализацию мер в соответствии с нормативными правовыми актами

Необходимо обеспечить наличие актуального комплекта ОРД по обработке и защите ПДн, выстроить процессы, определить ответственных лиц

Базы данных ПДн, обязательно должны быть локализованы на территории РФ

С чего начать?

Определение ответственных лиц

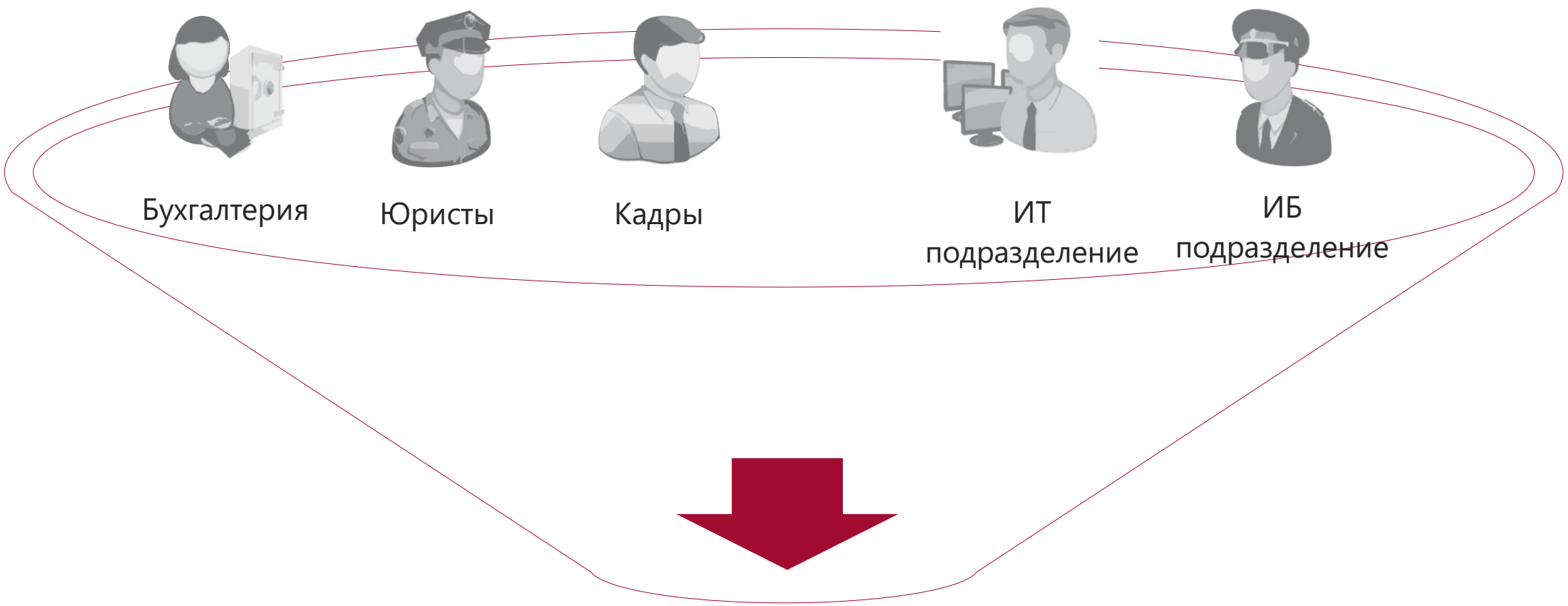
- В соответствии с ч.1 ст.22.1 Федерального закона №152-ФЗ оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки ПДн, которое должно, как минимум:

❑ осуществлять внутренний контроль за соблюдением законодательства в области обеспечения безопасности ПДн;

❑ доводить до работников оператора информацию об изменении законодательства, норм и правил обработки ПДн;

❑ организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей.

