Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 3

Нормативно-правовое обеспечение

Толстой Александр Иванович
к.т.н., доцент
Кафедра «Информационная безопасность банковских систем»
Институт интеллектуальных кибернетических систем
Факультет «Кибернетика и информационная безопасность»
НИЯУ МИФИ

Москва, 2017

3. Нормативно-правовое обеспечение

3.1. Предмет и содержание проблемы

3.2.Нормативно правовая база ИБ в РФ

3.3.Техническое регулирование в области ИБ

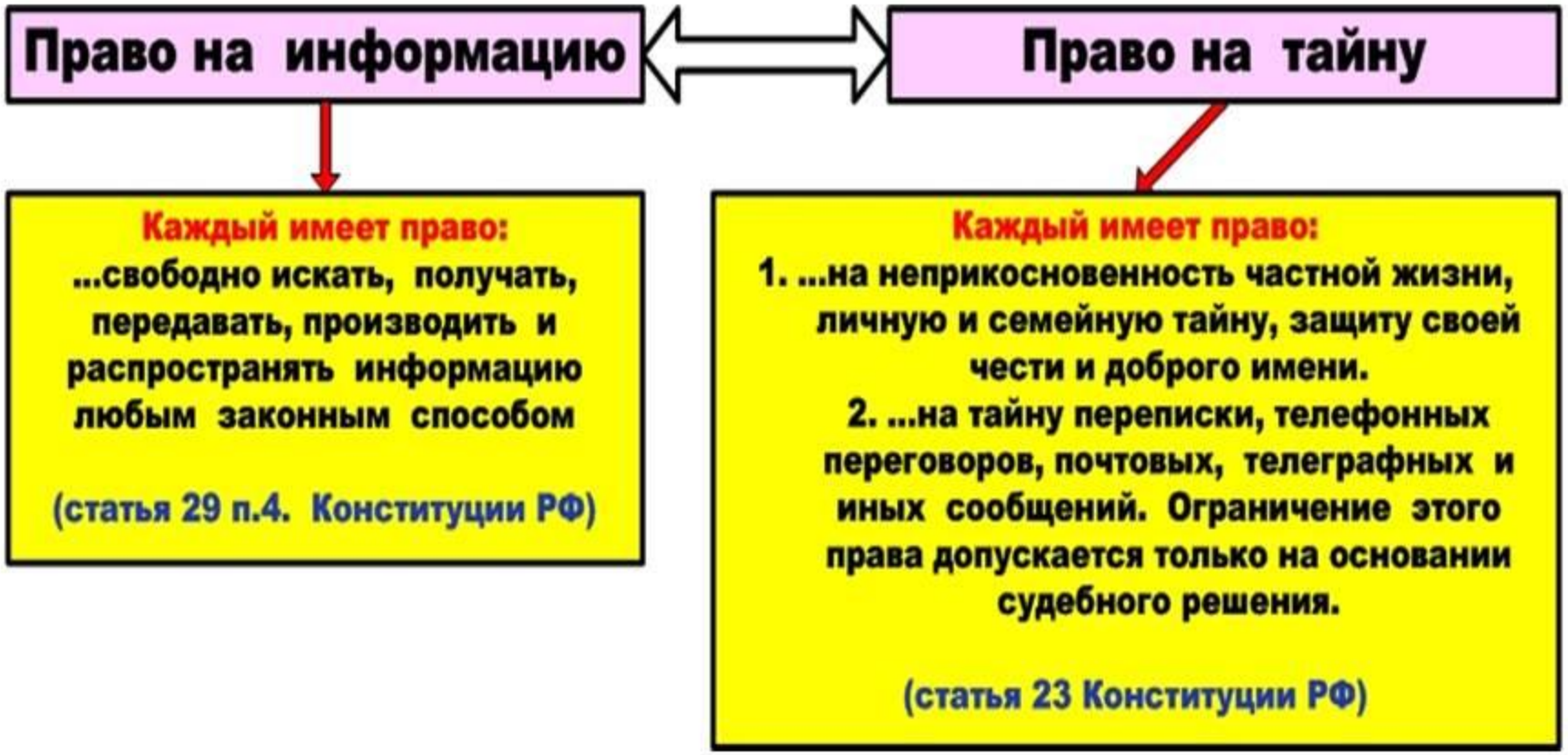
3.4.Стандартизация обеспечения ИБ

3.5.Нормативно-правовое обеспечение безопасности КВО

3.1. Предмет и содержание проблемы:

Конституция РФ: Информация как объект права

Фундаментальная проблема информационного права:



3.1. Предмет и содержание проблемы:

Нормативно-правовое обеспечение -???

