Персональные данные. Вводная

Slides before 1st Section Divider

Unused Section Space 1

Классификация персональных данных

Практика ?!

Unused Section Space 2

Что же делать ?

Unused Section Space 3

Unused Section Space 4


TechDays.ru

Персональные данные. Вводная

pptPlex Section Divider

The slides after this divider will be grouped into a section and given the label you type above. Feel free to move this slide to any position in the deck.

Персональные данные

Дмитрий Колесников
Ст. инженер
УФСКН России по Саратовской области

Notes (hidden)

- Зачем появился «Закон о защите персональных данных»?
- Федеральные законы и основные нормативно-правовые акты (НПА) регулирующие отношения связанные с обработкой персональных данных
- Что относится к персональным данным?
- Вопросы?
- Какие мероприятия по защите ПДн необходимо провести?
- Какая может быть ответственность за нарушение закона?
- Вопросы?

NEXT: <next slide title>

Зачем появился «Закон о защите персональных данных»?

- Вступление во Всемирную торговую организацию, потребовало принятия международных Конвенций по автоматизированной обработке персональных данных, напрямую неприменимых к Российскому законодательству, что и повлекло необходимость создания собственных законов в этой области права.

- Необходимость совершенствования системы государственного управления, ее контрольно-надзорных, а также правоприменительных функций, путем создания Системы персонального учета населения Российской Федерации.

Федеральные законы и основные НПА регулирующие отношения связанные с обработкой персональных данных

Федеральные законы

- 160-ФЗ от 19.12.2005 г. «О ратификации Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных»
- 152-ФЗ от 27.07.2006 г. «О защите персональных данных»

Постановления Правительства РФ

- 2007 г. № 781
- 2008 г. № 419
- 2008 г. № 687

Методические документы «регуляторов»

- ФСБ России
- ФСТЭК Росси
- Россвязь-комнадзор

Постановления правительства

- Постановление Правительства РФ № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 17.11.2007 г.
- Постановление Правительства РФ от 2 июня 2008 г. № 419 «О федеральной службе по надзору в сфере связи и массовых коммуникаций».
- Постановление Правительства РФ от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"

- Перечень сведений конфиденциального характера, Указ Президента РФ № 188 от 06.03.1997 г. (в ред. Указа Президента РФ от 23.09.05 г. № 1111)

Регулирующие документы ФСБ России

- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные ФСБ 21 февраля 2008 года.
- «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащих сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в персональных системах персональных данных», утвержденные ФСТЭК 21 февраля 2008 года.

Методические документы ФСТЭК России

- Приказ ФСТЭК, ФСБ и Мининформсвязи от 13 февраля 2008 г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»
- «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», утвержденные ФСТЭК 15 февраля 2008 года.
- «Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных», утвержденная ФСТЭК 14 февраля 2008 года.
- «Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных», утвержденная ФСТЭК 15 февраля 2008 года.
- «Рекомендации по обеспечению безопасности персональных данных при их обработке, в информационных системах персональных данных», утвержденные ФСТЭК 15 февраля 2008 года.

Для получения перечисленных документов для служебного пользования можно обратиться во ФСТЭК России.

Приказы Россвязькомнадзора

- Приказ Россвязькомнадзора от 28 марта 2008 г. № 154 «Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных»
- Приказ Россвязькомнадзора от 17 июля 2008 г. №8 «Об утверждении образца формы уведомления об обработке персональных данных».

Классификация персональных данных

pptPlex Section Divider

The slides after this divider will be grouped into a section and given the label you type above. Feel free to move this slide to any position in the deck.

Что относится к персональным данным?

