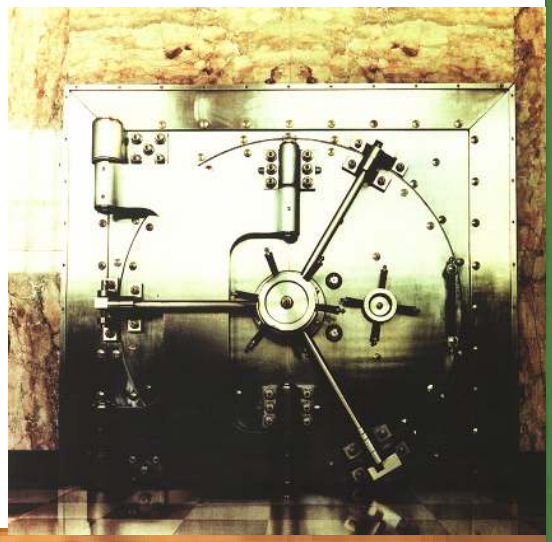
Консалтинговые услуги
в области
информационной
безопасности

Global Trust Solutions

# Практика обеспечения соответствия в области персональных данных


Александр Астахов
GlobalTrust Solutions

Тел.: +7 (495) 651-6617
Факс: +7 (495) 967-7600
Email: info@globaltrust.ru
Web: www.globaltrust.ru

# Содержание

- Понятие персональных данных
- Основные принципы обработки и защиты персональных данных
- Ответственность за нарушения законодательства в области персональных данных
- Основные этапы работ по созданию системы защиты персональных данных
- Варианты решений по защите персональных данных

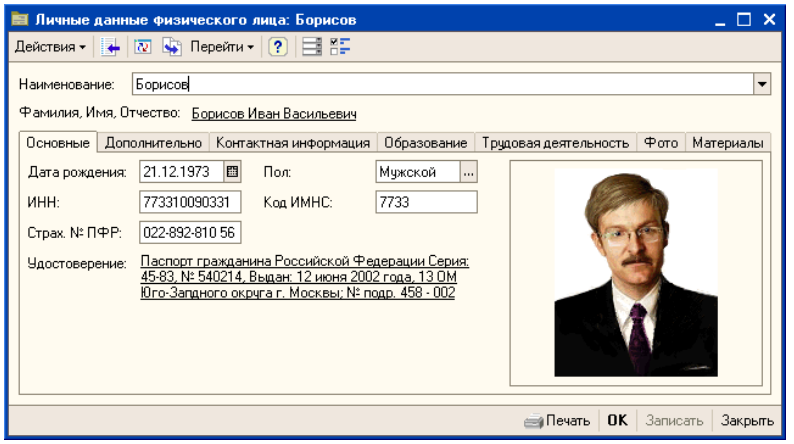
# Почему так сложно обеспечить соответствие ФЗ-152 «О персональных данных»?


- Недостаточно проработан понятийный аппарат (понятие персональных данных, обезличивание, автоматизированная обработка и т.п.)
- Избыток регуляторов и несогласованных нормативных документов, которые постоянно пересматриваются
- Классификация ИСПДн нуждается в уточнении
- Государственная система регулирования отрасли защиты информации (лицензирование и сертификация) плохо работает в коммерческом секторе

# Понятие персональных данных (российское и европейское)

- персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация
- **и включающая в себя любое выражение мнения об инцивидууме и любые признаки намерения оператора данных или любого другого лица в отношении индивидуума**

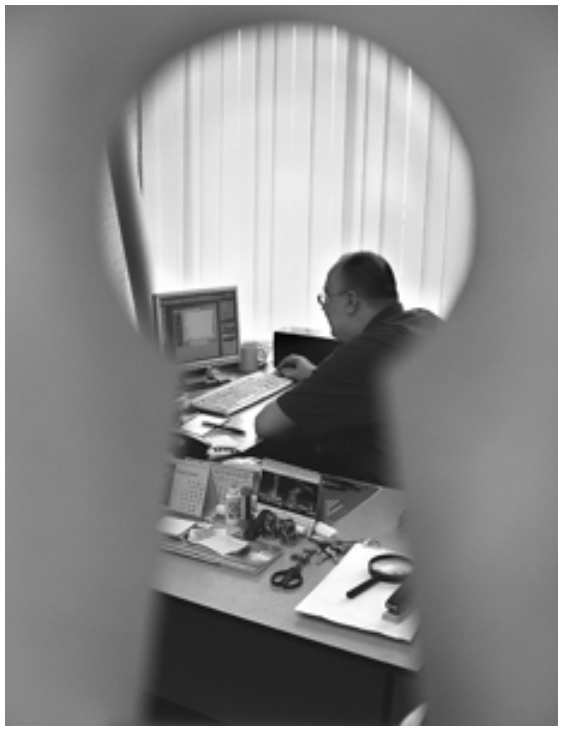
# Вопрос: Что из перечисленного является персональными данными?