Доктрина информационной безопасности Российской Федерации

«Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»

3.1. Предмет и содержание проблемы:

Нормативно-правовое обеспечение -???

Доктрина информационной безопасности Российской Федерации

«Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»

Для достижения баланса необходимо наличие:

- **совокупности правил и норм;**
- **процедур регулирования;**
- **субъектов и объектов регулирования**

Этому служит нормативно-правовое обеспечение ИБ

3.2.Нормативно-правовая база ИБ в РФ

Структура законодательства РФ

3.2.Нормативно-правовая база в РФ

- Конституция РФ
- Доктрина информационной безопасности
- Уголовный кодекс;
- Гражданский кодекс;
- Трудовой кодекс;
- Федеральные законы:
- Указы президента;
- Постановления Правительства;
- Нормативные документы уполномоченных федеральных органов
- Отраслевые нормативные документы

3.2.Нормативно-правовая база в РФ

Уголовный кодекс (уголовно-правовое регулирование информационных правоотношений).

Санкции за нарушение информационных правоотношений представлены в УК в прямой постановке следующими статьями:

- Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.
- Статья 140. Отказ в предоставлении гражданину информации.
- Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.

- Статья 272. Неправомерный доступ к компьютерной информации.
- Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.
- Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

- Статья 275. Государственная измена.
- Статья 276. Шпионаж.
- Статья 283. Разглашение государственной тайны.
- Статья 284. Утрата документов, содержащих государственную тайну.

3.2.Нормативно-правовая база в РФ

Уголовный кодекс (уголовно-правовое регулирование информационных правоотношений):

УК РФ Глава 28. Преступления в сфере компьютерной информации
Статья 272. Неправомерный доступ к компьютерной информации
1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, -
•наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.
2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, -
•наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

3.2.Нормативно-правовая база в РФ

Уголовный кодекс (уголовно-правовое регулирование информационных правоотношений):

УК РФ Глава 28. Преступления в сфере компьютерной информации

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами -

- наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, -

- наказываются лишением свободы на срок от трех до семи лет.

3.2.Нормативно-правовая база в РФ

Уголовный кодекс (уголовно-правовое регулирование информационных правоотношений):

УК РФ Глава 28. Преступления в сфере компьютерной информации

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, -
- наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, -
- наказывается лишением свободы на срок до четырех лет.

3.2.Нормативно-правовая база в РФ

Федеральные законы:

- «О безопасности» (№390-ФЗ от 28.12.2010);
- «О государственной тайне» (№ 5485-1 от 21.07.93, посл.изм. 2010г.);
- «Об информации, информационных технологиях и о защите информации» (№ 149-ФЗ от 27.07.2006, посл.изм.2011 г.);
- «О связи» (№ 126-ФЗ от 07.07.2003)
- «О лицензировании отдельных видов деятельности» (№ 99-ФЗ от 04.05.2011);
- «О коммерческой тайне» (№98-ФЗ от 29.07.2004, посл изм.2011 г.);
- «О техническом регулировании» (№184-ФЗ от 27.12.2002, посл.изм.01.09.2013г.);
- «О персональных данных (№ 152-ФЗ от 27.07.2006, посл.изм.2011 г.));
- «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» (№190-ФЗ от 19.12.2005)
- «Об электронной цифровой подписи» (№ 1-ФЗ от 10.01.2002, посл.изм. 2010 г.)
- «Об электронной подписи» (№ 63 от 06.04.2011)

3.2.Нормативно-правовая база в РФ

Указы президента:

- «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» (№ 334, 03 апреля 1995);
- «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне» (Распоряжение Президента № 151-рп, 16 апреля 1995) ;
- «Об утверждении Перечня сведений, отнесенных к государственной тайне» (№ 1203, 30 ноября 1995);
- «О перечне сведений, отнесенных к государственной тайне» (№ 61, 24 января 1998);
- «Об утверждении перечня сведений конфиденциального характера» (№188, 6.03.97);
- «Доктрина информационной безопасности РФ» (№ ПР-1895, 9.09.2000)
- «О стратегии национальной безопасности России до 2020 г.» (№537, 112.05.2009);

3.2.Нормативно-правовая база в РФ

Указы президента:

