leta
IT-COMPANY

Защита персональных данных

ОБЗОР ИЗМЕНЕНИЙ ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ

ОБЗОР ИЗМЕНЕНИЙ ЗАКОНОДАТЕЛЬСТВА

Федеральный закон от 27.07.2006 **№152-ФЗ** «О персональных данных»

Постановление Правительства РФ от 17.11.2007 **№781** «Об утверждении Положения об обеспечении безопасности ПДн при их обработке в ИСПДн»

Постановление Правительства РФ от 06.07.2008 **№ 512** «Об утверждении требований к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн»

Постановление Правительства РФ от 15.09.2008 **№687** «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации»

ОБЗОР ИЗМЕНЕНИЙ ЗАКОНОДАТЕЛЬСТВА

Постановление Правительства РФ от 17.11.2007 **№781** «Об утверждении Положения об обеспечении безопасности ПДн при их обработке в ИСПДн»

Приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 №55/86/20 «Об утверждении Порядка проведения классификации ИСПДн»

ФСТЭК РОССИИ:

- Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн
- Базовая модель угроз безопасности ПДн при их обработке в ИСПДн
- Рекомендации по обеспечению безопасности ПДн при их обработке в ИСПДн
- Основные мероприятия по организации и техническому обеспечению безопасности ПДн, обрабатываемых в ИСПДн

ФСБ РОССИИ:

- Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для ЗИ, не содержащей сведений, составляющих гос. тайну в случае их использования для обеспечения безопасности ПДн при их обработке в ИСПДн

ОБЗОР ИЗМЕНЕНИЙ ЗАКОНОДАТЕЛЬСТВА

февраль
5
2010

Постановление Правительства РФ от 17.11.2007 **№781** «Об утверждении Положения об обеспечении безопасности ПДн при их обработке в ИСПДн»

Приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 №55/86/20 «Об утверждении Порядка проведения классификации ИСПДн»

ФСТЭК РОССИИ:

Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн

Базовая модель угроз безопасности ПДн при их обработке в ИСПДн

Приказ ФСТЭК России от 05.02.2010 №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»

ФСБ РОССИИ:

Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации

Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для ЗИ, не содержащей сведений, составляющих гос. тайну в случае их использования для обеспечения безопасности ПДн при их обработке в ИСПДн

ОБЗОР ИЗМЕНЕНИЙ ЗАКОНОДАТЕЛЬСТВА

Федеральный закон от 27.07.2006 **№152-ФЗ** «О персональных данных»

Постановление Правительства РФ от 17.11.2007 **№781** «Об утверждении Положения об обеспечении безопасности ПДн при их обработке в ИСПДн»

Постановление Правительства РФ от 06.07.2008 **№ 512** «Об утверждении требований к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн»

Постановление Правительства РФ от 15.09.2008 **№687** «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации»

Правительство РФ должно установить уровни защищенности ПДн при их обработке в ИСПДн

Операторы, которые осуществляли обработку ПДн до 1 июля 2011 года, обязаны представить сведения (п. 5, 7.1, 10 и 11 ч. 3 статьи 22 ФЗ-152) в Роскомнадзор
не позднее **1 января 2013**

ОБЗОР ИЗМЕНЕНИЙ ЗАКОНОДАТЕЛЬСТВА

ноябрь
1
2012

Федеральный закон от 27.07.2006 **№152-ФЗ** «О персональных данных»

Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите ПДн при их обработке в ИСПДн»

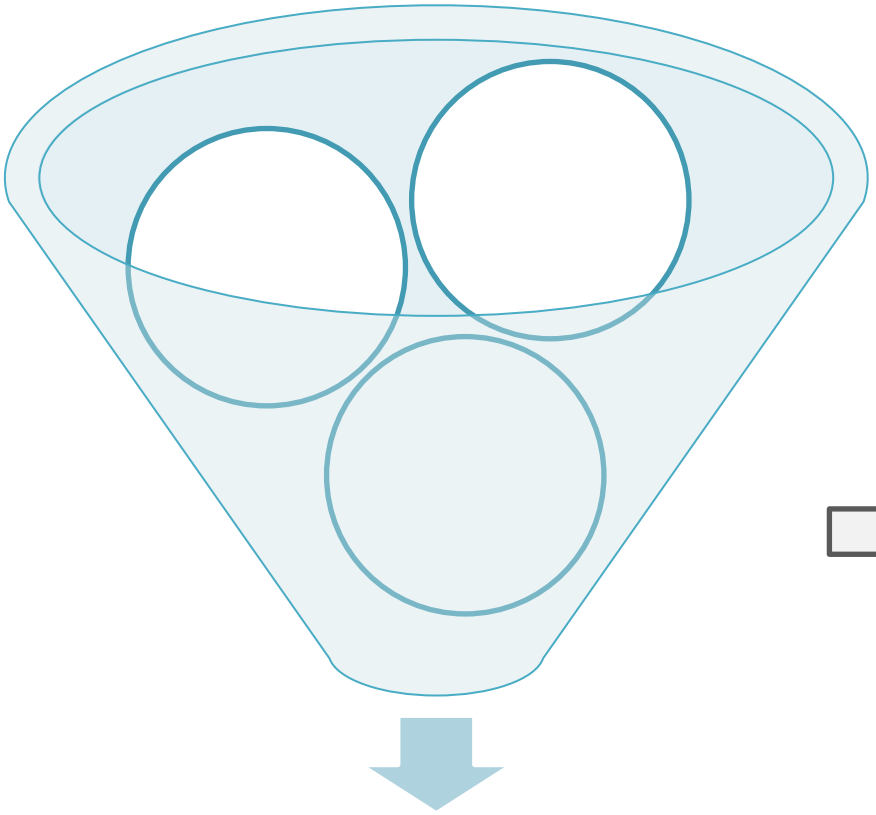
Постановление Правительства РФ от 06.07.2008 **№ 512** «Об утверждении требований к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн»

Постановление Правительства РФ от 15.09.2008 **№687** «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации»

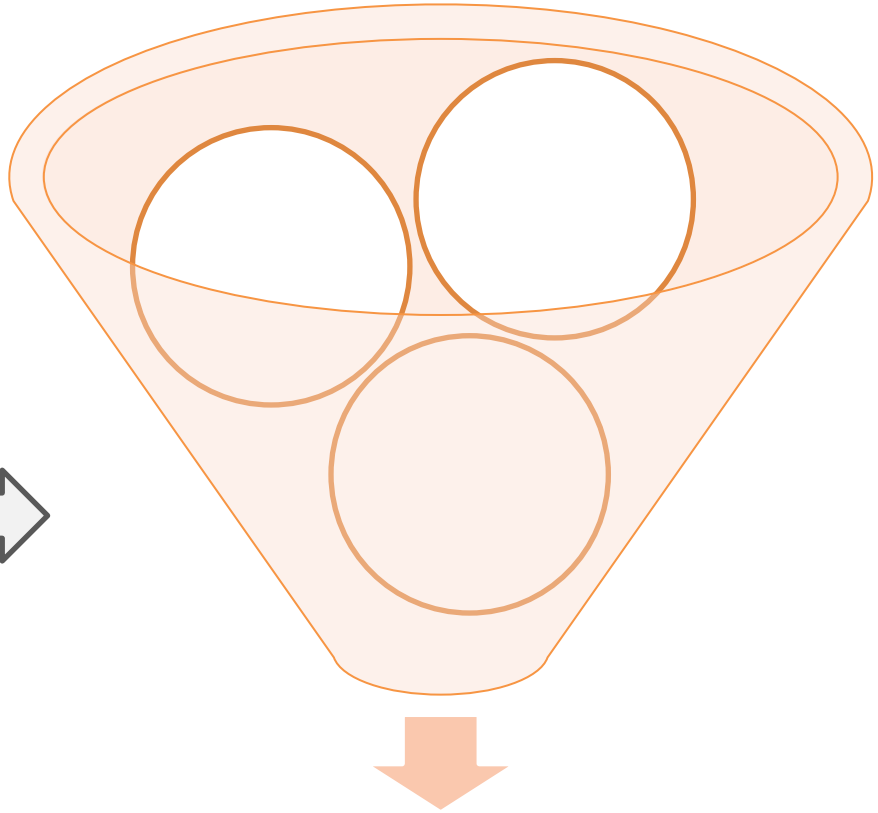
Нормативно-правовые акты ФСТЭК России
проекты документов – **до 7 декабря 2012**

Нормативно-правовые акты ФСБ России
утвержденные документы – **январь 2013**

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №1119
ЧТО ИЗМЕНИЛОСЬ?



