«Информационная безопасность: современные технологии»
Ижевск, 21 мая 2009

Информационная безопасность. Технологии и средства защиты информации

Майшев Вадим Владимирович
Заместитель генерального директора по безопасности

Научно-производственное предприятие
“ИЖИНФОРМПРОЕКТ”

НПП «Ижинформпроект»

- автоматизация бизнес-процессов
- услуги телематических служб и передачи данных
- услуги по контролю движения транспортных средств с помощью систем глобального позиционирования
- поставка, установка, настройка и сопровождение средств и систем защиты информации
- услуги специализированного оператора связи по обеспечению представления отчетности в контролирующие органы
- услуги по организации защищенного электронного документооборота и защищенного межсетевого взаимодействия
- услуги Удостоверяющего центра InfoTrust
- консультационные услуги в области информационной безопасности

Лицензии

Управление ФСБ России
по Удмуртской Республике

- на право распространения шифровальных (криптографических) средств № 01 от 22.08.2008
- на право технического обслуживания шифровальных (криптографических) средств № 02 от 22.08.2008
- на право предоставления услуг в области шифрования информации № 03 от 22.08.2008

Россвязьохранкультура

- на право предоставления услуг связи по передаче данных № 59491 от 18.08.2008
- на право предоставления телематических услуг связи
№ 59492 от 18.08.2008

Информационная безопасность

- невозможность нанесения вреда свойствам объекта безопасности (человек, общество, государство), обусловливаемым информацией и информационной инфраструктурой

Защита информации

- комплекс мероприятий, направленных на обеспечение информационной безопасности. Это поддержание целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных

Цели защиты информации

Обеспечение:

- своевременного доступа (за приемлемое время) к необходимой информации;
- конфиденциальности (сохранения в тайне) определенной части информации;
- достоверности (полноты, точности, адекватности, целостности) информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);
- защиты части информации от незаконного ее тиражирования (защиты авторских прав, прав собственника информации и т.п.);
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации.

Безопасность автоматизированной системы

- защищенность всех компонентов (помещения, аппаратных средств, программного обеспечения, данных и персонала) от нежелательных для субъектов информационных отношений воздействий

Задачи защиты ИТС

- управление доступом пользователей к ресурсам АС с целью ее защиты от неправомерного случайного или умышленного вмешательства в работу системы и несанкционированного (с превышением предоставленных полномочий) доступа к ее информационным, программным и аппаратным ресурсам со стороны посторонних лиц, а также лиц из числа персонала организации и пользователей;
- защита данных, передаваемых по каналам связи;
- регистрация, сбор, хранение, обработка и выдача сведений обо всех событиях, происходящих в системе и имеющих отношение к ее безопасности;
- контроль работы пользователей системы со стороны администрации и оперативное оповещение администратора безопасности о попытках несанкционированного доступа к ресурсам системы;
- контроль и поддержание целостности критичных ресурсов системы защиты и среды исполнения прикладных программ;
- обеспечение замкнутой среды проверенного программного обеспечения с целью защиты от бесконтрольного внедрения в систему потенциально опасных программ (в которых могут содержаться вредоносные закладки или опасные ошибки) и средств преодоления системы защиты, а также от внедрения и распространения компьютерных вирусов;
- управление средствами системы защиты.

Информация в зависимости от категории доступа

- ФЗ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)

Ограничение доступа к информации

- устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства
- обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами
- 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

Информация ограниченного доступа

- Информация, составляющая государственную тайну
  - Особой важности
  - Совершенно секретно
  - Секретно
- Конфиденциальная информация
  - Коммерческая тайна (№ 98-ФЗ от 29.07.2004)
  - Профессиональная тайна (врачебная, банковская, нотариальная, адвокатская, налоговая тайна, тайна вероисповедания, связи и т.д.)
  - Служебная тайна (ГК)
  - Персональные данные (№ 152-ФЗ от 27.07.2006)

Ответственность

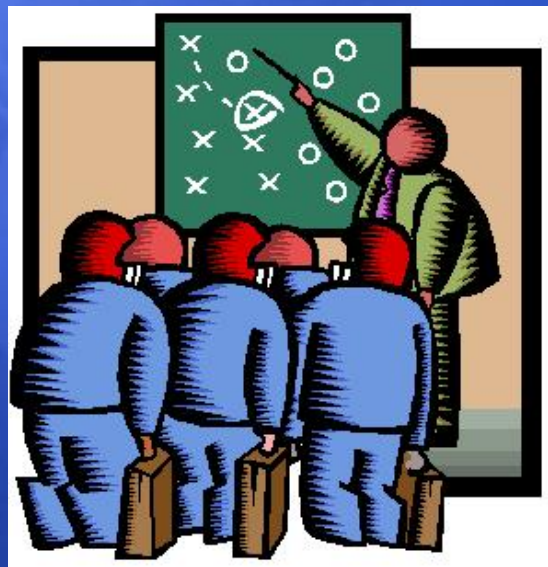
Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