Формирование комиссии



Выявление процессов обработки ПДн

Пример собранных данных

№	ВОПРОСЫ	ОТВЕТЫ
1	Опишите процесс, в котором используются ПДн (этапы обработки персональных данных)	Каровый учет
2	Чьи и какие ПДн участвуют в процессе? (например, работник – ФИО, должность, номер телефона)	Сотрудники: • ФИО • Должность • Дата рождения • ИНН • СНИЛС • Паспортные данные
3	При помощи каких информационных систем осуществляется процесс обработки ПДн?	1С: ЗУП
4	Чьи и какие ПДн обрабатываются в ИСПДн?	1С: ЗУП Сотрудники: • ФИО; • Должность; • Дата рождения; • ИНН • СНИЛС • Паспортные данные

№	ВОПРОСЫ	ОТВЕТЫ
5	Перечень действий с ПДн	сбор; запись; систематизация; накопление; хранение; уточнение (обновление, изменение); использование; передача (предоставление, доступ); блокирование; удаление; уничтожение
6	Перечень лиц / структурных подразделений, задействованных в процессе	• Отдел кадров
7	Передача третьим лицам	Пенсионный фонд
8	Трансграничная передача	Да, Франция Сотрудники: • ФИО • Должность

Уточнение архитектуры ИСПДн

ИСПДн

Кто обслуживает и кто использует?

Состав ПДн, объем и категория

Взаимодействия с другими ИСПДн

Пример собранных данных

№	ВОПРОСЫ	ОТВЕТЫ
1	Наименование информационной системы персональных данных (ИСПДн)	1С: Зарплата и управление персоналом
2	Назначение системы	Ведение кадрового учета, Исполнение договоров
3	Законное основание использования (Аренда (IaaS/PaaS/SaaS) / Право собственности)	Право собственности
4	Разработчик системы	1С
5	Какими структурными подразделениями и (или) внешними организациями осуществляются: — администрирование ИСПДн; — доработка и поддержка ИСПДн.	Администрирование – Отдел информационных технологий Доработка и поддержка – ООО «Пиксель»
6	Какими структурными подразделениями используется ИСПДн?	Отдел персонала, Бухгалтерия, Отдел продаж

№	ВОПРОСЫ	ОТВЕТЫ
7	Перечень лиц (должностей), имеющих доступ и непосредственно допущенных к работе с ПДн субъектов ПДн (в электронной форме, на материальных носителях)	<u>В электронной форме:</u> Отдел персонала: руководитель отдела кадров, сотрудник отдела кадров, юрист Бухгалтерия: главный бухгалтер, стажер и т.д. <u>В бумажной форме:</u> Отдел персонала: руководитель отдела кадров (Если сотрудник может вывести ПДн из ИСПДн, например, при помощи печати, отнести к обеим формам доступа)
8	Категории субъектов, персональные данные которых обрабатываются в системе (сотрудники, клиенты и т.д.)	Работник Контрагент
9	Количество субъектов, персональные данные которых обрабатываются в системе (менее 100 000, более 100 000)	Работники менее 100 000 Субъекты, не являющиеся работниками более 100 000
10	Состав полей системы, содержащих персональные данные (список персональных данных, обрабатываемых в системе) по каждой категории субъектов ПДн, указанных в п. 9	Работник: ФИО, паспортные данные и тд. Контрагент: ФИО, должность, организация и т.д.
11	Источники персональных данных для системы (указать наименования анкет, заявлений, других систем, из которых информация заносится в систему)	Трудовой договор
12	Взаимодействие с внешними системами	Да (перечислить системы сторонних организаций и способы взаимодействия) / Нет
13	Взаимодействие с внутренними системами	Если есть выгрузка / загрузка данных в другие системы Общества
14	Территориальное расположение баз данных, содержащих ПДн	Указать страну, где происходит хранение ПДн

Технические и организационные меры

Постановление Правительства от 1 ноября 2012 г. № 1119

Регламентирует:

