Практические аспекты защиты персональных данных в РФ

Александр Астахов

Генеральный директор

Global Trust Solutions

Продукты и услуги в области информационной безопасности

В центре внимания Роскомнадзора

«По результатам анализа имевшейся контрольно-надзорной практики был определен **приоритетный круг категорий операторов**, осуществляющих обработку чувствительного объема персональных данных значительного числа российских граждан. В указанный круг вошли **рекрутинговые агентства**, страховые компании, организации гостиничного и туристического бизнеса, операторы электронной дистанционной торговли, сервисы бронирования билетов в рамках осуществления пассажирских перевозок, кредитные организации, дилерские центры и др.»

Global Trust Solutions

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.

Global Trust Solutions

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.

Global Trust Solutions

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.

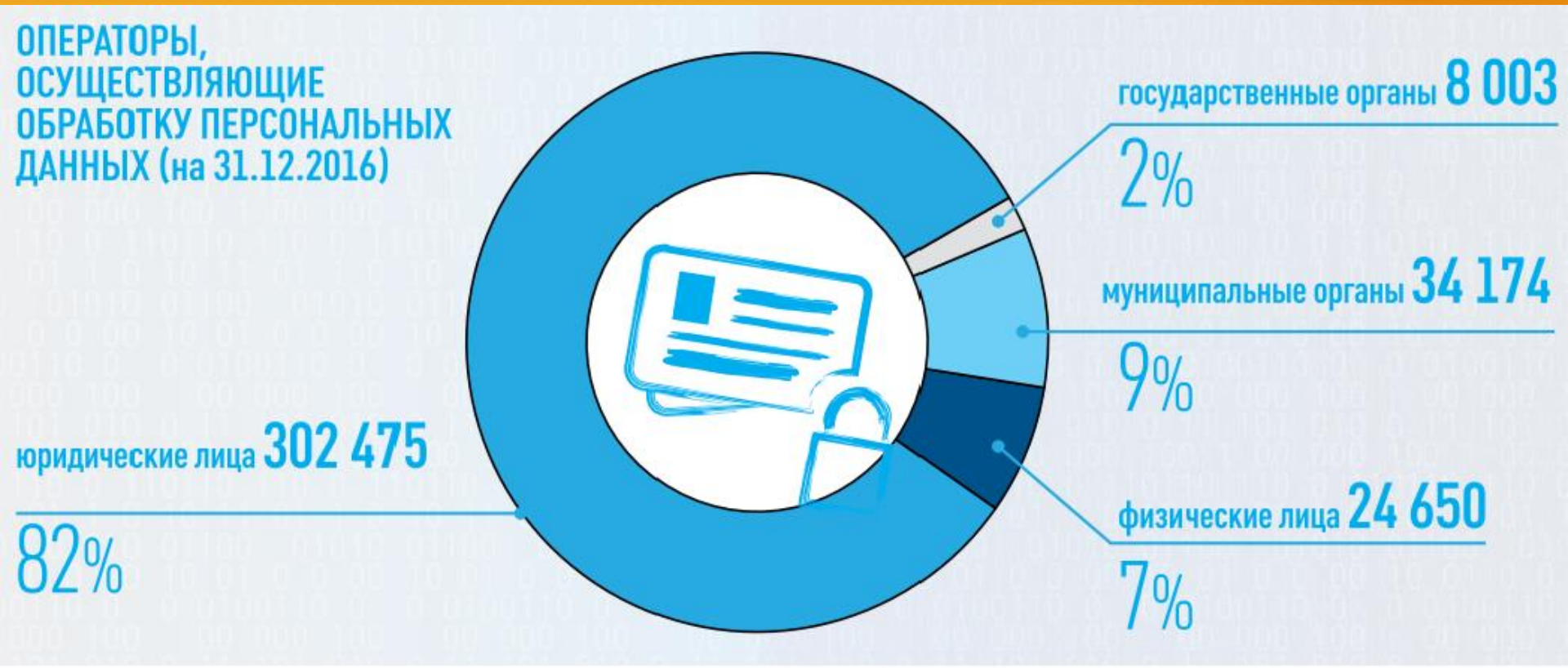
Global Trust Solutions

Проверки Роскомнадзора в 2016

- 1307 плановых проверок и 99 внеплановых
- Выявлено 2134 нарушений, выдано 619 предписаний, направлено в суды 6930 протоколов, 5 982 200 руб. сумма штрафов
- Наиболее частые нарушения:
  - Неполные или недостоверные сведения в уведомлениях
  - Несоответствие содержания письменных согласий субъектов ПДн требованиям 152-ФЗ
  - Отсутствие в поручении лицу, которому оператор поручает обработку ПДн, обязанности обеспечения конфиденциальности и безопасности ПДн, а также требований по защите ПДн