1. «Степан Степаныч проживает в Москве на ул. Смольная, д. 10 и работает дворником»
2. «VISA CLASSIC, № 2374 4095 3443 2342, STEPAN STEPANYCH»
3. «Степан Степаныч, моб. телефон 111-1111»
4. «Задолжность за свет по адресу: Москва, ул. Ступина, 1, 15 составляет 23 000 руб.»
5. «небольшой лысеватый человек, проживающий в квартире справа от меня и паркующий свой запорожец у нас под окнами, не платит за квартиру»
6. Журнал регистрации участников семинара в формате: «ФИО, должность, название компании»
7. Фотография участников семинара
8. Записи в ЗАГСе об умерших гражданах

# Вопрос: Имеет ли право работодатель осуществлять мониторинг действий своих сотрудников (ст. 138 УК РФ «вмешательство в частную жизнь»)?

- Просмотр электронной переписки
- Запись сетевой активности и работы в Интернет
- Запись снимков экрана и клавиатурных вводов
- Видеозапись в помещениях
- Запись телефонных разговоров



# Ответ: Имеет право, но ... важна цель и содержание обработки ПДн

**При мониторинге действий сотрудников необходимо обеспечить:**

- Соблюдение прав сотрудников как субъектов ПДн
  - Открытость, согласие, заявленные цели обработки
  - Не собирать избыточную информацию о сотруднике
  - Не делать это скрытно: субъект ПДн имеет право знать: кто, что и для чего обрабатывает
- Обеспечение адекватной защиты персональных данных сотрудников
- Оправданность мониторинга целями защиты интересов бизнеса или общества, предотвращения утечки конфиденциальной информации и нарушений политики безопасности, расследование преступлений
- Довести до сведения сотрудников под роспись (желательно, до заключения трудового договора):
  - Соглашение о конфиденциальности
  - Правила допустимого использования ресурсов
  - Правила поведения

# Вопрос: Правильно ли Оператор обезличил персональные данные?

- Есть несколько ИСПДн классов К2-К1 (больше 1000 записей, категория ПДн 1-2)
- ФИО заменили на абстрактные идентификаторы
- Комбинация ФИО-ID хранится отдельно в службе каталогов
- Получили системы класса К4-К3

# Ответ: Это не обезличивание! так как:

- Оператор ПДн все равно может идентифицировать субъекта
- Цель обработки ПДн осталась прежней: обработка ПДн о конкретных субъектах и принятие на основании этих данных решений, затрагивающих интересы этих субъектов
- Оператор просто перераспределил ПДн по нескольким базам данных

# Вопрос: Являются ли в данном случае результаты анализов персональными данными?

- Поликлиника заменяет ФИО пациентов абстрактными идентификаторами и передает результаты анализов в Лабораторию
- Лаборатория определят, что ряд пациентов имеет проблемы, и сообщает в поликлинику
- Поликлиника связывается с соответствующими пациентами и назначает лечение

# Ответ: это зависит от того, кто эти данные обрабатывает и от уровня их защиты

- Данные, переданные в Лабораторию не являются персональными при условии, что Поликлиника обеспечивает достаточный уровень их защиты
- Эти же данные являются персональными, если Оператор – Поликлиника

