С е м и н а р

г. Самара, **15-17** декабря 2009 года, ***ГБУ СО «РЦУП»***

«Обеспечение безопасности персональных данных в соответствии с требованиями законодательства РФ. Федеральный Закон № 152»

Минин Виктор – Сопредседатель комитета по информационной безопасности МОО Союз ИТ-директоров России, Советник Председателя МОО Ассоциация защиты информации, член Консультативного совета при уполномоченном органе по защите прав субъектов персональных данных
itsec@rucio.ru, mvv@azi.ru,

С чего все началось

- Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных личного характера от 28.01.1981 EST № 108

- Федеральный закон от 19.12. 2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»

Нормативная база по защите ПД

- Конституция РФ
- Федеральные законы
- Постановления Правительства Российской Федерации
- Документы уполномоченных федеральных органов в виде приказов, положений, требований, методик и рекомендаций (открытые и ограниченного доступа)

Законодательство о персональных данных

- ФЗ «**Об информации, информационных технологиях и о защите информации**» №149-ФЗ от 27 июля 2006 года
- ФЗ «**О персональных данных**» №152-ФЗ от 27 июля 2006 года
- ФЗ **«О лицензировании отдельных видов деятельности»** №128-ФЗ от 8 августа 2001 года
- **Трудовой кодекс Российской Федерации** № 197-ФЗ от 30 декабря 2001 года (глава 14)
- **Кодекс Российской Федерации об административных правонарушениях** № 195-ФЗ от 30 декабря 2001 года (Статья 13.11.)
- ФЗ **«О государственной гражданской службе Российской Федерации»** № 79-ФЗ от 27 июля 2004 года (Глава 7)
- ФЗ **«О муниципальной службе в Российской Федерации»** № 25-ФЗ от 2 марта 2007 года (Статья 29)

Подзаконные нормативные акты Правительства РФ

- Постановление Правительства РФ от 17 ноября 2007 г. № 781 «**Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных**»
- Постановление Правительства РФ от 6 июля 2008 г. № 512 «**Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных**»
- Постановление Правительства РФ от 15 сентября 2008 г. № 687 «**Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации**»

Подзаконные нормативные акты ведомств

Приказ Россвязьохранкультуры от 28 марта 2008 г. № 154 «**Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных**»

Приказ Россвязькомнадзора от 17 июля 2008 г. № 08 «**Об утверждении образца формы уведомления об обработке персональных данных**»

Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «**Об утверждении Порядка проведения классификации информационных систем персональных данных**»

Методические документы ФСТЭК («ДСП»)

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»,
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»,
- «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных»
- «Рекомендации по обеспечению безопасности персональных данных при обработке при их обработке в информационных системах персональных данных»

Методические документы ФСБ

- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных

- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации

Полный перечень нормативных правовых актов в области персональных данных

на сайте

Информационного проекта «Персональные данные»:
http://www.privacy-info.ru

Государственные органы, регулирующие вопросы использования и защиты персональных данных

- Министерство связи и массовых коммуникаций РФ
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций РФ
- Федеральная служба по техническому и экспортному контролю РФ
- Федеральная служба безопасности РФ

Государственные органы, регулирующие вопросы использования и защиты персональных данных

- **Роскомнадзор** (федеральная служба по надзору в сфере связи и массовых коммуникаций), является основным исполнительным и надзорным органом по защите прав физических лиц, чьи персональные данные обрабатываются. http://www.rsoc.ru (федеральная служба по надзору в сфере связи и массовых коммуникаций), является основным исполнительным и надзорным органом по защите прав физических лиц, чьи персональные данные обрабатываются. http://www.rsoc.ru и http://pd.rsoc.ru

- **ФСТЭК России** (Федеральная служба по техническому и экспортному контролю РФ) – лицензирование деятельности операторов персональных данных при осуществлении ими технической защиты конфиденциальной информации. http://www.fstec.ru

- **ФСБ России** (Федеральная служба безопасности РФ) традиционно контролирует деятельность операторов персональных данных, при использовании ими при защите персональных данных

ФЗ «О персональных данных»

Статья 2. Цель настоящего Федерального закона

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

ФЗ «О персональных данных»

1) определил понятие ПД, выделил специальные категории ПД

2) установил принципы, условия и особенности обработки ПД

3) установил права субъектов ПД

4) установил обязанности оператора

5) определил уполномоченный орган, порядок контроля и надзора за обработкой ПД

6) предусмотрел ответственность за нарушение ФЗ и переходные положения

ФЗ «О персональных данных» (ст. 3)

1) 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;

Таким образом, ПД – это информация, которая может находиться в различных режимах охраны.

ФЗ «О персональных данных» (ст. 3)

10) **конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

Приказ от 13 февраля 2008 № 55/86/20

8. По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, информационные системы подразделяются на типовые и специальные информационные системы.