- 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 (Ст.3 ФЗ-152)

- «Персональные данные» означают любую информацию об определенном или поддающемся определению физическом лице (субъект данных) (ФЗ-160)

Классификация ИСПДн

При классификации типовых ИСПДн учитываются комбинации следующих признаков:

- Категория обрабатываемых данных
- Объем обрабатываемых данных

Дополнительно при классификации также учитываются следующие признаки:

- Структура ИС (автономные, локальные и распределённые)
- Режим обработки персональных данных (однопользовательские и многопользовательские)
- Режим разграничения прав доступа (равный доступ и разграничение доступа)
- Наличие подключений к Интернет и сетям общего пользования
- Местонахождение технических средств (в пределах и за пределами РФ)

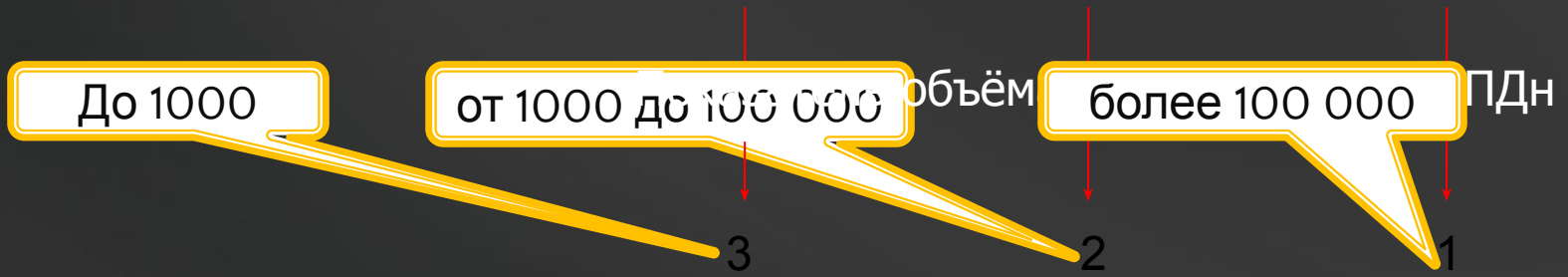
Категории ПДн

- КАТЕГОРИЯ 1 – ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни
- КАТЕГОРИЯ 2 – ПДн, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1
- КАТЕГОРИЯ 3 – ПДн, позволяющие идентифицировать субъекта персональных данных
- КАТЕГОРИЯ 4 – обезличенные и (или) общедоступные ПДн

Возможные значения показателя объема обрабатываемых данных

- ЗНАЧЕНИЕ 1 – ИСПДн обрабатывает ПДн свыше 100 000 субъектов или ПДн субъектов в пределах субъекта РФ или РФ в целом
- ЗНАЧЕНИЕ 2 – ИСПДн обрабатывает ПДн от 1 000 до 100 000 субъектов или обрабатывает ПДн субъектов работающих в отрасли экономики, в органе госвласти или проживающих в пределах муниципального образования
- ЗНАЧЕНИЕ 3 – ИСПДн обрабатывает ПДн менее 1 000 субъектов или обрабатывает ПДн субъектов в пределах одной организации

Как определяется итоговый класс типовой ИСПДн?



Категории обрабатываемых ПДн	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

Примечание: в ИСПДН 1 и 2 классов должны быть реализованы мероприятия по защите персональных данных от утечки за счёт ПЭМИН

Конец первой секции

Вопросы ?

Дмитрий Колесников
Ст. инженер
УФСКН России по Саратовской области

Что же делать ?

pptPlex Section Divider

The slides after this divider will be grouped into a section and given the label you type above. Feel free to move this slide to any position in the deck.

Персональные данные

Что же делать ?

Дмитрий Колесников
Ст. инженер
УФСКН России по Саратовской области

Ч. 2

Какая информация содержащая ПДн защищается в ИСПДн?

Во всех ИСПДн вне зависимости от класса:

- Носители на бумажной, магнитной, оптической и иной основе
- Информационные массивы в зависимости от формы представления (объекты файловой системы, баз данных) и т.п.

Дополнительно в ИСПДн 1 и 2 класса

- Информация, обрабатываемая техническими средствами

Дополнительно в ИСПДн 1 класса

- Информация в виде информативных электрических сигналов
- Информация в виде физических полей
- Акустическая (речевая) информация (в случае если предусмотрены функции голосового ввода ПДн)

СУБЪЕКТЫ ПРАВОВЫХ ОТНОШЕНИЙ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ
(ФЗ от 27 июля 2006 г. № 149--ФЗ, ст. 2)

- Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

1. Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.
2. От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

- Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в её базах данных.
- Обладатель информации, составляющей коммерческую тайну - лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении её режим коммерческой тайны. (ФЗ О коммерческой тайне №98-ФЗ от 29.07.2004 г.)