  *(те же соображения относятся к обработке статистических данных учеными)*

# Чего добивается от оператора ПДн законодатель?

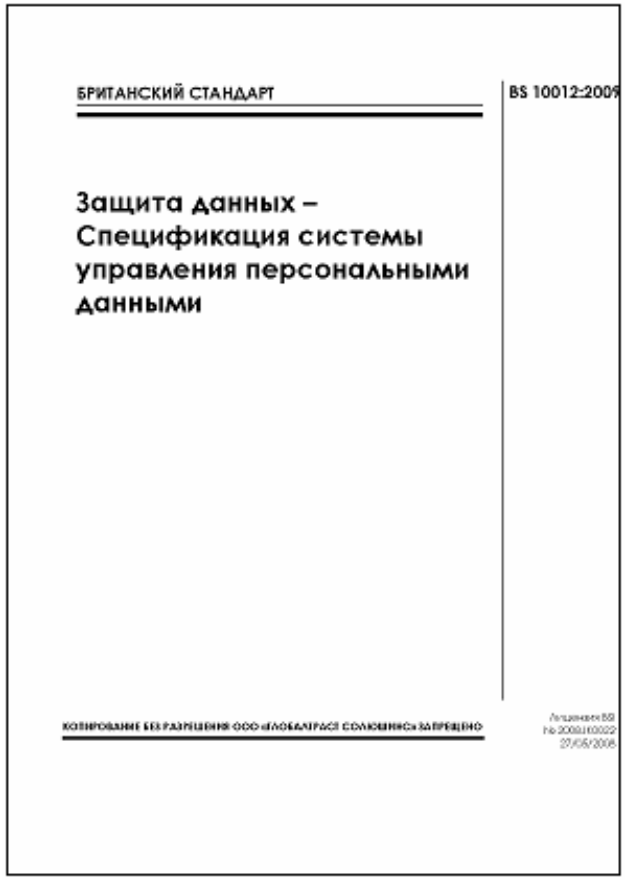
1) **Определить цели и содержание обработки ПДн**
2) **Уведомить Роскомнадзор об обработке ПДн**
3) **Соблюдать права субъектов ПДн**
4) **Обеспечить безопасность ПДн**
5) **Соблюдать принципы обработки ПДн**

# Принципы обработки ПДн

1) Законность целей и способов обработки ПДн
2) Соответствие целей обработки ПДн целям, заранее определенным и заявленным
3) Соответствие объема и характера обрабатываемых ПДн целям их обработки
4) Достоверности, достаточности, недопустимости обработки избыточных ПДн
5) Недопустимости объединения созданных для несовместимых между собой целей баз данных ИСПДн

# Использование передового опыта управления персональными данными

- BS 10012 - первый в мире стандарт на систему управления персональными данными
- Соответствует ISO 27001 и PAS 99
- Соответствует британским и европейским директивам и конвенциям по защите данных
  - Data Protection Act 1998
  - Directive 95/46/EC


БРИТАНСКИЙ СТАНДАРТ

BS 10012:2009

Защита данных – Спецификация системы управления персональными данными

КОПИРОВАНИЕ БЕЗ РАЗРЕШЕНИЯ ООО «ГЛОБАЛТРАСТ СОЛЮШНЗ» ЗАПРЕЩЕНО

# Принципы обработки ПДн согласно европейского законодательства

1. **обрабатываться добросовестно и на законных основаниях**
2. **собираться только для определенных целей и обрабатываться только в соответствии с этими целями**
3. **быть адекватной, соответствующей целям и не избыточной**
4. **быть достоверной и актуальной**
5. не должна храниться дольше, чем это необходимо
6. обрабатываться с соблюдением законных прав физических лиц, включая право на получение доступа к личной информаци
7. быть защищенной
8. не должна передаваться в страны, находящиеся за пределами Европейской экономической зоны без обеспечения надлежащей защиты

# Ответственность за нарушение ФЗ-152


Статья 24 Закона № 152-ФЗ: «Лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность»

*Кстати!*

*с 6 апреля 2010 г. в Великобритании за нарушение DPA может налагаться штраф до 500 000 фунтов стерлингов*

# Кодекс РФ об Административных Правонарушениях


- «…КоАП РФ. Статья 13.11. Нарушение установленного законом «О персональных данных» порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

  Нарушение установленного законом «О персональных данных» порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) – влечет **предупреждение или наложение административного штрафа**…»

- «…КоАП РФ. Статья 13.14. Разглашение информации с ограниченным доступом

  Разглашение информации, доступ к которой ограничен федеральным законом «О персональных данных» (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 настоящего Кодекса, (Ст.14.33- недобросовестная конкуренция) влечет **наложение административного штрафа**...»