- **Типовые информационные системы -** информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

- **Специальные информационные системы -** информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

Проблемы применения Федерального закона «О персональных данных»

- Соотношение режимов конфиденциальности
- Перечень персональных данных
- Согласие субъекта
- Требование классификации информационных систем
- Требование лицензирования деятельности по технической защите конфиденциальной информации
- Требование сертификации средств защиты информации
- Требование регистрации информационных систем персональных данных

В результате выполнение работ по защите ПДн внедряется решение, которое состоит из следующих компонентов (этапов):

- организационно-правовые мероприятия (нетехническая защита ПДн)
- инженерно-технические мероприятия (техническая защита ПДн)
- процессы обеспечения системы защиты ПДн

Один из основных этапов создания корпоративной системы персональных данных

Основа организации работ с персональными данными является внутренняя нормативная документация определяющая и регламентирующая все виды деятельности по обработке персональных данных в компании

Регуляторы при проведении проверочных мероприятий первичную оценку положения дел в компании делают на основании предоставленной документации

Порядок проведения классификации ИСПД

Определяются следующие категории обрабатываемых в информационной системе персональных данных (Хпд):

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

Порядок проведения классификации ИСПД

Хнпд может принимать следующие значения:
1 - в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;
2 - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных.данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;
3 - в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

Основные мероприятия по обеспечению безопасности ПД

Конкретный состав мероприятий по защите ПД определяется в зависимости от класса ИС и характеристик информационных систем. Мероприятия по защите ПД должны быть реализованы в рамках следующих подсистем:

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

«…должна проводиться сертификация программного обеспечения ИСПДн на отсутствие не декларированных возможностей…»

Уязвимости на 15 ноября 2009

- Linux Kernel 2.6.x 373
- Sun Solaris 10 863
- Red Hat Enterprise Linux Server v.5 928
- FreeBSD 6.x 80
- Microsoft Windows Server 2003 Ent. 283
- Microsoft Windows Server 2008 114

- Apple Mac OS X – 1087
- Red Hat Enterprise Linux Client v.5 1006
- Ubuntu Linux 8.04 (апрель 2008) 659
- Windows Vista 143
- Window 7 5

- Oracle Database 11.x 239
- IBM DB2 9.x 58
- MySQL 5.x 35
- Microsoft SQL Server 2005 18
- Microsoft SQL Server 2008 0

- Mozilla Firefox 3.x 133
- Opera 9.x 54
- Microsoft Internet Explorer 8.x 16

- Cisco ASA 7.x 51
- Microsoft ISA Server 2006 7

http://http://secunia.com

Порядок действий по созданию системы защиты ИСПДн

- Обследование (аудит) бизнеспроцессов компании на наличие в них ПДн
- Инвентаризация ИС, обрабатывающих ПДн
- Оценка законности обработки ПДн и наличие согласия субъектов на обработку
- Контроль и корректировка договорных отношений с субъектами
- Формирование перечня ПДн и проведение категорирования
- Определение целей обработки ПДн
- Определение сроков и условий прекращения обработки ПДн
- Разграничение доступа пользователей к ПДн в ИСПДн
- Формирование документов регламентирующих работу с ПДн
- Формирование модели угроз, содержащей актуальные угрозы информационной безопасности персональным данным при их обработке в информационной системе
- Классификация ИСПДн
- При, необходимости определенной в №152-ФЗ, направить уведомление об обработке ПД в уполномоченный орган по защите прав субъектов персональных данных, Роскомнадзор httpРоскомнадзор http://Роскомнадзор http://wwwРоскомнадзор http://www.Роскомнадзор http://www.rsocРоскомнадзор http://www.rsoc.Роскомнадзор http://www.rsoc.ruРоскомнадзор http://www.rsoc.ru/Роскомнадзор http://www.rsoc.ru/mainРоскомнадзор http://www.rsoc.ru/main/Роскомнадзор http://www.rsoc.ru/main/directionsРоскомнадзор http://www.rsoc.ru/main/directions/874/
- Приведение системы защиты ПДн в соответствие требованиям регуляторов
- При необходимости, определенной методическими документами ФСТЭК России

Результаты работы по созданию ИСПДн

Комплект организационно-распорядительной документации

Комплект проектной документации системы защиты, включающий:

- требования к системе защиты информации персональных данных;
- модель угроз безопасности персональных данных;
- модель нарушителя безопасности персональных данных;
- концепцию обеспечения безопасности персональных данных.