ЗАЩИТА ИНФОРМАЦИИ

(Федеральный закон от 27 июля 2006 г. № 149-ФЗ ст. 9)

- Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами. (требование для выполнения лицом, получившим доступ к определенной информации, не передавать такую информацию третьим лицам без согласия её обладателя).
- Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.
- Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение. (ФЗ 2004 г. №98 «О коммерческой тайне»).
- Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.
- Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных. (ФЗ 2006 г. №152 «О персональных данных»).

ЗАЩИТА ИНФОРМАЦИИ

(Федеральный закон от 27 июля 2006 г. № 149-ФЗ ст. 16)

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Что является правовым основанием обработки персональных данных?

- Наличие согласия субъектов ПДн (ФЗ 2006 г. № 152 ст. 6 п.1,10,11), либо иные законодательные основания (ФЗ 2006 г. № 152 ст. 6 п.2)
- Наличие в учредительных документах видов экономической деятельности, связанных с обработкой данных и созданием (использованием) баз данных и информационных ресурсов (ОКВЭД 72.30, 72.40)

Что необходимо сделать руководителями организаций и предприятий в сфере защиты персональных данных?

1. Оформить правовые основания обработки персональных данных
2. Определить класс своей ИСПДн
3. Создать систему защиты информационной системы персональных данных (далее по тексту ИСПДн)
4. Разработать документы, регламентирующие обработку персональных данных в организации
5. Уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных
6. Провести аттестацию (декларирование соответствия) по требованиям безопасности информации
7. Организовать повышение квалификации сотрудников в области защиты персональных данных
8. Получить необходимые лицензии (для ИСПДН 1,2 и распределённых 3 класса)

Какие мероприятия по защите ПДн необходимо провести?

Мероприятия по защите ПДн

Защита от НСД к информации ПДн

- обеспечение целостности
- управление доступом
- регистрация и учет
- межсетевое экранирование
- антивирусная защита
- анализ защищенности (сканеры безопасности)
- обнаружение уязвимостей

Сфера деятельности регулируемая ФСТЭК России

ЗИ от утечки по техническим каналам

- использование сертифицированных технических средств
- использование сертифицированных средств ЗИ
- размещение объектов защиты на максимально-возможном расстоянии относительно границ КЗ
- обеспечение электромагнитной развязки
- обеспечение развязки цепей электропитания
- размещение трансформаторных подстанций внутри КЗ

Применение средств криптографической защиты информации и обнаружение вторжений

1. Применение средств сертифицированных СКЗИ
2. Применение сигнатурных и аномальных систем обнаружения вторжений

Сфера деятельности регулируемая ФСБ России

Примечание: «Основные мероприятия …» п. 2.2 Мероприятия по обеспечению безопасности ПДн формируются в зависимости от класса ИСПДн с учётом возможного возникновения угроз безопасности ….

Что?

Subtitle color

Практика ?!

pptPlex Section Divider

The slides after this divider will be grouped into a section and given the label you type above. Feel free to move this slide to any position in the deck.

Какие документы необходимо иметь организации обрабатывающей ПДн

Материалы проектирования СЗИ от НСД ИСПДн

1. Материалы предпроектного исследования
2. Результаты технического проектирования (материалы разработки и обоснования мероприятий по защите ПДн)
3. Результаты опытной эксплуатации и итоговых (аттестационных) испытаний

Эксплуатационные документы

1. Приказы
2. Акты
3. Технические журналы
4. Инструкции по эксплуатации и правила пользования
5. Форма и соглашения
6. Перечени
7. Матрица доступа

и т.п.