- «…КоАП РФ. Статья 5.39. Отказ в предоставлении гражданину информации

  Неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина, либо несвоевременное предоставление таких документов и материалов, непредоставление иной информации в случаях, предусмотренных законом «О персональных данных», либо предоставление гражданину неполной или заведомо недостоверной информации – влечет **наложение административного штрафа**…»

# Уголовный Кодекс РФ


- «…УК РФ. Статья 137. Нарушение неприкосновенности частной жизни

  1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации - наказываются штрафом, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо **арестом на срок до четырех месяцев**...»

- «…УК РФ. Статья 140. Отказ в предоставлении гражданину информации

  Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан, - наказываются штрафом, либо **лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет**...»

- «…УК РФ. Статья 272. Неправомерный доступ к компьютерной информации

  1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом, либо исправительными работами на срок от шести месяцев до одного года, либо **лишением свободы на срок до двух лет**…»

# Регламент проверок Роскомнадзора

Роскомнадзор

- Плановые проверки проводятся на основании ежегодного плана (размещается на сайте rsoc.ru)
- Проверки проводятся в отношении Операторов, включенных и не включенных в Реестр не чаще, чем раз в 3 года
- Внеплановые проверки проводятся по следующим основаниям:
  - Истечение срока исполнения Оператором ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства РФ в области ПДн.
  - Поступление обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о фактах возникновения угрозы или причинения вреда жизни, здоровью граждан.
  - Нарушение прав и законных интересов граждан действиями (бездействием) Операторов при обработке их ПДн.
  - Нарушение Операторами требований законодательства РФ в области ПДн, а также о несоответствии сведений, содержащихся в уведомлении об обработке ПДн, фактической деятельности.
- Уведомление Оператора о проведении проверки: плановой – за 3 дня, внеплановой – за 1 день или без уведомления.
- Проверки (плановые и внеплановые) проводятся в документарной и выездной форме.

# Проверочные мероприятия Роскомнадзора

- Обследование ИСПДн в части, касающейся персональных данных субъектов ПДн, обрабатываемых в ней.
- Рассмотрение документов Оператора:
  - Уведомления об обработке персональных данных.
  - Документы, необходимые для проверки фактов, содержащих признаки нарушения законодательства РФ в области ПДн, изложенных в обращениях граждан, и информации, поступившей в Службу или ее территориальный орган.
  - Документы, подтверждающие выполнение Оператором предписаний об устранении ранее выявленных нарушений законодательства РФ в области ПДн.
  - Письменное согласие субъекта ПДн на обработку его персональных данных.
  - Документы, подтверждающие соблюдение требований законодательства РФ при обработке специальных категорий и биометрических персональных данных.
  - Документы, подтверждающие уничтожение Оператором персональных данных субъектов ПДн по достижении цели обработки.
  - Локальные акты Оператора, регламентирующих порядок и условия обработки персональных данных.

# Права должностных лиц Роскомнадзора

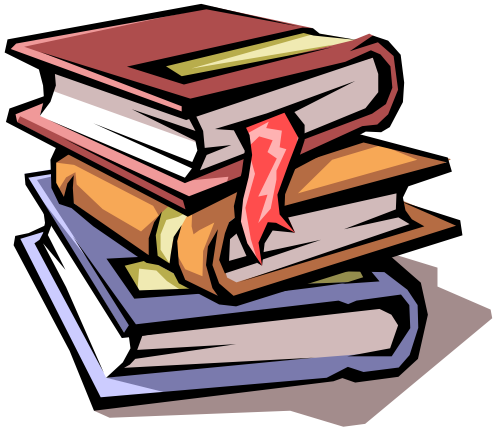
- Выдавать обязательные для выполнения предписания об устранении выявленных нарушений
- Составлять протоколы об административном правонарушении или направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении дел об административных правонарушениях, а также о возбуждении уголовных дел
- Обращаться в суд с исковыми заявлениями в защиту прав субъектов ПДн
- Использовать технику и оборудование, принадлежащие Роскомнадзору
- Запрашивать и получать необходимые документы (сведения)
- Получать доступ к ИСПДн в режиме просмотра и выборки информации
- Направлять заявление в орган, осуществляющий лицензирование деятельности Оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию лицензии
- Принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушениями требований законодательства РФ
- Требовать от Оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных.