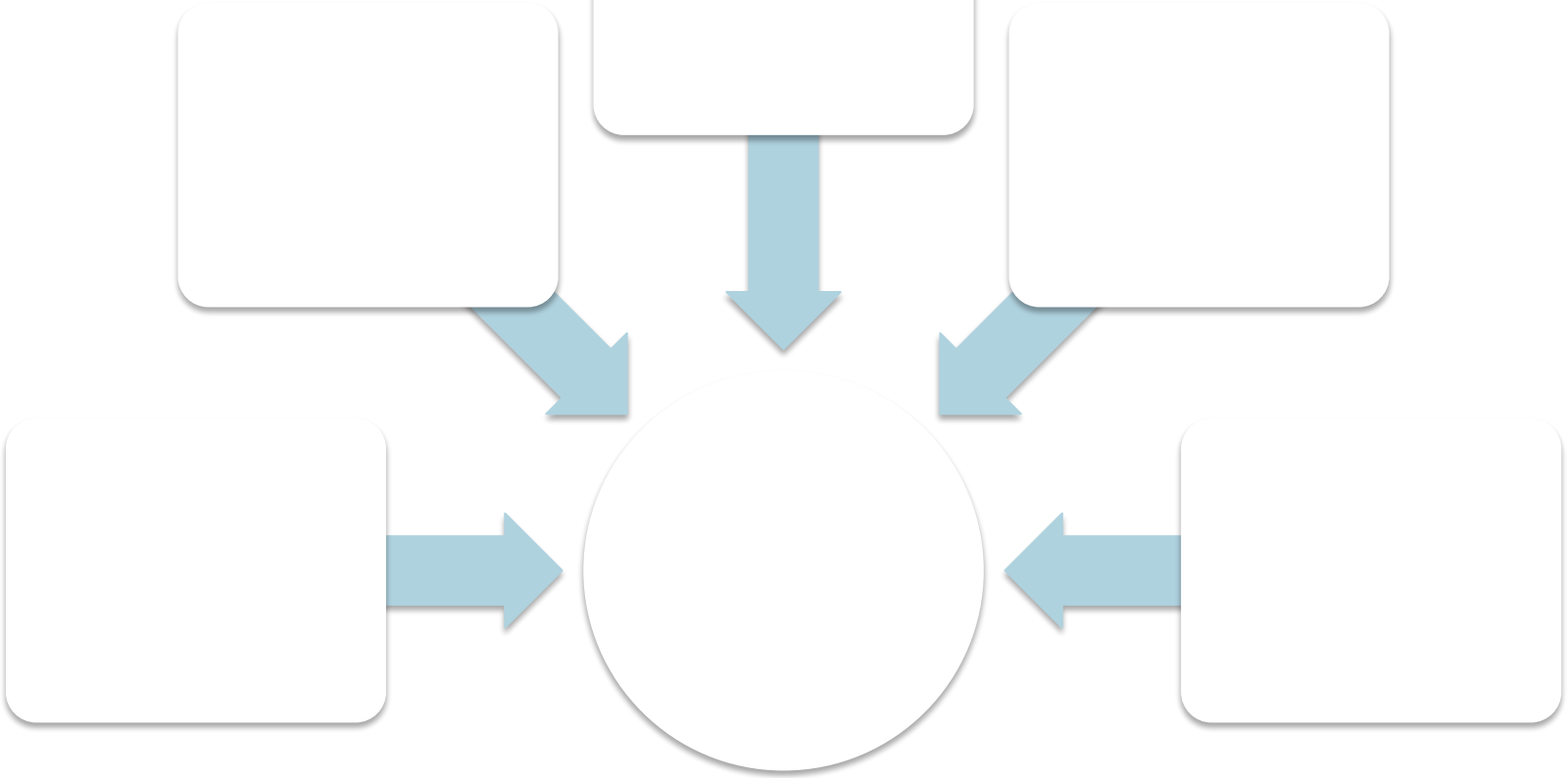
Требования к защите ПДн при их обработке в ИСПДн



Требования к защите ПДн при их обработке в ИСПДн

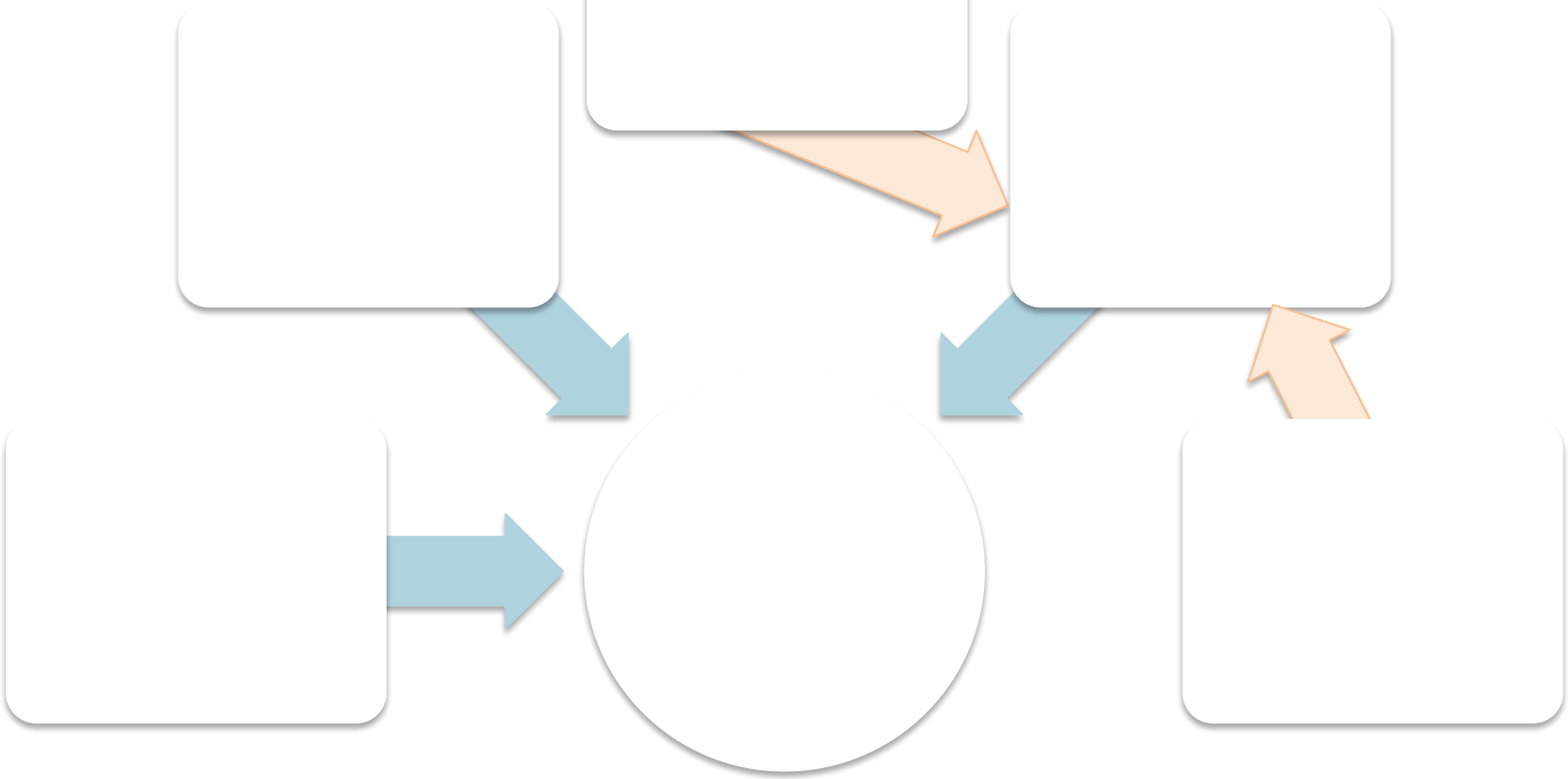
ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №1119 АНАЛИЗ ДОКУМЕНТА

Согласно ч. 3 ст. 19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» Правительство РФ должно было установить уровни защищенности ПДн,
с учетом:



ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №1119 АНАЛИЗ ДОКУМЕНТА

Согласно Постановлению Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к за обработке в ИСПДн» уровни защищенно ны, с учетом:



ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №1119
АНАЛИЗ ДОКУМЕНТА

Содержание ПДн категория обрабатываемых ПДн	**Содержание ПДн** категория субъектов обрабатываемых ПДн	**Объем ПДн** количество субъектов ПДн	**Тип актуальных угроз**		
			1 тип	2 тип	3 тип
специальные категории ПДн	субъекты ПДн, не являющиеся сотрудниками оператора	более 100 000	**УЗ – 1**	**УЗ – 1**	**УЗ – 2**
		менее 100000	**УЗ – 1**	**УЗ – 2**	**УЗ – 3**
	сотрудники оператора	более 100 000	**УЗ – 1**	**УЗ – 2**	**УЗ – 3**
		менее 100000	**УЗ – 1**	**УЗ – 2**	**УЗ – 3**
биометрические ПДн	субъекты ПДн, не являющиеся сотрудниками оператора	более 100 000	**УЗ – 1**	**УЗ – 2**	**УЗ – 3**
		менее 100000	**УЗ – 1**	**УЗ – 2**	**УЗ – 3**
	сотрудники оператора	более 100 000	**УЗ – 1**	**УЗ – 2**	**УЗ – 3**
		менее 100000	**УЗ – 1**	**УЗ – 2**	**УЗ – 3**
иные ПДн	субъекты ПДн, не являющиеся сотрудниками оператора	более 100 000	**УЗ – 1**	**УЗ – 2**	**УЗ – 3**
		менее 100000	**УЗ – 1**	**УЗ – 3**	**УЗ – 4**
	сотрудники оператора	более 100 000	**УЗ – 1**	**УЗ – 3**	**УЗ – 4**
		менее 100000	**УЗ – 1**	**УЗ – 3**	**УЗ – 4**
общедоступные ПДн	субъекты ПДн, не являющиеся сотрудниками оператора	более 100 000	**УЗ – 2**	**УЗ – 2**	**УЗ – 4**
		менее 100000	**УЗ – 2**	**УЗ – 3**	**УЗ – 4**
	сотрудники оператора	более 100 000	**УЗ – 2**	**УЗ – 3**	**УЗ – 4**
		менее 100000	**УЗ – 2**	**УЗ – 3**	**УЗ – 4**

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №1119
АНАЛИЗ ДОКУМЕНТА

ИНФОРМАЦИОННАЯ СИСТЕМА, ОБРАБАТЫВАЮЩАЯ СПЕЦИАЛЬНЫЕ КАТЕГОРИИ ПДН

обрабатываются ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн

ИНФОРМАЦИОННАЯ СИСТЕМА, ОБРАБАТЫВАЮЩАЯ БИОМЕТРИЧЕСКИЕ ПДН

обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн (при этом не обрабатываются специальные категории ПДн)

ИНФОРМАЦИОННАЯ СИСТЕМА, ОБРАБАТЫВАЮЩАЯ ОБЩЕДОСТУПНЫЕ ПДН

обрабатываются ПДн субъектов ПДн, полученные только из общедоступных источников ПДн, созданных в соответствии со статьей 8 Федерального закона «О персональных данных»

ИНФОРМАЦИОННАЯ СИСТЕМА, ОБРАБАТЫВАЮЩАЯ ИНЫЕ КАТЕГОРИИ ПДН

обрабатываются иные категории ПДн (при этом не обрабатываются специальные категории ПДн, биометрические ПДн, общедоступные ПДн)

в том числе, сведения о судимости , ПДн, прошедшие процедуру обезличивания, ПДн, сделанные общедоступными субъектом ПДн

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №1119
АНАЛИЗ ДОКУМЕНТА

ИНФОРМАЦИОННАЯ СИСТЕМА ОБРАБАТЫВАЮ СПЕЦИАЛЬНЫЕ КА ПДН

обрабатываются ПДн, расовой, наци принадлежности, п взглядов, религиозн философских убеждени здоровья, интимной жиз ПДн

ИНФОРМАЦИО СИСТЕМА ОБРАБАТЫВАЮ ОБЩЕДОСТУПНЫ

обрабатываются ПДн с полученные только из источников ПДн, с соответствии со статьей 8 закона «О персональных

Статья 10. Специальные категории персональных данных

1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка указанных в части 1 настоящей статьи специальных категорий персональных данных допускается в случаях, если:

…

3. Обработка **персональных данных о судимости** может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

4. Обработка **специальных категорий персональных данных**, осуществлявшаяся в случаях, **предусмотренных частями 2 и 3** настоящей статьи, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

ИНФОРМАЦИОННАЯ

ПДн, сделанные общедоступными субъектом ПДн

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №1119 АНАЛИЗ ДОКУМЕНТА

ИНФОРМАЦИОННАЯ СИСТЕМА, ОБРАБАТЫВАЮЩАЯ СПЕЦИАЛЬНЫЕ КАТЕГОРИИ ПДН

обрабатываются ПДн, расовой, нац принадлежности, взглядов, религиоз философских убежден здоровья, интимной жи ПДн

ИНФОРМАЦИОННАЯ СИСТЕМА, ОБРАБАТЫВАЮЩАЯ БИОМЕТРИЧЕСКИЕ ПДН

которые и века, на вить его ератором ПДн (при циальные

ИНФОРМАЦИ СИСТЕМ ОБРАБАТЫВА ОБЩЕДОСТУПН

обрабатываются ПДн полученные только из общедоступных источников ПДн, созданных в соответствии со статьей 8 Федерального закона «О персональных данных»

Дн (при этом не обрабатываются специальные категории ПДн, биометрические ПДн, в том числе, сведения о судимости , общедоступные ПДн)

ПДн, прошедшие процедуру обезличивания,
ПДн, сделанные общедоступными субъектом ПДн

Статья 8. Общедоступные источники персональных данных

1. В целях информационного обеспечения могут создаваться общедоступные источники ПДн (в том числе справочники, адресные книги). В общедоступные источники ПДн **с письменного согласия субъекта ПДн** могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн, сообщаемые субъектом ПДн.
2. Сведения о субъекте ПДн должны быть в любое время исключены из общедоступных источников ПДн по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов.

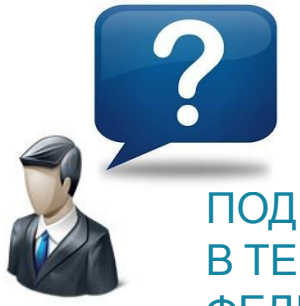
ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №1119
АНАЛИЗ ДОКУМЕНТА

ИНФОРМАЦИОННАЯ СИСТЕМА, ОБРАБАТЫВАЮЩАЯ ПДН СОТРУДНИКОВ ОПЕРАТОРА

ИСПДн, в которой обрабатываются ПДн только указанных сотрудников

ИНФОРМАЦИОННАЯ СИСТЕМА, ОБРАБАТЫВАЮЩАЯ ПДН СУБЪЕКТОВ, НЕ ЯВЛЯЮЩИХСЯ СОТРУДНИКАМИ ОПЕРАТОРА

все остальные случаи, не попадающие под определение ИСПДн, обрабатывающей ПДн сотрудников оператора



ПОД ТЕРМИНОМ «СОТРУДНИК» ПОНИМАЕТСЯ РАБОТНИК В ТЕРМИНОЛОГИИ ТРУДОВОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №1119 АНАЛИЗ ДОКУМЕНТА

Требования, выполнение которых необходимо для обеспечения соответствующего уровня защищенности ПДн при их обработке в ИСПДн	Уровни защищенности			
	УЗ – 1	УЗ – 2	УЗ – 3	УЗ – 4
организация режима обеспечения безопасности помещений, в которых размещена ИСПДн	+	+	+	+
обеспечение сохранности носителей ПДн	+	+	+	+
утверждение документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей	+	+	+	+
использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз	+	+	+	+
назначение должностного лица (работника), ответственного за обеспечение безопасности ПДн в ИСПДн	+	+	+	
ограничение доступа к содержанию электронного журнала сообщений только для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей	+	+		
автоматическая регистрация в электронном журнале безопасности изменений полномочий сотрудников оператора по доступу к ПДн, содержащимся в ИСПДн	+			
создание структурного подразделения, ответственного за обеспечение безопасности ПДн в ИСПДн, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности	+			

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №1119
АНАЛИЗ ДОКУМЕНТА

использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз

- ✔ использование средств защиты информации, не прошедших процедуру оценки соответствия, не может считаться фактором, снижающим вероятности каких-либо угроз
- ✔ при этом требование использования средств защиты информации, прошедших процедуру оценки соответствия, содержится в пункте 3 части 2 статьи 19 ФЗ-152
- ✔ на настоящее время под упомянутой в ПП РФ №1119 процедурой оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации понимается именно сертификация
- ✔ текущие сертификаты соответствия средств защиты информации переоформлению не подлежат

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №1119
АНАЛИЗ ДОКУМЕНТА

ограничение доступа к содержанию электронного журнала сообщений только для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей

- ✔ под электронным журналом сообщений понимается электронный журнал, в котором автоматизированными средствами информационной системы регистрируются запросы пользователей информационной системы на получение ПДн, а также факты предоставления ПДн по этим запросам

автоматическая регистрация в электронном журнале безопасности изменений полномочий сотрудников оператора по доступу к ПДн, содержащимся в ИСПДн

- ✔ под электронным журналом безопасности понимается электронный журнал, в котором отражены полномочия сотрудника оператора по доступу к ПДн, содержащимся в информационной системе

КАК ДЕЙСТВОВАТЬ ОПЕРАТОРАМ, ЗАВЕРШИВШИМ РАБОТЫ ПО ЗАЩИТЕ ПДН?