- Определение уровня защищенности ПДн в ИСПДн
- Организацию режима обеспечения безопасности помещений
- Обеспечение сохранности носителей ПДн
- Определение перечня лиц, доступ которых к ПДН, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей
- Использование СЗИ, прошедших процедуру оценки соответствия требованиям законодательства РФ
- Назначение ответственного за обеспечение безопасности ПДН в ИСПДн (от УЗ-3 и выше)

Категории ПДн		Специальные			Биометрические	Иные			Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		более 100 тыс.	менее 100 тыс.			более 100 тыс.	менее 100 тыс.		более 100 тыс.	менее 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

Постановление Правительства от 15 сентября 2008 г. № 687

Регламентирует:

Обработку ПДн без использования средств автоматизации

Фиксацию ПДн на разных материальных носителях цели обработки которых заведомо не совместимы

Уведомление о факте обработки должностными лицами ПДн

Требования к типовым формам, содержащим ПДн

Определение перечня лиц, допущенных к обработке ПДн

Приказ ФСТЭК России от 18 февраля 2013 г. № 21

Регламентирует:

- Применение мер по обеспечению безопасности персональных данных
- Оценку эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных

Приказ ФСБ России от 10 июля 2014 г. №378

Регламентирует:

обработку в ИСПДн с использованием средств криптографической защиты информации (СКЗИ)
организацию режима обеспечения безопасности помещений
обеспечение сохранности носителей ПДн
определение перечня лиц, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим в связи с выполнением ими трудовых обязанностей
использование СЗИ, прошедших процедуру оценки соответствия требованиям законодательства РФ

Политика обработки ПДн

Политика обработки ПДн

Что важно?!

- Обеспечить доступ к Политике обработки ПДн
- Актуализировать при изменениях

Ключевые изменения 152-ФЗ от 14.07.2022 № 266-ФЗ

Обязанность лица, обрабатывающего обработку ПДн по поручению оператора, соблюдать конфиденциальность ПДн, обеспечивать выполнение обязанностей, предусмотренных 152-ФЗ

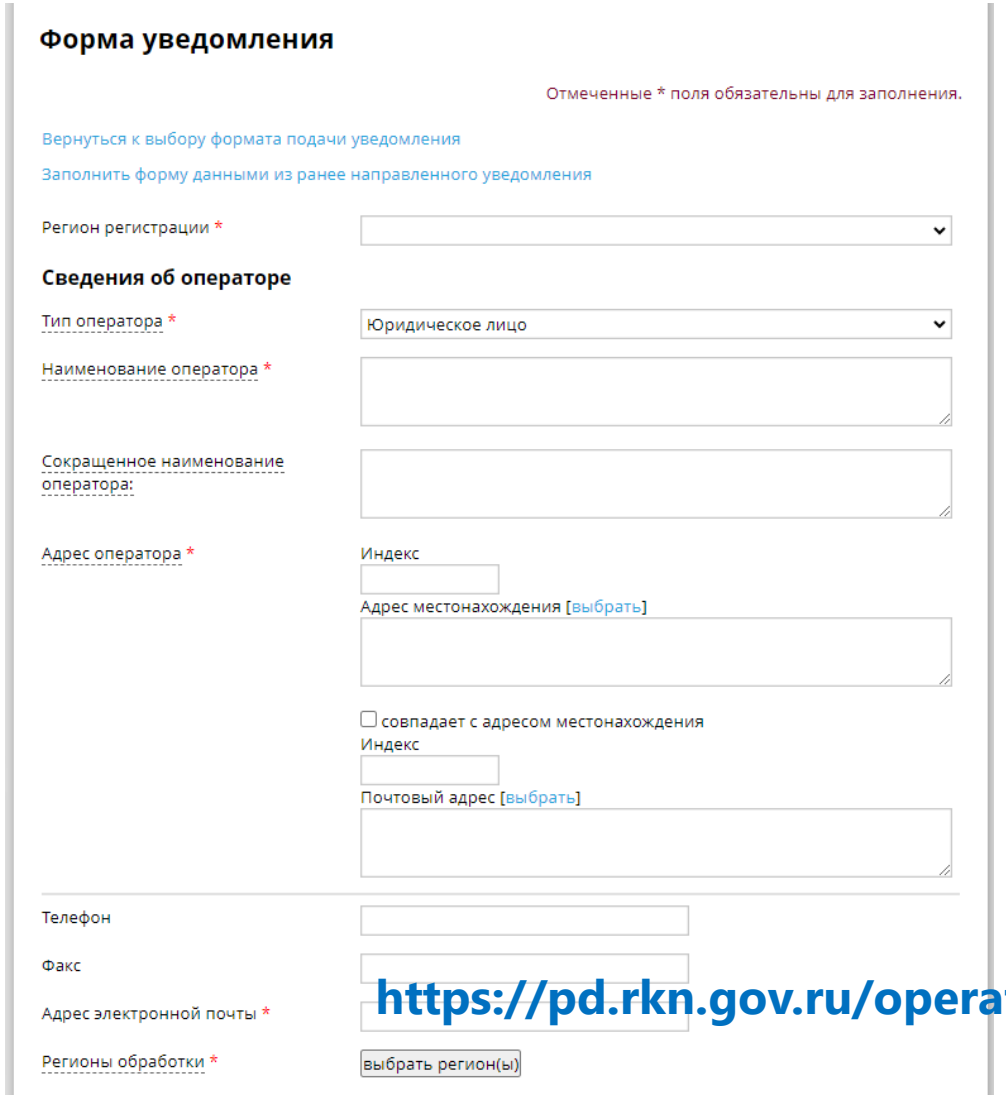
Операторы до начала трансграничной передачи ПДн обязаны уведомить о ней РКН уведомлением