# Система защиты ПДн

## Организационная составляющая

1) **Политика управления доступом к ИСПДн**
2) **Антивирусная политика**
3) **Парольная политика**
4) **Политика резервного копирования и восстановления данных**
5) **Регламент работы с мобильными устройствами и с цифровыми носителями ПДн**
6) **Процедуры аварийного восстановления ИСПДн**
7) **Политика управления инцидентами безопасности**
8) **Политика контроля эффективности и мониторинга СЗПДн**

*и еще пара десятков документов ...*



# Система защиты ПДн

## Техническая составляющая

1) **Подсистема управления доступом**
2) **Подсистема регистрации и учета**
3) **Подсистема обеспечения целостности**
4) **Подсистема антивирусной защиты**
5) **Подсистема обнаружения вторжений**
6) **Подсистема межсетевого экранирования**
7) **Подсистема анализа защищенности**
8) **Криптографическая подсистема**
9) **Подсистема предотвращения утечек информации**
10) **…**

# Обеспечение соответствия ФЗ-152

## Этап 1 – Определение требований и подходов

1) Обследование ИСПДн и оценка текущего положения дел
2) Классификация ИСПДн
3) Разработка моделей угроз ИСПДн
4) Разработка ТЗ на создание СЗПДн
5) Разработка Концепции защиты ПДн

# Обеспечение соответствия ФЗ-152

## Этап 2 – Проектирование и внедрение СЗПДн

1) Техническое проектирование СЗПДн
2) Внедрение сертифицированных СЗИ
3) Разработка ОРД по защите и обработке ПДн
4) Обучение сотрудников правилам работы с ПДн
5) Ревизия договорных отношений

# Спецификация СЗПДн
# Вариант 1

| Подсистема защиты ИСПД | Продукт | Кол-во, шт. | Цена, руб. |
|---|---|---|---|
| Подсистема защиты внешнего периметра корпоративной сети (МЭ, VPN, IPS, AV, AS) | WG50750 WatchGuard Firebox X750e 3 класс (сертификат ФСТЭК) | 1 | 140000 |
| Подсистема защиты от вредоносного ПО | Kaspersky Enterprise Space Security | 100 | 180000 |
| Подсистема защиты от НСД | Панцирь-К (сетевая версия) | 100 | 300000 |
| Подсистема шифрования данных | Сертифицированный Aladdin Secret Disk 4 | 100 | 210000 |
| | Сертифицированные USB ключи eTokenPRO 64K | 100 | 100000 |
| Сертифицированные версии ОС и офисного ПО (только за сертификаты, лицензии на данные продукты должны быть в наличии) | Microsoft windows XP Prof, Server 2003 Standard Edition, Office 2007 Pro | 100 | 500000 |
| Подсистема контроля защищенности | Ревизор сети, ФИКС, TERIER | 100 | 100000 |
| **Итого:** | | | **1530000** |

# Спецификация СЗПДн Вариант 2

| № | Подсистема | Продукт | Описание | Количество | Стоимость, руб. (оценочная) |
|---|---|---|---|---|---|
| 1 | Управления Доступом | ПО Dallas Lock 7.5 сертификат ФСТЭК России № 1685 от 18.09.08 по классу К1. | ПО контроля целостности ОС и защиты от НСД В комплект входят ПО, ПО центр управления безопасностью. | Пользовательских лицензий – 10 шт. | 60 000 |
| | | | | Центр управления безопасностью - 2 шт | 30 000 |
| 2 | Регистрации и учета | ПО Dallas Lock 7.5 сертификат ФСТЭК России № 1685 от 18.09.08 по классу К1. | ПО контроля целостности ОС и защиты от НСД В комплект входят ПО, ПО центр управления безопасностью. | - | - |
| 3 | Контроля целостности | ПО Dallas Lock 7.5 сертификат ФСТЭК России № 1685 от 18.09.08 по классу К1. | ПО контроля целостности ОС и защиты от НСД В комплект входят ПО, ПО центр управления безопасностью. | - | - |
| 4 | Антивирусной защиты | ESET NOD32 Platinum Pack 4.0 с сертификатом ФСТЭК по классу К1 | В комплект входит: конверт, лицензия, копия сертификата ФСТЭК, формуляр, DVD-box, диск с наклейкой ФСТЭК и дистрибутивами продуктов: ESET NOD32 Антивирус (32- и 64-bit), ESET NOD32 Smart Security (32- и 64-bit), ESET Remote Ad | Пользовательских лицензий – 5 шт. | 9 340 |
| | | | | Сертифицированный дистрибутив | 2 500 |
| 5 | Анализа защищенности | Сканер безопасности XSpider 7.7 Сканер безопасности MBSA 2.1 | ПО XSpider 7.7 имеет сертификат соответствия ФСТЭК России № 1323 от 23 января 2007 г., подтверждающий контроль отсутствия недекларированных возможностей по 2 классу и оценочный уровень доверия ОУД 3 | Лицензия на 16 IP-адресов, 1 год технической поддержки и сертифицированный дистрибутив | 19440 |
| 6 | Обнаружения вторжения | D-link DFL-800/1600 | IDS в составе МЭ | - | - |
| 7 | Межсетевого экранирования | D-link DFL-800/1600 | Программно-аппаратный МЭ | - | - |
| 8 | VPN | ПО SecureCRT 5.2, Radmin 3.2 | ПО удаленного администрирования | - | - |
| **ИТОГО** | | | | | **121 280** |