Как действовать операторам, которые только что закончили работы по защите ПДн (приведение процессов обработки ПДн и ИСПДн в соответствие с требованиями законодательства РФ, построение СЗПДн), которые выполнялись на основании требований утратившего силу Постановления №781 и нормативных правовых актов, разработанных во исполнение Постановления №781?

Позиция ФСТЭК России

Нормативный правовой акт ФСТЭК России, устанавливающий состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, будет применяться к информационным системам персональных данных, для которых решение о создании системы защиты информации будет принято после вступления в силу указанного нормативного правового акта.

Позиция ФСБ России

В настоящее время ПП РФ №1119 уже является действующим нормативным документом и каких-либо отсрочек в части выполнения установленных им требований не предусматривает. В то же время, в ходе проводимых ФСБ России контрольных мероприятий необходимость наличия определенного времени на доработку системы защиты персональных данных (в случае, если такая необходимость возникла в связи с принятием ПП РФ №1119) будет учитываться.

ОПЫТ ПРОВЕДЕНИЯ ПРОВЕРОК РОСКОМНАДЗОРА

ОСНОВНЫЕ РЕКОМЕНДАЦИИ ОПЕРАТОРАМ

НОРМАТИВНАЯ БАЗА

АДМИНИСТРАТИВНЫЙ РЕГЛАМЕНТ
исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных

Федеральный закон от 26.12.2008г. №294-ФЗ
«О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»

ПРАВА И ОБЯЗАННОСТИ

должностных лиц при осуществлении государственного контроля (надзора)

лиц, в отношении которых осуществляются мероприятия по контролю

ФОРМАТ ПРОВЕДЕНИЯ ПРОВЕРКИ

ПРОВЕРКИ РОСКОМНАДЗОРА

ПЛАНОВЫЕ И ВНЕПЛАНОВЫЕ

ДОКУМЕНТАРНЫЕ И ВЫЕЗДНЫЕ

- ✔ Ежегодный план проведения плановых проверок (размещается на официальном сайте)
- ✔ Срок проведения как плановой, так и внеплановой проверки не может превышать двадцать рабочих дней.
- ✔ В случае возникновения необходимости срок проведения проверки может быть продлен, но на срок не более двадцати рабочих дней

С ЧЕГО ВСЁ НАЧИНАЕТСЯ

ПРИКАЗ О ПРОВЕДЕНИИ ПРОВЕРКИ

УВЕДОМЛЕНИЕ О ПРОВЕДЕНИИ ПРОВЕРКИ

ПРОГРАММА ПРОВЕДЕНИЯ ПЛАНОВОЙ ПРОВЕРКИ
(+ ПЕРЕЧЕНЬ ПРОВЕРЯЕМЫХ ТРЕБОВАНИЙ)

РЕКОМЕНДАЦИИ ОПЕРАТОРАМ

РЕКОМЕНДАЦИЯ №1

- ✔ Соберите всю имеющуюся документацию;
- ✔ Проведите самоаудит, основываясь на перечне проверяемых требований, указанных в программе проведения проверки.

ВАЖНО!

- ✔ Все ли пункты требований перекрываются вашей организационно-распорядительной документацией?
- ✔ Все ли требования реально реализованы?

РЕКОМЕНДАЦИИ ОПЕРАТОРАМ

РЕКОМЕНДАЦИЯ №2

- ✔ Оповещение работников о проведении проверки на территории офиса;
- ✔ Напоминание всем о существовании организационно-распорядительной документации и необходимости ознакомится с ней при необходимости

ВАЖНО!

- ✔ Все реально ознакомлены с документами, и это зафиксировано?
- ✔ Реально ли исполняются ли требования ?

РЕКОМЕНДАЦИИ ОПЕРАТОРАМ

РЕКОМЕНДАЦИЯ №3

- ✔ «Свежесть» предоставляемых документов;
- ✔ Создаём хорошее впечатление (чистота и порядок).

ВАЖНО!

- ✔ Донести до проверяющих мысль о том, что мы добросовестные операторы и стремимся выполнить закон!
- ✔ В случае привлечения внешних консультантов, оповестите об этом ответственное лицо со стороны проверяющих!

БОЛЬШИЙ ИНТЕРЕС СО СТОРОНЫ ПРОВЕРЯЮЩИХ

- ✔ Организация пропускного режима;
- ✔ Бухгалтерия;
- ✔ Отдел кадров;
- ✔ Сервисы, предоставляемые через сайт.

РЕКОМЕНДАЦИИ ОПЕРАТОРАМ

РЕКОМЕНДАЦИЯ №4

- ✔ Протокол/акт проверки (внимание к деталям).

ВАЖНО!

- ✔ Каждое замечание/недостаток должно иметь под собой законное основание.
- ✔ Всегда письменно излагайте свои возражения.

РЕКОМЕНДАЦИИ ОПЕРАТОРАМ

РЕКОМЕНДАЦИЯ №5

- ✔ Оперативное реагирование на замечания;
- ✔ Документальное подтверждение того, что недостаток устранён.

ВАЖНО!

- ✔ Проверяющие лояльно относятся к возможности устранения выявленных недостатком.
- ✔ Реагировать необходимо не только на недостатки, указанные в протоколе, но и на устные замечания.

РЕКОМЕНДАЦИИ ОПЕРАТОРАМ

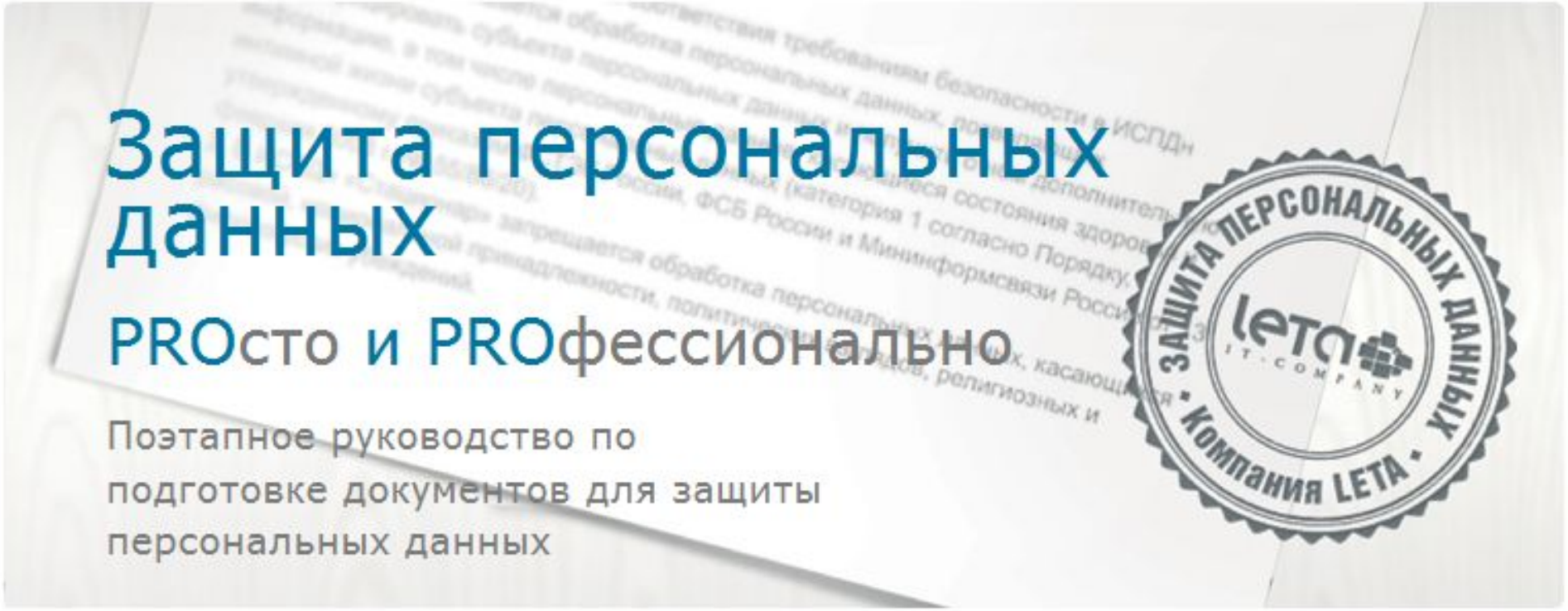
РЕКОМЕНДАЦИЯ №6

- ✔ С пониманием отнеситесь к запросам информации со стороны проверяющих… им же тоже отчет надо писать.