Изменен формат уведомления РКН о факте обработки Оператором ПДн

Оператор обязан уведомлять РКН и ФСБ о неправомерной или случайной передачи ПДн, повлекшей нарушение прав субъектов ПДн, в течение 72 ч. направить результаты внутреннего расследования: в случае если оператор ПДн является субъектом КИИ – в ГосСОПКА, если не является субъектом КИИ – на портал Роскомнадзора

Оператор теперь обязан обеспечивать взаимодействие с ГосСОПКА

Уведомление об обработке ПДн



Форма уведомления

Отмеченные * поля обязательны для заполнения.

Вернуться к выбору формата подачи уведомления

Заполнить форму данными из ранее направленного уведомления

Регион регистрации *

Сведения об операторе

Тип оператора * Юридическое лицо

Наименование оператора *

Сокращенное наименование оператора:

Адрес оператора * Индекс

Адрес местонахождения [выбрать]

совпадает с адресом местонахождения

Индекс

Почтовый адрес [выбрать]

Телефон

Факс

Адрес электронной почты *

Регионы обработки * выбрать регион(ы)

https://pd.rkn.gov.ru/operators-registry/notification/form/

Уведомление о трансграничной обработке ПДн

УВЕДОМЛЕНИЕ
о намерении осуществлять трансграничную передачу ПД

Наименование оператора: ООО «Оператор»

ИНН: 771234567890

Адрес оператора: 123456, г. Москва, ул. Комсомольская, д. 1, оф. 1

Наличие в реестре операторов: да

Регион регистрации: Москва;

Адрес электронной почты: pochta@yandex.ru

ФИО лица, ответственного за организацию обработки персональных данных: Иванов Михаил Владимирович

Номер контактного телефона, почтовые адреса и адреса электронной почты: +79999999999, 123456, г. Москва, ул. Комсомольская, д. 1, оф. 1 pochta@yandex.ru

Цели трансграничной передачи:

1: Цель трансграничной передачи: Заключение договора об оказании информационно-консультативных услуг

Правовое основание трансграничной передачи:

обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем

Категории передаваемых персональных данных:

Персональные данные: фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; пол; адрес электронной почты; номер телефона; гражданство; данные документа, удостоверяющего личность за пределами Российской Федерации; профессия; должность;

Категории субъектов ПД, персональные данные которых передаются: Работники;

Перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных:
Армения; Белоруссия; Сербия; Турция;

Дата окончания проведения оценки: 10.02.2023

https://pd.rkn.gov.ru/cross-border-transmission/form2/

Какой итог проведенных работ?