Перечень мероприятий по защите персональных данных в соответствии с выбранным классом информационной системы персональных данных

Комплект эксплуатационной документации на систему защиты персональных данных

Аттестат (сертификат) информационной системы персональных данных по требованиям безопасности персональных данных

Что будет, если ничего не делать

Ответственность:

- КоАП - Статья 13.12: При систематических нарушениях приостановление деятельности в области защиты информации на срок до 90 суток

- ФЗ №152 - Приостановление действия или аннулирование лицензии по защите конфиденциальной информации при нарушении требований по защите персональных данных

- УК - Статья 137: Нарушение неприкосновенности частной жизни. Незаконное собирание или распространение сведений касающихся частной жизни…

Роскомнадзор имеет право ходатайствовать об отзыве лицензий на основной вид деятельности

Российский Союз ИТ-директоров СоДИТ

Институт современного развития (ИНСОР)

АЗИ

Рекомендации

СоДИТ ИТ-директорам России по защите персональных данных, выработанные на заседании экспертов 6 февраля 2009 г. при участии МОО АЗИ и Института Современного Развития.

Москва
2009 г.

Ключевые даты

Федеральный закон от 27 июля 2006 г. № 152-ФЗ:

- После дня вступления в силу настоящего Федерального закона обработка персональных данных, включенных в информационные системы персональных данных до дня его вступления в силу, осуществляется в соответствии с настоящим Федеральным законом.

- Не позднее 1 января 2010 года 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 2008 года операторы … обязаны направить в уполномоченный орган по защите прав субъектов персональных данных … уведомление, предусмотренное частью 3 статьи 22 настоящего Федерального закона

Закон вступил в силу 26 января 2007 года

Для чего Вам все ЭТО?

- Заниматься работой по защите ПД необходимо
- ФЗ №152 – средство защиты бюджетов на ИБ перед руководством организации
- Фактическая защищенность и реализация требований регуляторов не одно и тоже
- Ключевой момент минимизации расходов на защиту ПД – правильная классификация и очерчивание границ ИСПДн

Как выбрать консультанта?

- Общая рекомендация - это, безусловно, квалификация и компетенция специалистов работающих в компании которую вы приглашаете.
- Компания должна быть лицензиатом ФСТЭК и/или ФСБ (www.fstec.ru)
- При самостоятельном подборе средств защиты информации внимательно читайте содержимое сертификатов на эти средства.

ЛИЦЕНЗИИ Федеральной службы безопасности Российской Федерации на осуществление:

– разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем;

ЛИЦЕНЗИЯ Федеральной службы безопасности Российской Федерации на

- осуществление разработки и (или) производства средств защиты конфиденциальной информации.

ЛИЦЕНЗИЯ Федеральной службы по техническому и экспортному контролю на проведение работ, связанных с созданием средств защиты информации:

– разработка, производство, реализация, установка, монтаж, наладка, испытания, ремонт, сервисное обслуживание.

ЛИЦЕНЗИЯ Федеральной службы по техническому и экспортному контролю на деятельность по технической защите конфиденциальной информации:

– осуществление мероприятий и оказание услуг по технической защите конфиденциальной информации.

СПАСИБО ЗА ВНИМАНИЕ

Вопросы можно задать по электронной почте СоДИТ - itsec@rucio.ru

Минин Виктор
Сопредседатель комитета по информационной безопасности МОО СОДИТ, член Правления МОО СОДИТ,
Советник Председателя Ассоциация защиты информации,
Председатель Общественного консультативного совета по научно-технологическим вопросам информационной безопасности Комиссии по информационной безопасности при Координационном совете государств-участников СНГ по информатизации при РСС

Ответственность за нарушение закона

Ответственность при невыполнении требований закона, увы, достаточно серьезна, чтобы, по крайней мере, принять ее к сведению. Проанализировав КоАП РФ и УК РФ, можно выделить ряд статей, в соответствии с которыми будет определяться ответственность за нарушение требований по защите ПДн. КоАП Статья 5.39 – отказ в предоставлении гражданину информации. Ответственность – штраф до 1 000 руб., но также это может явиться основанием для ответственности по статье 3.12 (Административное приостановление деятельности). КоАП Статья 13.11 – нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах. Ответственность – штраф до 1 000 руб.

КоАП Статья 13.12 – нарушение правил защиты данных. Ответственность – штраф от 10 000 до 20 000 руб. с конфискацией несертифицированных средств защиты информации или административное приостановление деятельности на срок до 90 суток. УК Статья 137 – нарушение неприкосновенности частной жизни. Ответственность может доходить до штрафа в размере ЗП осужденного за 18 месяцев или ареста на 6 месяцев. УК Статья 140 –отказ в предоставлении гражданину информации. Ответственность – штраф до ЗП за 18 месяцев либо лишение права занимать ряд должностей или заниматься определенной деятельностью. УК Статья 171 – незаконное предпринимательство. Ответственность – до 5 лет лишения свободы со штрафом в размере ЗП осужденного за 6 месяцев.

Зоны ответственности регуляторов в сфере персональных данных