ВАЖНО!

- ✔ По каждому пункту запроса проверяющий должен получить документально подтвержденный ответ.
- ✔ Не игнорируйте запросы, даже если они касаются предоставления информации о процессах, которых нет в Вашей организации.
- ✔ Все документы, на которые вы ссылаетесь в справках и информационных письмах должны быть так же предоставлены.

ЗНАКОМСТВО С СЕРВИСОМ



leta
IT-COMPANY

152pro – онлайн-эксперт в вопросах выполнения закона «О персональных данных» !

ФЕДЕРАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО

26 января 2007 года вступил в силу
Федеральный закон № 152-ФЗ «О персональных данных»

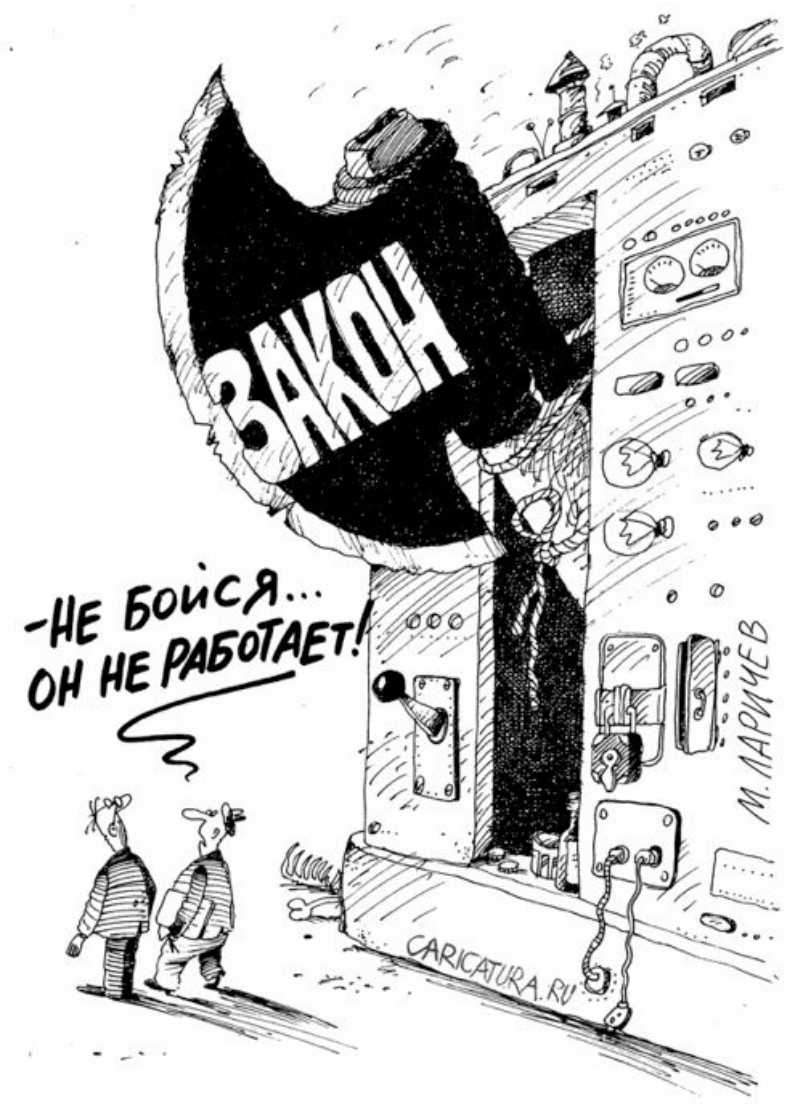
Закон обязывает Операторов персональных данных привести свои информационные системы персональных данных (ИСПДн) в соответствие требованиям Закона и регулирующих органов.

Регулирующими органами, ответственными за контроль соблюдения требований Закона, а также за формирование отдельных требований в рамках своих полномочий, определены :

Роскомнадзор

ФСТЭК России

ФСБ России


ЗАКОН
-НЕ БОЙСЯ... ОН НЕ РАБОТАЕТ!
М. ЛАРИЧЕВ
CARICATURA.RU

Количество выявленных в ходе проверок нарушений в 2011 году (2250) в 4 раза превысило показатели 2009 года (557), **общая сумма** наложенных **штрафов** за трехлетний период **возросла в 100 раз** и составила более 12 млн. рублей.

Если, по состоянию на конец 2009 года Роскомнадзором было рассмотрено 465 обращений, то в 2011 году эта цифра составила 3920, что демонстрирует **8-кратный рост количества рассмотренных обращений граждан**

Из отчета Роскомнадзора за 2011 г.

Обработка персональных данных без согласия субъекта (субъектов) персональных данных в случаях, когда такое согласие обязательно, а равно обработка персональных данных с нарушением установленной законом формы согласия субъекта (субъектов) персональных данных, с целью извлечения дохода -

влечет **наложение административного штрафа** на граждан – от четырех тысяч до пяти тысяч рублей; на должностных лиц – от десяти тысяч до пятнадцати тысяч рублей; **на индивидуальных предпринимателей** – в величине, равной **сумме выручки** от реализации товаров (услуг) с использованием персональных данных, обработка которых осуществлялась без согласия субъекта (субъектов) персональных данных …. **за календарный год…., но не менее 300 тысяч рублей**, на **юридических лиц** – ….**не менее 500 тысяч рублей**.

Проект Федерального Закона «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»

СТАТИСТИКА

Крупный бизнес

Малый и средний бизнес

ОСНОВНЫЕ ПРОБЛЕМЫ

Слабая осведомленность о существовании закона «О персональных данных»

Отсутствие денежных средств

Отсутствие квалифицированных кадров в штате

Непонимание / Неверное толкование норм законодательства

Ко мне не придут !

ЧТО ТРЕБУЕТСЯ

Выполнение закона 152-ФЗ «О персональных данных»

Проведение орг.мероприятий

Установка средств защиты

ОСНОВНЫЕ ПРОБЛЕМЫ

Слабая осведомленность о существовании закона «О персональных данных»

Отсутствие денежных средств

Отсутствие квалифицированных кадров в штате

Непонимание / Неверное толкование норм законодательства

Ко мне не придут !

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Методические рекомендации по выполнению требований закона «О персональных данных» – 2009 г.

Выход: создание онлайн-системы (консультанта), который поможет выполнить требования законодательства:

- разъяснение норм законодательства
- подготовка пакета необходимых документов
- подбор средств защиты информации
- индивидуальные онлайн консультации

152ПР

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

ШАГ 1

Инициация работ по защите персональных данных

ОПИСАНИЕ ШАГА | ССЫЛКИ И РАЗЪЯСНЕНИЯ

В начале всех работ по выполнению требований федерального закона «О персональных данных» в вашей организации необходимо назначить ответственного (ответственных) за организацию обработки и защиты персональных данных.

Действующая нормативная база предусматривает необходимость наличия в организации лиц, исполняющих следующие "роли":

Лицо, **ответственное за организацию обработки ПДн** (см. ст. 22.1 Федерального закона от 27.07.2006 №ФЗ-152 "О персональных данных"). Как правило, таким лицом назначается работник, который имеет широкие полномочия и от имени руководителя организации может организовать все работы, необходимые для реализации требований Закона (в т.ч. способен самостоятельно принимать управленческие решения). Примеры: Заместитель генерального директора по административным вопросам; Заместитель генерального директора по операционной деятельности, Директор по безопасности; Технический директор; Директор по персоналу.