- ✓ Назначены ответственный и комиссия
- ✓ Сформированы перечни ПДн, ИСПДн
- ✓ Определен и зафиксирован перечень лиц, допущенных к обработке ПДн
- ✓ Разработана и опубликована политика обработки ПДн
- ✓ Подано уведомление об обработке ПДн
- ✓ Определены уровни защищенности ИСПДн
- ✓ Определен базовый перечень необходимых мероприятий для выполнения требований по безопасности ПДн

Что делать дальше?

Что еще нужно разработать?

- 1. Положение об обработке ПДн
- 2. Положение об обеспечении безопасности ПДн
- 3. Положение о порядке обработки ПДн без использования средств автоматизации.
- 4. Согласия на обработку ПДн
- 5. Регламент контроля обеспечения безопасности ПДн
- 6. Порядок рассмотрения запросов субъектов ПДн и контролирующих органов
- 7. Инструкция пользователя ИСПДн
- 8. Паспорт ИСПДн
- 9. Акт определения уровня защищенности ПДн.
- 10. Акт оценки возможного вреда субъектам ПДн.
- 11. Форма акта уничтожения носителей ПДн
- 12. Приказ об утверждения перечня материальных носителей персональных данных, включая перечень материальных носителей персональных данных.
- 13. Модель угроз безопасности информации.
- 14. Проект по созданию системы защиты ПДн.

Первый блок работ по проекту ЗПДн

Трансформация.
Успешная. Цифровая. Защищенная.

1 Обследование

Результат

1. Перечень процессов обработки ПДн
2. Перечень ИСПДн

2 Деятельность комиссии

Результат

1. Приказ о создании экспертной комиссии

3 Определение УЗ

Результат

1. Акты определения УЗ ПДн
2. Акты оценки вреда субъектам ПДн

4 Моделирование угроз

Результат

1. Модель (модели) угроз безопасности информации

5 Разработка ОРД

Результат

1. Комплект организационно-распорядительной документации

Второй блок работ по проекту ЗПДн

Трансформация.
Успешная. Цифровая. Защищенная.

1 Разработка техзадания

Результат

1. ТЗ на проектирование системы защиты ИСПДн

2 Техническое проектирование

Результат

1. Технический проект или концепция защиты ПДн
2. Комплект рабочей документации

3 Пилотирование

Результат

1. Отчет по пилотированию

4 Поставка СЗИ

Результат

1. Акты приема-передачи

5 Внедрение СЗИ

Результат

1. Программа и методика испытаний СЗИ
2. Акт передачи в опытную (промышленную) эксплуатацию

6 Контроль эффективности принимаемых мер

Результат

1. Отчет по результатам проведенных работ

Немного об ответственности

Актуальные штрафы за нарушения

Статья	Характер нарушения	Минимум	Максимум
13.11 ч.1	Нарушения при обработке ПДн	60 000	100 000
13.11 ч.1.1	Повторное нарушение	100 000	300 000
13.11 ч.2	Обработка без письменного согласия субъекта	30 000	150 000
13.11. ч.2.1	Повторное нарушение	300 000	500 000
13.11. ч.5	Невыполнение требований субъекта об уточнении, блокировании или уничтожении ПДн в установленный срок	50 000	90 000
13.11. ч5.1	Повторное нарушение	300 000	500 000
13.11. ч.8	Нарушения при локализации баз данных на территории РФ	1 000 000	6 000 000
13.11.ч.8.1	Повторное нарушение	6 000 000	18 000 000


softline®
Мы всё сможем
30
лет в ИТ
Трансформация.
Успешная. Цифровая. Защищенная.