- Нарушение требований закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ
- Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством РФ требования о защите информации

Типовой подход

- Цель / основание защиты
- Условия отнесения информации к защищаемым сведениям / перечень сведений
- Регламентация допуска и доступа к сведениям
- Обязательность соблюдения конфиденциальности и ответственность за разглашение / компенсация ущерба

- Регламентация процессов обработки и применения СЗИ
- Контроль



Основные методы защиты информации

- правовая защита информации
- организационная защита информации
- инженерно-техническая защита информации
- программно-аппаратная защита информации

Правовая защита информации

- методы и основы правовой защиты тайны,
- правовая основа допуска и доступа персонала к защищаемым сведениям,
- система правовой ответственности,
- правовые основы деятельности подразделений защиты информации,
- законодательство РФ в области защиты тайны

Организационная защита информации

- принципы, силы, средства и условия организационной защиты информации,
- порядок засекречивания и рассекречивания,
- допуск и доступ к конфиденциальной информации,
- организация внутриобъектового и пропускного режимов, охраны,
- организация аналитической работы по предупреждению утечки конфиденциальной информации,
- направления и методы работы с персоналом

Инженерно-техническая защита информации

- принципы добывания и обработки информации техническими средствами,
- классификация и структура технических каналов утечки информации,
- основные способы и принципы работы средств наблюдения объектов, подслушивания и перехвата сигналов и соответствующих средств защиты информации,
- организационные и технические меры,
- технические средства охраны,
- специальные технические средства

Программно-аппаратная защита информации

- Защита данных от несанкционированного доступа (НСД),
- Шифрование,
- Электронная цифровая подпись,
- Контроль и разграничение доступа,
- Программно-аппаратные средства защиты
- Защита программ
- Защита сетевого взаимодействия ЛВС/ГВС
- Защита от разрушающих программных воздействий (РПВ), компьютерных вирусов

Правовое поле

- ФЗ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- ФЗ от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи»
- ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
- ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных»
- Доктрина информационной безопасности РФ от 09.09.2000 № ПР-1895
- Постановление Совета Министров - Правительства РФ от 15.09.1993 № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам»
- Постановление Правительства РФ от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»
- Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»
- Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена»

Правовое поле (продолжение)

- Федеральный закон от 08.08.2001 № 128-ФЗ «О лицензировании отдельных видов деятельности»
- Постановление Правительства РФ от 29.12.2007 № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»
- Постановление Правительства РФ от 30.05.2003 № 313 «Об уполномоченном федеральном органе исполнительной власти в области использования электронной цифровой подписи»
- Постановление Правительства РФ от 12.02.2003 № 95 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»
- Постановление Правительства РФ от 27.05.2002 № 348 «Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»
- Постановление Правительства РФ от 15.08.2006 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»
- Постановление Правительства РФ от 15.07.2002 № 526 «Об утверждении Положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность»

Правовое поле (продолжение)

- Решение Гостехкомиссии и ФАПСИ от 27.04.1994 № 10 «Об утверждении Положения о государственном лицензировании деятельности в области защиты информации»
- Постановление Правительства РФ от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»
- Приказ ФСБ РФ от 23.08.1995 № 28 «Об утверждении Инструкции о порядке проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну»
- Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)
- Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

Правовое поле (продолжение)

- Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации»
- Положение о сертификации средств защиты информации по требованиям безопасности информации (Гостехкомиссия)
- Система сертификации средств криптографической защиты информации (СКЗИ) от 15.11.1993 № РОСС RU.0001.030001
- Приказ ФСБ России от 13.11.1999 № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»
- Положение по аттестации объектов информатизации по требованиям безопасности информации (Гостехкомиссия)
- Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании»
- Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года одобрена Распоряжением Правительства Российской Федерации от 27.09.2004 № 1244-р

Государственное регулирование

- Лицензирование деятельности
- Сертификация средств защиты информации
- Аттестация объектов информатизации

Лицензирование

ФЗ от 08.08.2001 № 128-ФЗ «О лицензировании отдельных видов деятельности»

- лицензия — специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий;
- лицензионные требования и условия — совокупность установленных требований и условий, выполнение которых лицензиатом обязательно при осуществлении лицензируемого вида деятельности

Лицензирование деятельности

- деятельность по распространению шифровальных (криптографических) средств;
- деятельность по техническому обслуживанию шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;
- деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- деятельность по разработке и (или) производству средств защиты конфиденциальной информации;
- деятельность по технической защите конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Сертификация СЗИ