Организационно-распорядительные документы

1. Положение о персональных данных
2. Руководство специалиста (ответственного) по защите ПДн (администратора безопасности ПДн)
3. Технологический регламент обработки персональных данных (на всех этапах жизненного цикла ИСПДн)
4. Положение о системе делопроизводства (документооборота на бумажных носителях)

Примечание: указанная документация создаёт необходимую основу для осуществления контроля и надзора за обработкой персональных данных со стороны уполномоченных органов (ФСБ, ФСТЭК, Россвязькомнадзора).

Уведомление об обработке ПДн

ФЗ № 152. Статья 25

1. Оператор **до начала обработки персональных данных** обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

...

4) являющихся общедоступными персональными данными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

...

О сертификации средств защиты

п. 5 Постановление правительства РФ 2007 г. № 781

Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

п. 3.3 «Основных мероприятий…»

Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации

п. 4.2 «Основных мероприятий»

ПО ИСПДн должно сертифицироваться на отсутствие недекларированных возможностей

п. 4.3 «Основных мероприятий» указывает на сертификацию по НДВ только для выделенных и встроенных в системное и прикладное ПО средств защиты

ЕСЛИ СЕРТИФИЦИРОВАННЫЕ СРЕДСТВА ОТСУТСТВУЮТ, ОПЕРАТОР ОБЯЗАН СЕРТИФИЦИРОВАТЬ ТЕ РЕШЕНИЯ, КОТОРЫЕ БУДЕТ ИСПОЛЬЗОВАТЬ

О сертификации средств криптографической защиты информации

«**Типовые требования … » ФСБ России**

2.1 … Обеспечение безопасности персональных данных с использованием криптосредств должно осуществляться в соответствии с:

Приказом ФСБ России от 9 февраля 2005 г. № 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)

Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)

… 2. Для криптографической защиты информации конфиденциального характера должны использоваться СКЗИ, удовлетворяющие требованиям по безопасности информации, устанавливаемым в соответствии с законодательством Российской Федерации.

«**Методические рекомендации … » ФСБ России**

3.1 п.7 Для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться сертифицированные в системе сертификации ФСБ России …

Что?

Subtitle color

Аттестация или декларирование соответствия?

- СПДн 1-2 класса
  обязательная аттестация
- ИСПДн 3-го класса
  декларирование соответствия
  или обязательная аттестация (по решению оператора)
- ИСПДн 4-го класса
  оценка соответствия (по решению оператора)

Что такое аттестация?

п. 1.4 Положение по аттестации объектов информатизации по требованиям безопасности информации

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России.

Наличие на объекте информатизации действующего "Аттестата соответствия" дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленными в "Аттестате соответствия".

Что такое декларирование соответствия?

ст.24 ФЗ 2002 г. № 184 «О техническом регулировании»
Декларирование соответствия осуществляется на основании собственных доказательств формируемых заявителем самостоятельно в целях подтверждения соответствия продукции требованиям технических регламентов. «В качестве доказательственных материалов используются техническая документация, результаты собственных исследований (испытаний) и измерений и (или) другие документы, послужившие мотивированным основанием для подтверждения соответствия продукции требованиям технических регламентов. Состав доказательственных материалов определяется соответствующим техническим регламентом»

Примечание: Регистрацию деклараций о соответствии осуществляют органы по сертификации аккредитованные в установленном порядке в соответствии с постановлением Правительства РФ 2008 г. № 1028 («Положение о формировании и ведении единого реестра деклараций о соответствии …»).

О необходимости получения лицензий?

Операторы ИСПДн 1, 2 классов и распределенных информационных систем 3 класса должны получить лицензию на осуществление деятельности по технической защите конфиденциальной информации в установленном порядке (п.3.14 «Основных мероприятий…»)

На деятельность в области шифрования необходимо получить лицензию ФСБ (в случае использования средств криптографической защиты информации)

Примечание: Порядок лицензирования деятельности по технической защите информации определяется постановлением Правительства РФ 2006 г. № 504. Лицензирование деятельности связанной с шифровальными (криптографическими) средствами осуществляется в соответствии с постановлением Правительства РФ 2007 г. № 957

Что такое лицензирование?