Обязанности данного лица:

- осуществлять *внутренний контроль* за соблюдением в организации (в т.ч. со стороны работников) законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- *доводить до сведения* работников организации положения

Подготовка документов (4/6)

Приказ о проведении работ по организации обработки и защиты персональных данных
Ввести данные

План проведения работ по организации обработки и защиты персональных данных
Ввести данные

Изменения в должностную инструкцию работника, ответственного за организацию обработки ПДн
Скачать

Изменения в должностную инструкцию работника, ответственного за обеспечение безопасности ПДн
Скачать

Изменения в должностную инструкцию работника, ответственного за организацию обработки и защиты ПДн
Скачать

Изменения в положение о структурном подразделении, ответственном за обеспечение безопасности ПДн
Скачать

Чек-лист выполненных задач (0/5)

- [ ] Определить лицо, ответственное за организацию обработки персональных данных
- [ ] Определить лицо или структурное подразделение, ответственное за обеспечение безопасности персональных данных
- [ ] Внести изменения в должностную инструкцию работника, ответственного за организацию обработки персональных данных
- [ ] Внести изменения в должностную инструкцию лица (в положение о подразделении), ответственного за обеспечение безопасности персональных данных
- [ ] Составить план и издать приказ о проведении работ по организации обработки и защиты персональных данных

Корзина решений

Alexander Bondarenko [LETA (Test)]

ВЫЙТИ

ГОТОВНОСТЬ 13%

СООБЩЕНИЯ 0/0

Заполните необходимую информацию

- [ ] Урегулирование убытков по договорам автострахования
- [ ] Урегулирование убытков по договорам личного страхования
- [ ] Урегулирование убытков по договорам страхования имущества

Процессы, связанные с деятельностью энергосбытовых компаний

- [ ] Биллинг (съем показаний приборов учета потребления энергоресурсов, подготовка счетов для оплаты энергоресурсов)
- [ ] Заключение, сопровождение, расторжение договоров энергоснабжения
- [ ] Оформление льгот на энергоснабжение
- [ ] Прием платежей за услуги энергоснабжения, взыскание задолженностей по договорам энергоснабжения

Процессы, связанные с гостиничным бизнесом

- [x] Бронирование гостиничных номеров
- [x] Контроль услуг, оказанных клиентам
- [x] Организация корпоративных мероприятий, конференций
- [x] Регистрация клиентов гостиницы и их гостей (граждане РФ, иностранные граждане)

Процессы, связанные с организацией пассажироперевозок

- [ ] Бронирование и продажа авиа, ж/д билетов
- [ ] Заключение договора перевозки (перевозка пассажиров, багажа, предоставление транспорта)
- [ ] Оформление льгот
- [ ] Оформление программ лояльности для клиентов
- [ ] Прием заявок на такси
- [ ] Проведение разбирательств по качеству предоставляемых услуг
- [ ] Регистрация пассажиров

Процессы, связанные с деятельностью кадровых агентств

- [ ] Ведение базы соискателей
- [ ] Обработка резюме и проведение собеседования с соискателями
- [ ] Оценка персонала работодателя (аттестации, тестирования)

0%

ШАГ 9

задач (0/5)

генерального директора по операционной деятельности, Директор по безопасности; Технический директор; Директор по персоналу.

Обязанности данного лица:

- осуществлять *внутренний контроль* за соблюдением в организации (в т.ч. со стороны работников) законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- *доводить до сведения* работников организации положения

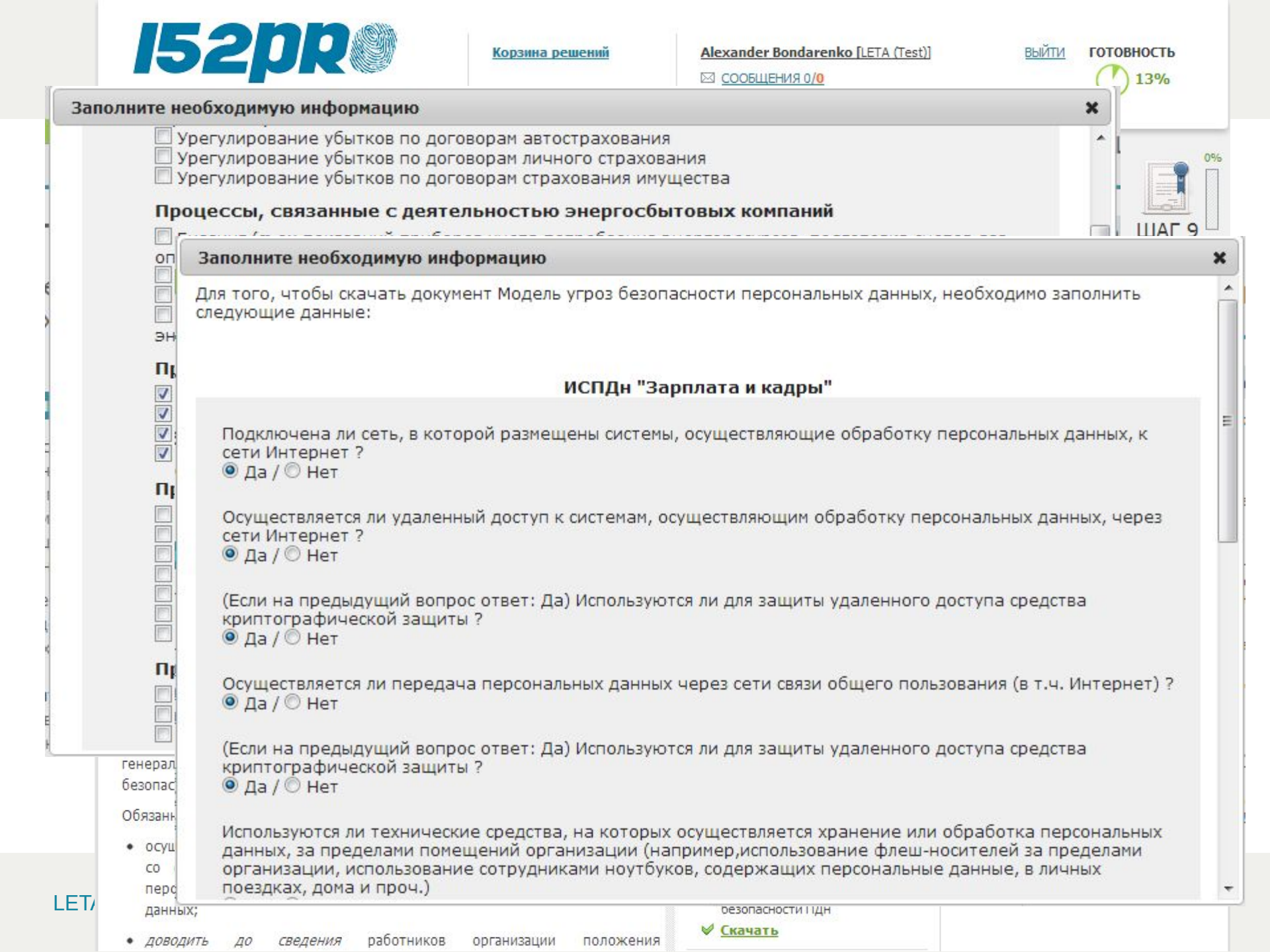
ответственного за организацию обработки и защиты ПДн

