Андрей Енькин

WEB-специалист

Закон №152-ФЗ «О персональных данных»:

Вопросы защиты информации и защиты от проверок

Андрей Енькин
WEB-специалист

E-mail: andrey@enkin.ru
Сайт: www.enkin.ru

Основные понятия: [закон "О персональных данных", ст. 3]

Персональные данные (ПДн) - 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.

Оператор ПДн - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Информационная система персональных данных (ИСПДн) - представляет собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств.

Андрей Енькин
WEB-специалист

E-mail: andrey@enkin.ru
Сайт: www.enkin.ru

Основные понятия: [закон "О персональных данных", ст. 3]

ОБРАБОТКА персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание (необратимо!), деперсонификация (обратимо!), блокирование, уничтожение

КОНФИДЕНЦИАЛЬНОСТЬ персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания

ОБЛАДАТЕЛЬ информации – лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (здесь противоречие с ст. 61 «Основ…», где обладатель информации – пациент!)

Андрей Енькин
WEB-специалист

E-mail: andrey@enkin.ru
Сайт: www.enkin.ru

Основные понятия: [закон "О персональных данных", ст. 3]

ИСПОЛЬЗОВАНИЕ персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ... или других лиц либо иным образом затрагивающих права и свободы субъекта ... или других лиц

ПЕРЕДАЧА (предоставление) персональных данных – действия, направленные на их получение ОПРЕДЕЛЕННЫМ кругом лиц

РАСПРОСТРАНЕНИЕ персональных данных – их ПЕРЕДАЧА или действия, направленные на их получение НЕОПРЕДЕЛЕННЫМ кругом лиц

БЛОКИРОВАНИЕ персональных данных – временное прекращение их обработки, в том числе их использования и передачи

ОБЕЗЛИЧИВАНИЕ персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных

Андрей Енькин
WEB-специалист

E-mail: andrey@enkin.ru
Сайт: www.enkin.ru

Основные понятия: [ст. 61 "Основ ... об охране здоровья ..."]

ВРАЧЕБНАЯ ТАЙНА – информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении

Необходимость [письменного] согласия пациента или его законного представителя на передачу сведений, составляющих врачебную тайну, другим лицам, в том числе должностным лицам, в интересах его обследования и лечения

Предоставление этих сведений БЕЗ согласия пациента допускается:
- в целях его обследования и лечения, в случае если он не способен из-за своего состояния выразить свою волю
- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений
- по запросу органов дознания и следствия, и суда
…

Андрей Енькин
WEB-специалист

E-mail: andrey@enkin.ru
Сайт: www.enkin.ru

Закон "О персональных данных" № 152-ФЗ от 27.07.2006

1. Гарантии конфиденциальности персональных данных при их обработке (ст. 7), но нет явной нормы об уведомлении субъекта ПД о случаях нарушении конфиденциальности (ст. 21)
2. Контроль и надзор за их выполнением (ч. 3 ст.19) : Роскомнадзор (ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ) – уполномоченный орган по защите прав субъектов персональных данных (ст. 23), ФСТЭК (Федеральная служба по техническому и экспортному контролю), ФСБ
3. *Право пациента на получение от оператора сведений о цели, способах и сроках обработки его персональных данных, и лицах которые имеют или могут иметь к ним доступ (ст. 14)*
4. *Обязанность оператора предоставить субъекту сведения об обработке его ПД, полученных от третьих лиц (ст. 18)*
5. Уведомление об обработке персональных данных ДО ИХ ОБРАБОТКИ БЕЗ уведомления - если обработка ПД -- без передачи третьим лицам:
6. возможность аутсорсинга обработки ПД (часть 4 ст. 6)

Андрей Енькин
WEB-специалист

E-mail: andrey@enkin.ru
Сайт: www.enkin.ru

Обязанности клиники – оператора ПД

1. Провести обследование ИСПД, определить состав ИСПД

2. Оформить акт об отнесении ИС ПД к классу К1 \ К3
   Класс ИСПД означает требования к защите ПД (состав мер, методы)

3. Зарегистрироваться в качестве оператора ПД – направить уведомление в Роскомнадзор – уполномоченный орган по защите прав субъектов персональных данных (ст. 22, 23 152-ФЗ), указать класс ИС

4. Организовать информирование пациентов по их запросам о способах и сроках обработки их ПД, лицах, имеющих к ним доступ (ст.14), а также об обработке их ПД, полученных от третьих лиц (ст.18)

5. Организовать и поддерживать систему обеспечения безопасности конфиденциальной информации
   надо издать около 40 организационно-распорядительных документов !