- сертификат соответствия — документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров;
- система сертификации — совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом;
- техническое регулирование — правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации…

Сертификация СЗИ

- Положение о сертификации средств защиты информации, утвержденное Постановлением Правительства РФ от 26.06.1995 № 608
- Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации и подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации

Аттестация объектов информатизации

- Система аттестации ОИ по требованиям безопасности информации - составная часть единой системы сертификации СЗИ и аттестации ОИ по требованиям безопасности информации
- Комплекс организационно-технических мероприятий, в результате которых «Аттестатом соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией (ФСТЭК) России

Аттестация объектов информатизации

- Аттестация предшествует началу обработки подлежащей защите информации - официальное подтверждение эффективности комплекса используемых мер и средств защиты информации
- Соответствие требованиям по защите информации
  - от несанкционированного доступа, в том числе от компьютерных вирусов,
  - от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие),
  - от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.
- Предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации

Нормативная база по оценке защищенности

- законодательные акты
- международные и национальные стандарты
- межведомственные и внутриведомственные приказы, руководящие документы и временные положения
- внутриведомственные методики и руководства

Руководящие документы Гостехкомиссии (ФСТЭК) России

- «Положение по аттестации объектов информатизации по требованиям безопасности информации» (Утверждено Председателем Гостехкомиссии России 25.11.1994 г.);
- «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования к защите информации» (Гостехкомиссия России, 1992);
- «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1992 г.);
- «Концепция защиты средств вычислительной техники от НСД к информации» (Гостехкомиссия России, 1992 г.);
- «Защита от НСД к информации. Термины и определения» (Гостехкомиссия России, 1992 г.);
- «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и СВТ» (Гостехкомиссия России, 1992 г.);
- «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1997 г.);
- «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» (Гостехкомиссия России, 1999 г.);
- «Специальные требования и рекомендации по технической защите конфиденциальной информации» (Гостехкомиссия России, 2002 г.).

Основные защитные механизмы

- идентификация (именование и опознавание), аутентификация (подтверждение подлинности) пользователей системы;
- разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям;
- регистрация и оперативное оповещение о событиях, происходящих в системе;
- криптографическое закрытие хранимых и передаваемых по каналам связи данных;
- контроль целостности и аутентичности (подлинности и авторства) данных;
- затирание остаточной информации на носителях;
- выявление и нейтрализация действий компьютерных вирусов;
- изоляция (защита периметра) компьютерных сетей (фильтрация трафика, скрытие внутренней структуры и адресации, противодействие атакам на внутренние ресурсы и т.д.);
- выявление уязвимостей (слабых мест) системы;
- обнаружение атак и оперативное реагирование.

Средства защиты информации

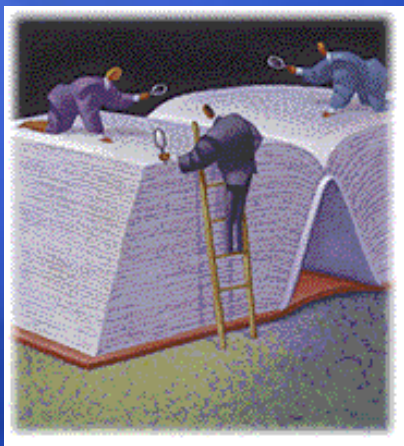
- Средства и системы идентификации, аутентификации, хранения криптографических ключей
- Криптографическая защита информации / Инфраструктура открытых ключей PKI
- Средства защиты от несанкционированного доступа (автономные)
- Средства защиты от несанкционированного доступа (в локальных сетях)
- Средства обеспечения сетевой безопасности (при взаимодействии с/через Интернет - межсетевые экраны, виртуальные частные сети и т.п.)
- Системы анализа защищенности
- Системы обнаружения и предотвращения атак
- Средства антивирусной защиты

Системы / технологии

- Защищенный электронный документооборот
  - конфиденциальность и юридическая значимость ЭД
  - прикладной уровень
  - On-line и off-line
- Защита межсетевого взаимодействия (VPN)
  - защита инфраструктуры
  - аутентификация участников и защита трафика
  - межсетевой и прикладной уровни
  - On-line
  - ЛВС-ГВС-ЛВС
  - ЛВС-ГВС-УП
- +
  - Средства защиты от несанкционированного доступа (автономные и ЛВС)
  - Системы анализа защищенности
  - Системы обнаружения и предотвращения атак
  - Средства антивирусной защиты

Персонал / обучение

- направление 090000 — Информационная безопасность
- раздел 090100 — Информационная безопасность
  - 090101 Криптография
  - 090102 Компьютерная безопасность
  - 090103 Организация и технология защиты информации (УдГУ)
  - 090104 Комплексная защита объектов информатизации
  - 090105 Комплексное обеспечение информационной безопасности автоматизированных систем (ИжГТУ)
  - 090106 Информационная безопасность телекоммуникационных систем
  - 090107 Противодействие техническим разведкам