Скачать

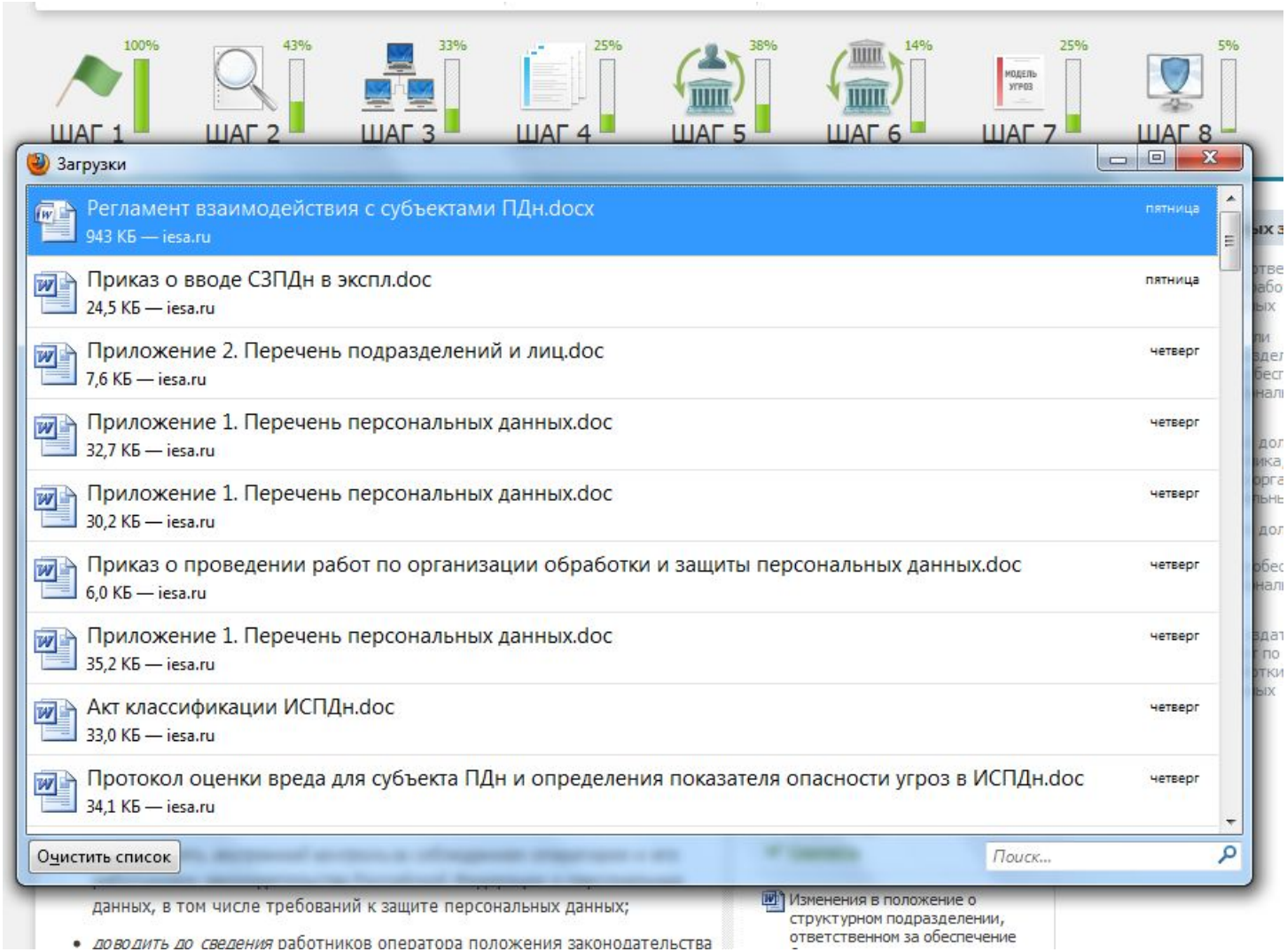
Изменения в положение о структурном подразделении, ответственном за обеспечение безопасности ПДн

Скачать

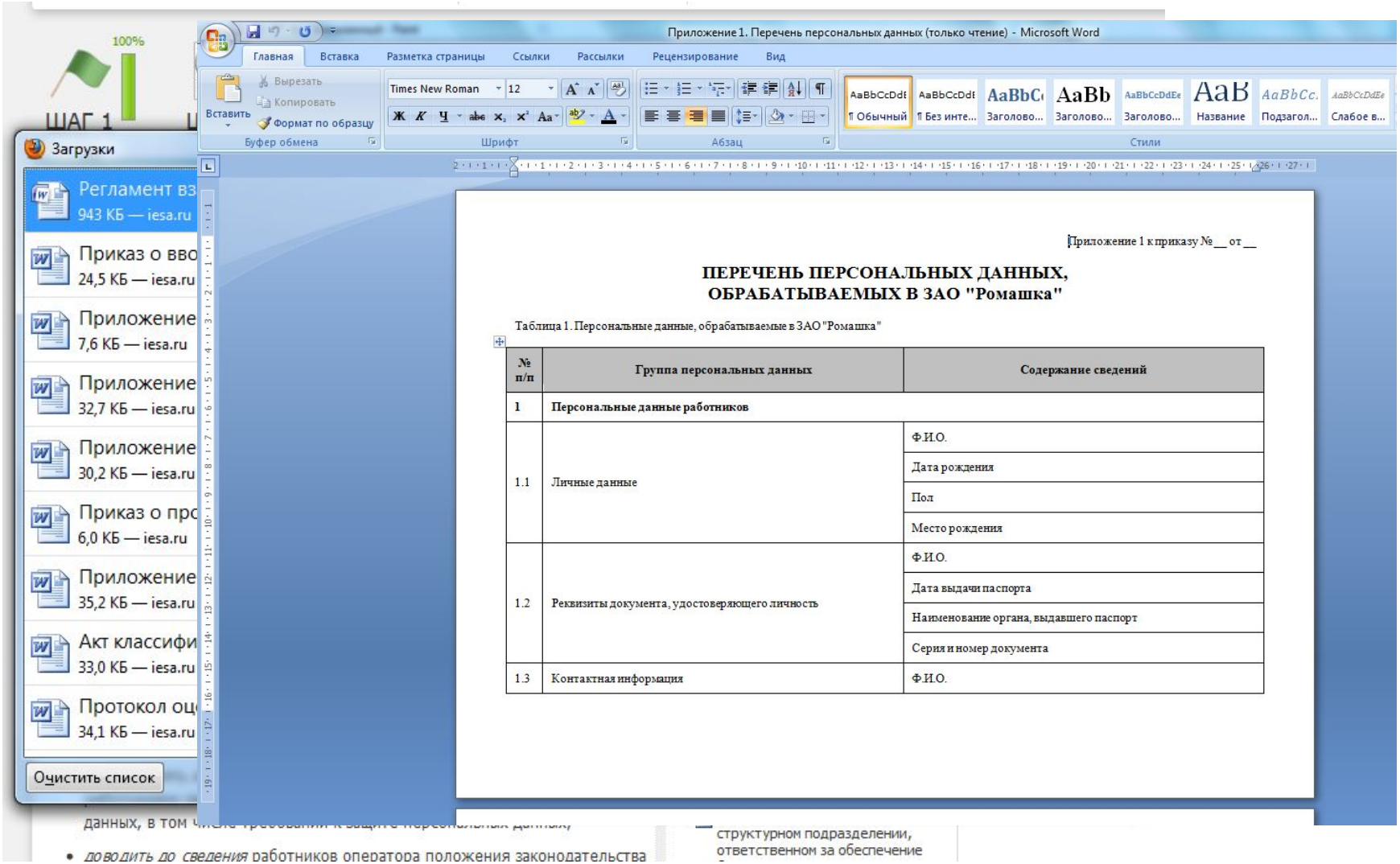
LETA


Корзина решений
Alexander Bondarenko [LETA (Test)]
ВЫЙТИ
ГОТОВНОСТЬ
СООБЩЕНИЯ 0/0
13%
Заполните необходимую информацию
Урегулирование убытков по договорам автострахования
Урегулирование убытков по договорам личного страхования
Урегулирование убытков по договорам страхования имущества
Процессы, связанные с деятельностью энергосбытовых компаний
0%
ШАГ 9
Заполните необходимую информацию
Для того, чтобы скачать документ Модель угроз безопасности персональных данных, необходимо заполнить следующие данные:
ИСПДн "Зарплата и кадры"
Подключена ли сеть, в которой размещены системы, осуществляющие обработку персональных данных, к сети Интернет ?
Да / Нет
Осуществляется ли удаленный доступ к системам, осуществляющим обработку персональных данных, через сети Интернет ?
Да / Нет
(Если на предыдущий вопрос ответ: Да) Используются ли для защиты удаленного доступа средства криптографической защиты ?
Да / Нет
Осуществляется ли передача персональных данных через сети связи общего пользования (в т.ч. Интернет) ?
Да / Нет
(Если на предыдущий вопрос ответ: Да) Используются ли для защиты удаленного доступа средства криптографической защиты ?
Да / Нет
Используются ли технические средства, на которых осуществляется хранение или обработка персональных данных, за пределами помещений организации (например,использование флеш-носителей за пределами организации, использование сотрудниками ноутбуков, содержащих персональные данные, в личных поездках, дома и проч.)
безопасности ПДн
Скачать
LETA
данных;
доводить до сведения работников организации положения

РЕШЕНИЕ ЛЕТА



РЕШЕНИЕ ЛЕТА



ШАГ 1

Инициация работ по защите персональных данных

ОПИСАНИЕ ШАГА | ССЫЛКИ И РАЗЪЯСНЕНИЯ

В начале всех работ по выполнению требований федерального закона «О персональных данных» в вашей организации необходимо назначить ответственного (ответственных) за организацию обработки и защиты персональных данных.

Действующая нормативная база предусматривает необходимость наличия в организации лиц, исполняющих следующие "роли":

Лицо, **ответственное за организацию обработки ПДн** (см. ст. 22.1 Федерального закона от 27.07.2006 №ФЗ-152 "О персональных данных"). Как правило, таким лицом назначается работник, который имеет широкие полномочия и от имени руководителя организации может организовать все работы, необходимые для реализации требований Закона (в т.ч. способен самостоятельно принимать управленческие решения). Примеры: Заместитель генерального директора по административным вопросам; Заместитель генерального директора по операционной деятельности, Директор по безопасности; Технический директор; Директор по персоналу.