Global Trust Solutions

Зарегистрированные операторы ПДн



Global Trust Solutions

109 326 обращений граждан в Роскомнадзор

Global Trust Solutions

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**…»

Global Trust Solutions

Уголовный Кодекс РФ

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

  1. Незаконное собирание или распространение сведений о частной жизни лица, составляющи 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**…»

Global Trust Solutions

Последствия нарушений в области ПДн

- Штрафные санкции (ст. 13.11 КоАП РФ, до 50 тыс. руб.)
- Приостановление или прекращение обработки ПДн
- Блокирование сайтов
- Попадание в отчеты Роскомнадзора
- Попадание на внеплановые проверки и совместные
- проверки с участием ФСТЭК и ФСБ
- Возмещение морального и материального вреда
- Конфискация несертифицированных СЗИ, СКЗИ, СВТ
- Дисквалификация руководителя организации
- Уголовная ответственность (ст. 137, 140 УК РФ)

Global Trust Solutions

Разъяснение вопросов по обработке ПДн

- Обработка ПДн работника не требует получения согласия, при условии, что объем обрабатываемых работодателем ПДн соответствует ТК РФ
- Обработка ПДн близких родственников работника не требует получения согласия в случаях, установленных законодательством РФ (получение алиментов, оформление допуска к государственной тайне, оформление социальных выплат).
- Обработка сведений о состоянии здоровья, относящихся к вопросу о возможности выполнения работником трудовой функции.
- Передача ПДн работников в ФСС РФ, НФ РФ осуществляется без их согласия.
- Работодатель вправе обрабатывать ПДн уволенного работника в случаях и в сроки, предусмотренные ФЗ. К таким случаям, в том числе, относится обработка ПДн в рамках бухгалтерского (5 лет) и налогового учета (4 года). По истечении сроков хранения личные дела работников и иные документы передаются на архивное хранение на срок 75 лет.
- В случае получения резюме соискателя по каналам электронной почты, факсимильной связи работодателю необходимо дополнительно провести мероприятия, направленные на подтверждение факта направления указанного резюме самим соискателем.
- Типовая форма анкеты соискателя может быть реализована в электронной форме на сайте организации, где согласие на обработку ПДн подтверждается соискателем путем проставлением отметки в соответствующем поле
- В случае отказа в приеме на работу сведения, предоставленные соискателем, должны быть уничтожены в течение 30 дней

Global Trust Solutions

Три кита гос. регулирования в области защиты информации

- **Лицензирование деятельности в области ТЗКИ и криптографии**
  - Бессрочное и не для собственных нужд (ПП РФ №313 от 16.04.12, письмо ФСТЭК №240/22/2222 от 30.05.12)
- **Сертификация СЗИ (СВТ, СКЗИ и т. д.)**
  - Сертификация или оценка соответствия?
  - Обязательная или добровольная? (СТР-К, ПП РФ №330 —
  - документы с грифом ДСП)
- **Аттестация ИСПДн (ИС, АС, АСУТП и т. д.)**
  - Обязательная аттестация ИСПДн для гос. учреждений? (только в
  - СТР-К: гриф ДСП и распространялся на защиту ПДн только до
  - принятия ФЗ-152)

Global Trust Solutions

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 ...

Global Trust Solutions

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) Подсистема защиты среды виртуализации
11) …..

Global Trust Solutions

Спецификация СЗПДн

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**

Global Trust Solutions

Проект обеспечения соответствия 152-ФЗ

Этап 1 – Предпроектное обследование

Этап 2 – Разработка ОРД

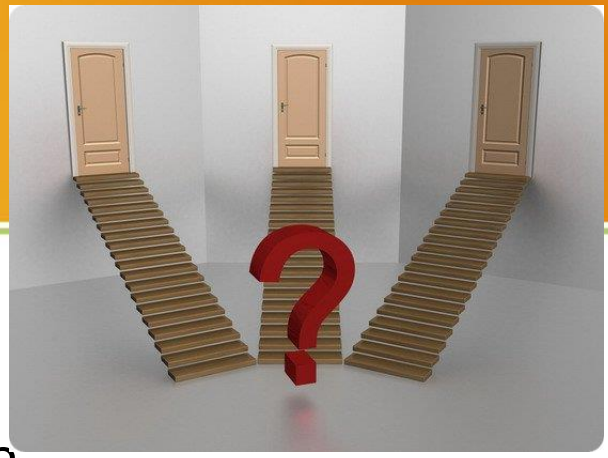
Этап 3 – Проектирование СЗПДн

Этап 4 – Внедрение СЗПДн

Этап 5 – Оценка соответствия ИСПДн

Global Trust Solutions

Какой подход к обеспечению соответствия выбрать?