Основы защиты ПДн

- ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных»
  - Цель - обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайны
  - ПДн - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его ФИО, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация
  - Оператор ПДн, обработка ПДн, конфиденциальность ПДн, информационная система ПДн (ИСПДн)

Условия обработки ПДн

Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных, за исключением специальных случаев:

- на основании ФЗ, устанавливающего ее цель, условия получения ПДн и круг субъектов, ПДн которых подлежат обработке, а также определяющего полномочия оператора;
- в целях исполнения договора, одной из сторон которого является субъект ПДн;
- для статистических или иных научных целей при условии обязательного обезличивания ПДн;
- необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
- необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;
- в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- подлежащих опубликованию в соответствии с ФЗ, в том числе ПДн лиц, замещающих государственные должности, должности государственной гражданской службы, ПДн кандидатов на выборные государственные или муниципальные должности.

Принципы обработки ПДн

- законность целей и способов обработки ПДн и добросовестности;
- соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям оператора;
- соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- достоверность ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем ПДн

Конфиденциальность ПДн

- Операторами и третьими лицами, получающими доступ к ПДн, должна обеспечиваться конфиденциальность таких данных
- Обеспечение конфиденциальности ПДн не требуется:
  - в случае обезличивания ПДн;
  - в отношении общедоступных ПДн

Меры по обеспечению безопасности ПДн при их обработке

Оператор при обработке ПДн обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий

Ответственность

- КОАП РФ от 30.12.2001 № 195-ФЗ
  - Ст. 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)
- УК РФ от 13.06.1996 № 63-ФЗ
  - Ст. 137. нарушение неприкосновенности частной жизни

Государственное регулирование

- Уполномоченный орган – Роскомнадзор (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций)
- Приказом Россвязькомнадзора от 17.07.2008 № 8 утверждены:
  - форма Уведомления об обработке (о намерении осуществлять обработку) ПДн;
  - Рекомендации по заполнению уведомления об обработке (о намерении осуществлять обработку) ПДн
- Методы и способы защиты информации в информационных системах устанавливаются и контролируются ФСТЭК России и ФСБ России в пределах их полномочий

Защита прав субъектов ПДн

- Реестр операторов, осуществляющих обработку персональных данных http://pd.rsoc.ru/ (Роскомнадзор)
- Управление Россвязькомнадзора по Удмуртской Республике
  - сайт - http://18.rsoc.ru/
  - формы/образцы заполнения уведомлений http://18.rsoc.ru/directions/96/

Обеспечение безопасности ПДн

- Постановление Правительства РФ от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности ПДн при их обработке в ИСПДн»
- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации»
- Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации ИСПДн»
- «Основные мероприятия по организации и техническому обеспечению безопасности ПДн, обрабатываемых в ИСПДн», ФСТЭК России 15.02.2008г.
- «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн», ФСТЭК России 15.02.2008г.
- «Рекомендации по обеспечению безопасности ПДн при их обработке в ИСПДн», ФСТЭК России 15.02.2008г.
- «Методика определения угроз безопасности ПДн при их обработке в ИСПДн», ФСТЭК России 14.02.2008г.
- 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 ПДн при их обработке в ИСПДн (ФСБ России, от 21.02.2008 № 149/6/6-622)
- Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации (ФСБ России, от 21.02.2008 № 149/54-144)

Проблемы защиты ПДн

- !? ПДн и ИСПДн повсеместно!!!!!
- 01 января 2010:
  - «Сидим-ждем пока накажут кого-нибудь…»
  - «К нам это не относится!»
- …Отсутствие наработанной практики (проверки/наказания)
- Сложность классификации ИСПДн:
  - Типовая или специальная?
  - Разработка и согласование модели угроз
  - Как понизить категорию ИСПДн (min расходов)?
- Уведомление об обработке ПДн
- !!!Только сертифицированные СЗИ (10 подсистем)
- !?! Аттестация ИСПДн (дорого и долго)
- ?Лицензирование ФСТЭК и ФСБ (трудно реализовать лицензионные требования)
- Аутсорсинг?
- С чего начать? Оптимизация бизнес-процессов?

Спасибо за внимание!

Вопросы?

Дополнительная информация
www.infotrust.ru security@infotrust.ru
+7 (3412) 918-100
г. Ижевск, ул. Бородина, 21, офис 207

Майшев Вадим Владимирович
Заместитель генерального директора по безопасности
mvv@infotrust.ru

Научно-производственное предприятие
“ИЖИНФОРМПРОЕКТ”