Лицензирование – мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением действия лицензий в случае административного приостановления деятельности лицензиатов за нарушение лицензионных требований и условий, возобновлением или прекращением действия лицензий, аннулированием лицензий, контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий, ведением реестров лицензий, а также с предоставлением в установленном порядке заинтересованным лицам сведений из реестров лицензий и иной информации о лицензировании;

Лицензии необходимые оператору

Лицензия на право деятельности по технической защите конфиденциальной информации — **ФСТЭК**

Примечание: Порядок лицензирования деятельности по технической защите информации определяется постановлением Правительства РФ 2006 г. № 504.

Лицензия на право деятельности по техническому обслуживанию шифровальных (криптографических) средств — **ФСБ**

Примечание: Лицензирование деятельности связанной с шифровальными (криптографическими) средствами осуществляется в соответствии с постановлением Правительства РФ 2007 г. № 957

В случае организации криптографической защиты с удалёнными клиентами (абонентами) ИСПДн:

Лицензия на право деятельности по предоставлению услуг в области шифрования информации — **ФСБ**

Лицензия на право деятельности по распространению шифровальных (криптографических) средств — **ФСБ**

Сроки выполнения требований законодательства

ФЗ № 152. Статья 25

…

3. Информационные системы персональных данных, созданные до дня вступления в силу настоящего Федерального закона, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее **1 января 2010 года**

4. Операторы, которые осуществляют обработку персональных данных до дня вступления в силу настоящего Федерального закона и продолжают осуществлять такую обработку после дня его вступления в силу, обязаны направить в уполномоченный орган по защите прав субъектов персональных данных, за исключением случаев, предусмотренных частью 2 статьи 22 настоящего Федерального закона, уведомление, предусмотренное частью 3 статьи 22 настоящего Федерального закона, не позднее **1 января 2008 года**…»

Какая может быть ответственность за нарушение закона?

Невыполнение требований законодательства по обеспечению защиты ПДн могут повлечь негативные последствия для должностных лиц или предприятия в целом

АДМИНИСТРАТИВНАЯ

УГОЛОВНАЯ

- гражданско-правовые иски со стороны клиентов, работников и уполномоченного органа по защите прав субъектов персональных
- принудительное приостановление или прекращение обработки ПДн в компании
- привлечение компании и (или) ее руководителя к административной или иным видам ответственности
- приостановление действия или аннулирование лицензий (при определенных условиях)
- репутационные риски
- риски связанные с недобросовестной конкуренцией

Административная ответственность

Кодекс об Административных правонарушениях (КоАП РФ)

«…КоАП РФ. Статья 13.13. Незаконная деятельность в области защиты информации

1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), – влечет наложение административного штрафа с конфискацией средств защиты информации или без таковой» (к ответственности могут быть привлечены граждане, должностные лица, юридические лица) …»

Уголовная ответственность?

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.

2. Те же деяния, совершенные лицом с использованием своего служебного положения, – наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев...»

Уголовная ответственность?

Уголовный Кодекс РФ (УК РФ) .

Статья 171. Незаконное предпринимательство

1. Осуществление предпринимательской деятельности без регистрации или с нарушением правил регистрации, а равно представление в орган, осуществляющий государственную регистрацию юридических лиц и индивидуальных предпринимателей, документов, содержащих заведомо ложные сведения, либо осуществление предпринимательской деятельности без специального разрешения (лицензии) в случаях, когда такое разрешение (лицензия) обязательно, или с нарушением лицензионных требований и условий, если это деяние причинило крупный ущерб гражданам, организациям или государству либо сопряжено с извлечением дохода в крупном размере, – наказывается штрафом, либо обязательными работами на срок от ставосьмидесяти до двухсот сорока часов, либо арестом на срок от четырех до шести месяцев...»

Уголовная ответственность?

Уголовный Кодекс РФ (УК РФ) .

Статья 171. Незаконное предпринимательство

2. То же деяние:

а) совершенное организованной группой;

б) сопряженное с извлечением дохода в особо крупном размере, -

наказывается штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок до пяти лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового.

Что?

Subtitle color

Microsoft®

Your potential. Our passion.™


TechDays.ru