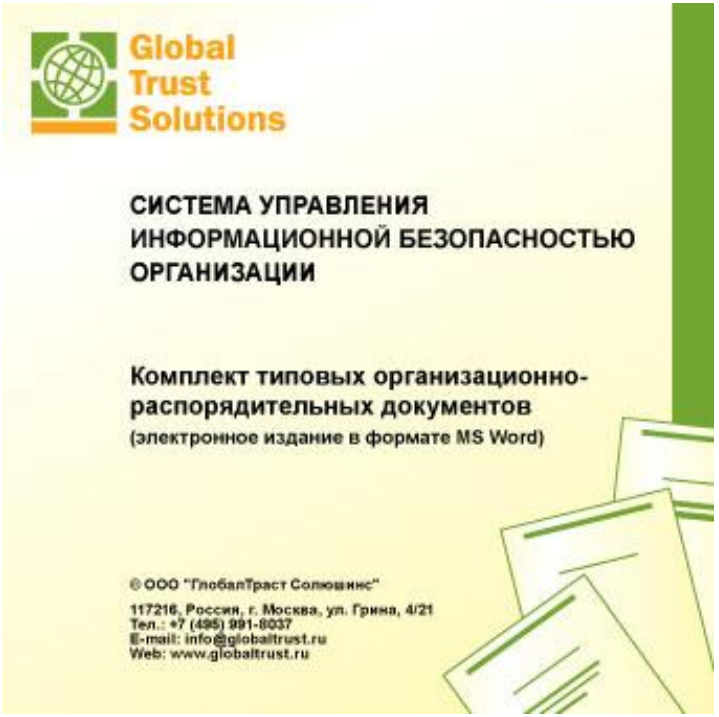


- Делать все самим
  - Сроки? Стоимость? Квалификация? Опыт?
  - Готовые документы – от 60 т.р.
- Заказать проект под ключ лицензиату ФСТЭК
  - от 300 т.р., ~ 2-3 месяца, Гарантии?
- Отдать защиту ИСПДн на аутсорсинг
  - SLA? Гарантии? Стоимость?
- Полностью отдать обработку персональных данных на аутсорсинг (в аттестованный ЦОД)
  - Кому? Как? Стоимость? Гарантии?

Global Trust Solutions

Комплект типовых документов для оператора персональных данных

- Проектные документы
- Положения
- Планы работ
- Инструкции
- Приказы
- Акты
- Журналы и перечни
- Согласия, обязательства и уведомления
- **Всего более 50 готовых документов**