Андрей Енькин
WEB-специалист

E-mail: andrey@enkin.ru
Сайт: www.enkin.ru

Регламентирующие документы:

О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информацинного обмена, Указ Президента РФ от 17.03.2008г. № 351

Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, постановление Правительства РФ от 17.11.2007 г. № 781

Об утверждении Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, постановление Правительства РФ от 06.07.2008 г. № 512

Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, постановление Правительства РФ от 15.09.2008 г. № 687

пп. 4, 7 = обособление ПД от других сведений + подпись пациента о согласии на обработку ПД = приказ МЗСР от 18.03.2009 г. № 119н (по ВМП)

Андрей Енькин
WEB-специалист

E-mail: andrey@enkin.ru
Сайт: www.enkin.ru

КЛАССЫ ИСПД:

3: одновременно обрабатываются данные менее чем 1000 субъектов ПД или в пределах конкретной организации

2: **от 1000 до 100 000** субъектов ПД или субъектов ПДн, работающих в органе гос. власти или проживающих в пределах муниципального образования

1: более чем **100 000 субъектов** ПД или в пределах субъекта РФ или Российской Федерации в целом

Хпд / Хнпд	3	2	1
Категория 4: **обезличенные и (или) общедоступные ПДн**	К4	К4	К4
Категория 3: **ПДн, позволяющие идентифицировать субъекта ПДн (ФИО, место и дата рождения)**	К3	К3	К2
Категория 2: **ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории 1**	К3	К2	К1
Категория 1: **ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни**	К1	К1	К1

Андрей Енькин
WEB-специалист

E-mail: andrey@enkin.ru
Сайт: www.enkin.ru

Защита персональной информации:

ПРИКАЗ («ТРЕХ»): ФСТЭК России, ФСБ России и Министерства информационных технологий и связи РФ от 13 февраля 2008 года №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

Характеристики безопасности информации:

1. **доступность**
2. **целостность**
3. **конфиденциальность**
4. **неотказуемость**
5. **защита авторских прав**

Андрей Енькин
WEB-специалист

E-mail: andrey@enkin.ru
Сайт: www.enkin.ru

Защита персональной информации - действия:

- использование средств ЭЦП -> обеспечение целостности информации
  шифрование ПДн при передаче по каналам связи и на внешних МН сертифицированными ФСБ средствами криптозащиты
- учет внешних носителей данных (маркировка, журнал учета и др.)
- резервное копирование / восстановление данных (регламент, учет копий) - обеспечение целостности данных
- раздельное хранение носителей данных с резервными копиями
- функциональная безопасность -> обеспечение непрерывности функционирования - доступность информации (надежность, отказоустойчивость, резервирование техники
- физическая защита - контроль доступа в помещения и к компьютерам,
- охрана периметра (контролируемой зоны)
- комплексное планирование, обеспечение ресурсами обучение персонала (инструктажи, допуск к работе, ознакомление с документы под роспись и т.д.)
- систематические проверки и контроль

Андрей Енькин
WEB-специалист

E-mail: andrey@enkin.ru
Сайт: www.enkin.ru

Ответственность:

	Содержание статьи	Возможные санкции
УК 137	Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия	Штраф 300.000 руб., арест до 6 месяцев
УК 138	Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений	Штраф 300.000 руб., арест до 4 месяцев, лишение права занимать определенные должности
УК 155	Разглашение тайны усыновления (удочерения)	Штраф 80.000 руб., арест до 4 месяцев
УК 183	Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну	200.000 руб. + дисквалификация должностного лица до 3 лет, лишение свободы до 10 лет

Андрей Енькин
WEB-специалист

E-mail: andrey@enkin.ru
Сайт: www.enkin.ru

Ответственность:

	Содержание статьи	Возможные санкции
УК 201	Злоупотребление полномочиями (при умышленном разглашении ПДн)	Штраф до 1.000.000 руб., лишение свободы до 10 лет
УК 272	Неправомерный доступ к компьютерной информации	Штраф 300.000 руб., исправительные работы на срок до 2 лет, лишение свободы до 5 лет
КоАП РФ ст. 13.12	Нарушение правил защиты информации, а также использование несертифицированных средств защиты информации, если они подлежат обязательной сертификации, а также грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации	Штраф 20.000 руб. + конфискация несертифицированных средств защиты информации + приостановление деятельности на срок до 90 суток

Андрей Енькин
WEB-специалист

E-mail: andrey@enkin.ru
Сайт: www.enkin.ru

Нужные ссылки:

www.rsoc.ru – Роскомнадзор (план проверок)
www.pd.rsoc – портал "Персональные данные" Роскомнадзора
www.fstec.ru – ФСТЭК
www.ispdn.ru + www.54.rsoc.ru + www.admin.smolensk.ru
www.medctat.narod.ru + + www.omskminzdrav.ru + www.miac74.ru

Андрей Енькин
WEB-специалист

E-mail: andrey@enkin.ru
Сайт: www.enkin.ru

Спасибо за внимание!

Для вопросов и деловых предложений:

Тел: 8 (931) 307- 31 - 17
E-майл: andrey@enkin.ru
andreyenkin@yandex.ru
Сайт: enkin.ru
ICQ: 206043439