Обязанности данного лица:

- осуществлять *внутренний контроль* за соблюдением в организации (в т.ч. со стороны работников) законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- *доводить до сведения* работников организации положения

Подготовка документов (4/6)

Приказ о проведении работ по организации обработки и защиты персональных данных
Ввести данные

План проведения работ по организации обработки и защиты персональных данных
Ввести данные

Изменения в должностную инструкцию работника, ответственного за организацию обработки ПДн
Скачать

Изменения в должностную инструкцию работника, ответственного за обеспечение безопасности ПДн
Скачать

Изменения в должностную инструкцию работника, ответственного за организацию обработки и защиты ПДн
Скачать

Изменения в положение о структурном подразделении, ответственном за обеспечение безопасности ПДн
Скачать

Чек-лист выполненных задач (0/5)

- [ ] Определить лицо, ответственное за организацию обработки персональных данных
- [ ] Определить лицо или структурное подразделение, ответственное за обеспечение безопасности персональных данных
- [ ] Внести изменения в должностную инструкцию работника, ответственного за организацию обработки персональных данных
- [ ] Внести изменения в должностную инструкцию лица (в положение о подразделении), ответственного за обеспечение безопасности персональных данных
- [ ] Составить план и издать приказ о проведении работ по организации обработки и защиты персональных данных

ШАГ 1

ШАГ 1

Инициаци

ОПИСАНИЕ ША

В начале все
персональных
ответственно
персональных

Действующая
организации л

Лицо, ответ
Федерального
правило, так
полномочия
работы, необ
самостоятель
генерального
генерального
безопасности

Обязанности

- осуществл
  со стороны
  персональ
  данных;
- доводить

Решение для ИСПДН ИСПДн "Зарплата и кадры"

Средство антивирусной защиты NOD32

ESET NOD32 Business Edition - централизованная защита файловых серверов и рабочих станций от троянских и шпионских программ, червей, рекламного ПО, фишинг-атак и других интернет-угроз в организациях любого масштаба.
Решение включает в себя приложение ESET Remote Administrator (ERA), которое обеспечивает централизованное администрирование антивирусного решения в корпоративных сетевых средах предприятия или глобальных сетях.
С единой консоли администрирования ESET можно удаленно устанавливать и управлять решениями ESET на рабочих станциях и серверах под управлением ОС Windows, Linux, BSD, Solaris и MacOS, запускать сканирование рабочих станций и серверов, удаленно настраивать конечные точки, быстро реагировать на события безопасности в сети, создавать отчеты, обновлять базы вирусных сигнатур, создавать внутри сети серверы для локального обновления продуктов ESET («зеркала»), которые позволяют существенно сократить внешний интернет-трафик.

Данное решение позволяет закрыть следующие урозы: несанкционированный доступ к информации внешнего нарушителя за счет внедрения вредоносного программного обеспечения, разглашение, уничтожение, блокирование или изменение информации в результате запуска/установки ПО, содержащего вредоносный код персоналом организации

Введите необходимое количество лицензий

Средство защиты от несанкционированного доступа SecretNet

Secret Net является сертифицированным средством защиты информации от несанкционированного доступа и позволяет привести автоматизированные системы в соответствие требованиям регулирующих документов.
Secret Net обеспечивает защиту отдельных рабочих станций в небольших организациях и вычислительных инфраструктур класса Enterprise.
Сетевой вариант Secret Net может быть успешно развернут в сложной доменной сети с большим количеством филиалов.
Основные возможности Secret Net:
аутентификация пользователей;
обеспечение разграничения доступа к защищаемой информации и устройствам;
доверенная информационная среда;
контроль каналов распространения конфиденциальной информации;
контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной информации;
централизованное управление политиками безопасности, позволяет оперативно реагировать на события НСД;
оперативный мониторинг и аудит безопасности;
масштабируемая система защиты, возможность применения Secret Net (сетевой вариант) в организации с большим количеством филиалов.

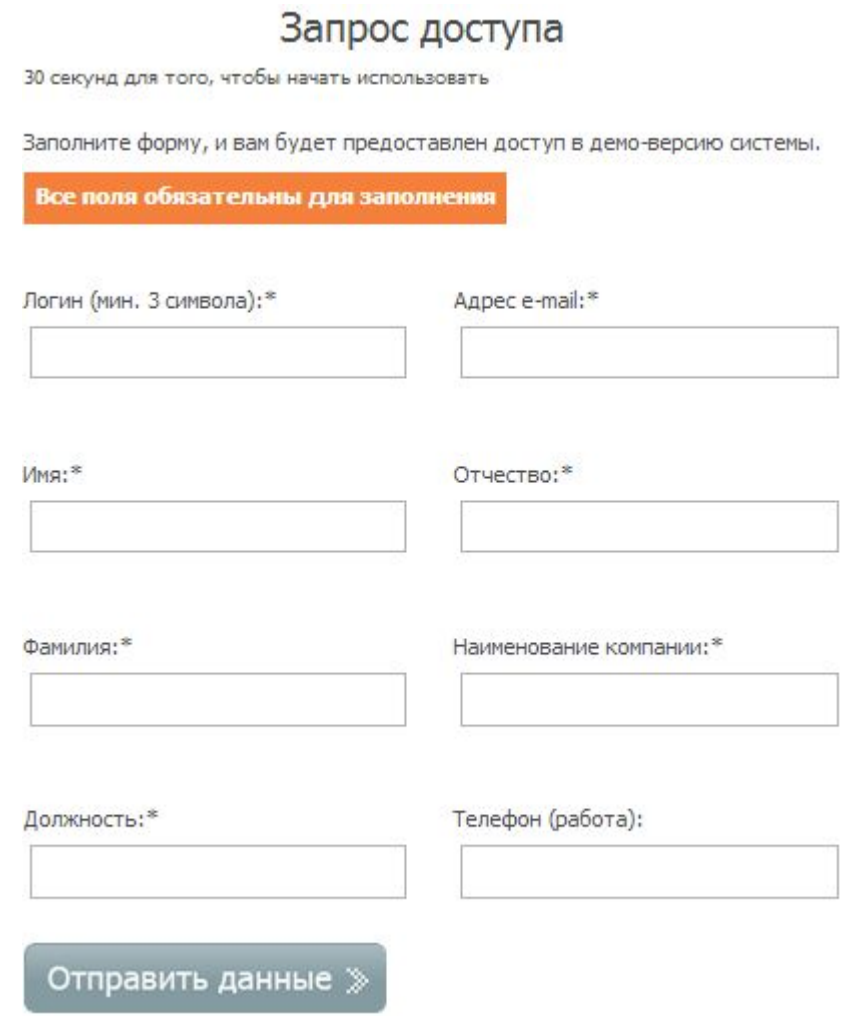
Данное решение позволяет закрыть следующие урозы: несанкционированный доступ к информации сторонних лиц, имеющих доступ на территорию организации (посетителей, клиентов, партнеров, подрядчиков), за счет использования оставленных без присмотра незаблокированных терминалов (АРМ, серверов)

Введите необходимое количество лицензий

Средство криптографической защиты информации Secret Disk

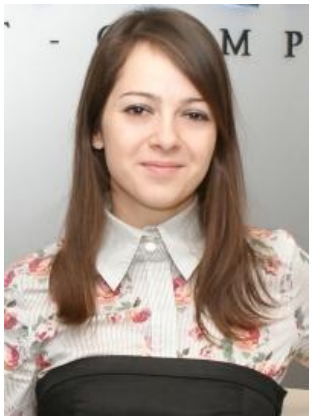
Secret Disk 4 – система защиты конфиденциальной информации и персональных данных, хранящихся и обрабатываемых на персональном компьютере или ноутбуке.
Назначение Secret Disk 4:
защита от несанкционированного доступа и раскрытия конфиденциальности информации, хранящейся и обрабатываемой на персональном

РЕШЕНИЕ ЛЕТА



КОНТАКТНАЯ ИНФОРМАЦИЯ

Максимов Максим
Руководитель отдела консалтинга
Mmaksimov@leta.ru



Садовникова Ольга
Ведущий консультант по информационной безопасности
OSadovnikova@leta.ru

Бондаренко Александр
Технический директор
ABondarenko@leta.ru

Компания LETA
109129, Россия, Москва, ул. 8-я Текстильщиков, д.11, стр. 2
Тел./факс: +7 (495) 921-1410
www.leta.ru