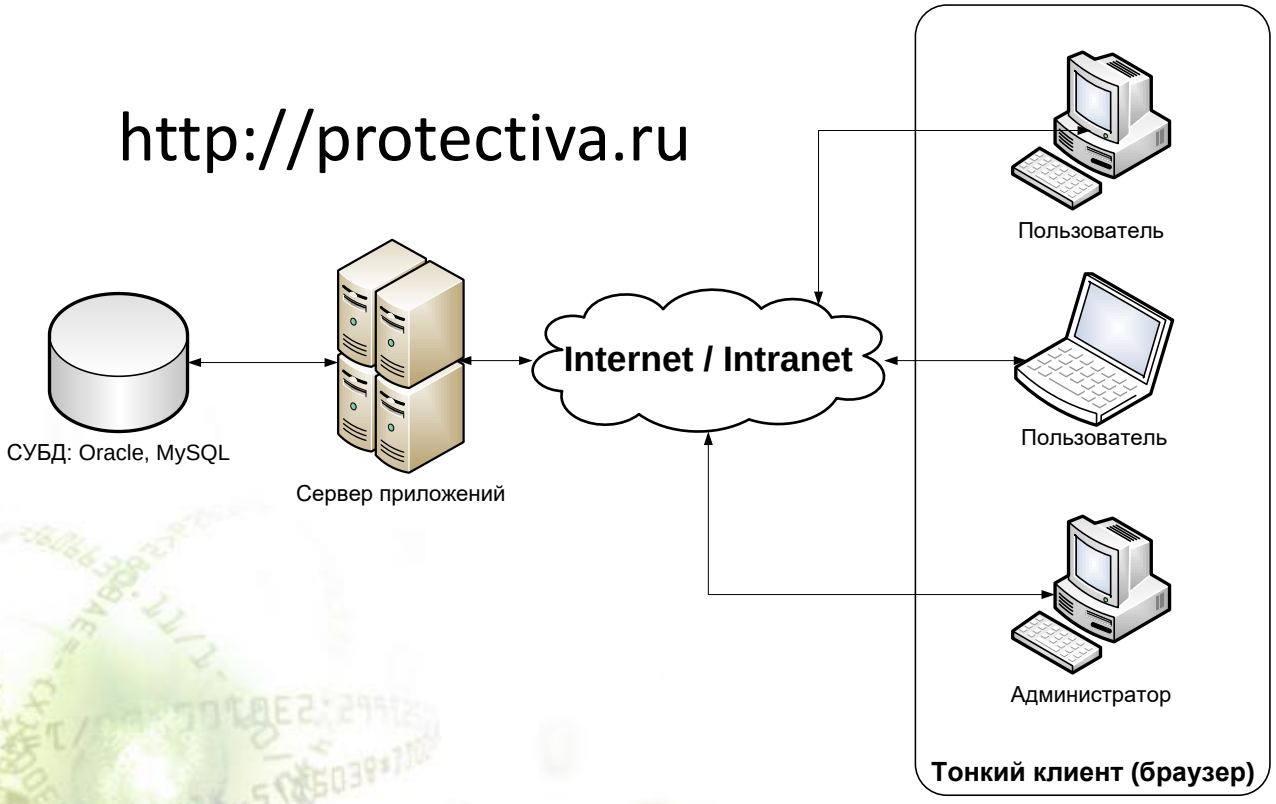
Global Trust Solutions

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

Global Trust Solutions

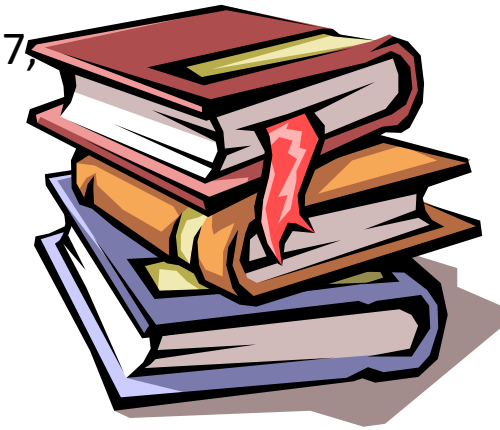
Интернет-сервис ПРОТЕКТИВА для оценки соответствия в области ПДн



ПРОТЕКТИВА

ПРОТЕКТИВА поддерживает любые нормативные документы

- **Федеральные законы РФ**: 161-ФЗ, ***152-ФЗ***, 98-ФЗ
- **Постановления Правительства РФ**: ***ПП-1119***, ПП-584, ПП-687, ПП-512, ПП-1233
- **Международные стандарты**: ISO 27001, 27032, 27034, 27035, 20000, 22301
- **Национальные стандарты РФ**: ГОСТ Р 51583-2014, ГОСТ Р 53113.1-2008, ГОСТ Р 53113.2-2009, ГОСТ Р 53131-2008, ГОСТ Р ИСО/МЭК 27033-1-2011, ГОСТ Р ИСО/МЭК 27005-2010, ГОСТ Р 56939-2016
- **Документы Банка России**: СТО БР ИББС, 382-П, 2831-У, 397-П, РС БР ИББС-2.6-2014, 49-Т, 154-Т, 36-Т, 146-Т
- **Приказы ФСТЭК России** № 17, ***21***, 31, СТР-К
- **Приказы ФСБ России** № 149/54-144, 149/6/6-622, 378
- **Отраслевые стандарты**, нормативные документы ***Роскомнадзора***, Минсвязи, Правительства Москвы
- **Внутренние политики** ГлобалТраст (более 40)
- **Любые документы без ограничений!**



ПРОТЕКТИВА

Спасибо за внимание!

ООО «ГлобалТраст Солюшинс»

Продукты и услуги в области
информационной безопасности

Астахов
Александр Михайлович

генеральный директор

123317, Россия, Москва,
Пресненская наб., 10, блок С,
Бизнес-центр «Регус»
www.globaltrust.ru

Тел.: **+7 (925) 203-95-11**
Моб.: **+7 (925) 242-06-86**
Факс: +7 (495) 967-76-00
E-mail: AlexAstahov@globaltrust.ru