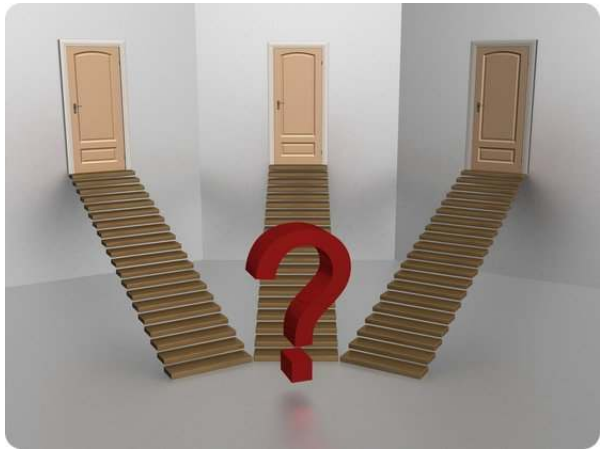
# Обеспечение соответствия ФЗ-152

## Этап 3 – Подтверждение соответствия

1) **Аттестация ИСПДн по требованиям безопасности информации**
2) **Лицензирование деятельности в области защиты информации**
3) **Самооценка**
4) **Независимый аудит**


НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

# Какой подход к обеспечению соответствия выбрать?



- Делать все самим
  - Сроки? Стоимость? Квалификация? Опыт?
- Заказать проект под ключ лицензиату ФСТЭК
  - от 1 млн. руб., ~ 4-5 месяцев, Гарантии?
- Отдать защиту ИСПДн на аутсорсинг
  - SLA? Гарантии? Стоимость?
- Полностью отдать обработку персональных данных на аутсорсинг
  - Кому? Как? Стоимость? Гарантии?

# Комплект типовых документов для оператора персональных данных

- **Проектные документы**
- **Положения**
- **Планы работ**
- **Инструкции**
- **Приказы**
- **Акты**
- **Журналы и перечни**
- **Согласия, обязательства и уведомления**
- **Всего более 40 готовых документов**

# Эволюция типовых документов ГлобалТраст

2003: первый комплект основных политик ИБ (около 20 документов)

2005: **GTS 1035** - комплект документов СУИБ по ISO 27001 (более 60 документов)

2008: **GTS 1056** - комплект документов СУИР по ISO 27005 и BS 7799-3 (по управлению рисками ИБ) (более 20 документов)

2010: **GTS 1071** - комплект документов для оператора ПДн (более 40 документов)

# Аналогичные продукты партнеров ГлобалТраст

- Alan Calder: ISO 27001 Toolkit
- Charles Cresson Wood: Information Security Policies Made Easy
- IT Governance Toolkit
- Business Continuity Toolkit
- PCI DSS Toolkit
- InformationShield Privacy Toolkit





# Преимущества типовых документов ГлобалТраст

- Гарантии качества документов
  - Соответствие законодательству, нормативной базе и стандартам
  - Опробированность
  - Политика возврата денег
  - Бесплатная доработка документов
- Поддержка внедрения
  - Консультации
  - Предоставление дополнительных материалов
  - Обновления документов

Консалтинговые услуги
в области
информационной
безопасности

Global Trust Solutions

# Практика обеспечения соответствия в области персональных данных


Александр Астахов
GlobalTrust Solutions

Тел.: +7 (495) 651-6617
Факс: +7 (495) 967-7600
Email: info@globaltrust.ru
Web: www.globaltrust.ru