- О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных» (Распоряжение Президента № 366-рп, 10 июля 2001);
- «Вопросы Федеральной службы безопасности» (№ 960, 11 августа 2003);
- «Вопросы Федеральной службы охраны» (№ 1013, 07 августа 2004;
- «Вопросы Федеральной службы по техническому и экспортному контролю» (1085, 16 августа 2004);
- «О Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия» (№ 320, 12 марта 2007);
- «Об утверждении положения о персональных данных государственного гражданского служащего и ведении его личного дела» (№ 609, 30 мая 2005);
- "О мерах по обеспечению ИБ РФ в сфере международного информационного обмена« (№611, 12.05.2004).
- «О мерах по обеспечению ИБ при использовании информационно-телекоммуникационных сетей международного информационного обмена» (№ 351, 17 марта 2008);

3.2.Нормативно-правовая база в РФ

Постановления Правительства РФ:

- «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» (№ 1233, 03 ноября 1994);
- «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности (№870, 4.09.95);
- «Об утверждении Правил разработки перечня сведений, отнесенных к государственной тайне» (№ 443, 23 июля 2005);
- «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» (№ 63,06.02.2010);
- «Вопросы Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия» (№ 353, 06.06.2007);

3.2.Нормативно-правовая база в РФ

Постановления Правительства РФ:

- «О сертификации средств защиты информации» (№608Б 26.06.1995);
- «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (№ 781, 17.11.2007);
- «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» (№ 512, 06.06.2008);
- «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (№ 687, 15.09.2008);

3.2.Нормативно-правовая база в РФ

Постановления Правительства РФ:

- «О лицензировании деятельности по технической защите конфиденциальной информации» (№ 504, 15 августа 2006);
- «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации» (№ 532, 31 августа 2006);
- «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» (№ 957, 29 декабря 2007); “Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)” (№313, 16.04.2012)

3.2.Нормативно-правовая база в РФ

Нормативные документы уполномоченных федеральных органов:

- ФСТЭК России (Гостехкомиссии России)
- ФСБ России
- Мининформсвязь
- Россвязькомнадзор
- Рособразование

3.2.Нормативно-правовая база в РФ

Нормативные документы уполномоченных федеральных органов:

ФСТЭК России (Гостехкомиссии России)

- Положение по аттестации объектов информатизации по требованиям безопасности информации (Приказ Председателя Гостехкомиссии России от 25.11.1994);
- Положение о сертификации средств защиты информации по требованиям безопасности информации (Приказ Председателя Гостехкомиссии России от 27.10.1995 г. № 199);
- «Защита от НСД к информации. Термины и определения» (Руководящий документ Гостехкомиссии России) ;
- «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» (Приказ ФСТЭК РФ № 58 от 05 февраля 2010);
- «Об утверждении Порядка проведения классификации информационных систем персональных данных» (Приказ ФСТЭК РФ № 55, ФСБ РФ № 86, Мининформсвязи РФ № 20 от 13 февраля 2008);

3.2.Нормативно-правовая база в РФ

Нормативные документы уполномоченных федеральных органов:

ФСБ России

- Приказ ФСБ РФ № 66 от 09 февраля 2005 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»
- Приказ ФСБ РФ № 104 от 16 марта 2009 г. «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по предоставлению услуг в области шифрования информации»
- Приказ ФСБ РФ № 105 от 16 марта 2009 г. «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по техническому обслуживанию шифровальных (криптографических) средств»
- Приказ ФСБ РФ № 106 от 16 марта 2009 г. «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по распространению шифровальных (криптографических) средств»

3.2.Нормативно-правовая база в РФ

Нормативные документы уполномоченных федеральных органов:

Минкомсвязь

- Письмо Минкомсвязи РФ № ДС-П11-2502 от 13 мая 2009 «Об осуществлении трансграничной передачи персональных данных»
- Приказ Минкомсвязи РФ № 104 от 25 августа 2009 «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования»
- Приказ Минкомсвязи РФ № 18 от 30 января 2010 «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции «Ведение реестра операторов, осуществляющих обработку персональных данных»

Россвязькомнадзор

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

Рособразование

- Письмо Рособразования № 17-110 от 29 июля 2009 г. «Об обеспечении защиты персональных данных»

3.3.Техническое регулирование в области ИБ

Федеральный закон: «О техническом регулировании» (№184-ФЗ от 27.12.2002, ред. от 23.07.2013);

Закон регулирует отношения, возникающие при
оценки соответствия;
при разработке, принятии, применении и исполнении требований :

- **обязательных**
  - объекты технического регулирования:
    - к продукции, в том числе зданиям и сооружениям (далее - продукция)
    - к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации
- **на добровольной основе**
  - выполнению работ или оказанию услуг

Техническое регулирование – правовое регулирование этих отношений.

3.3.Техническое регулирование в области ИБ: ФЗ«О техническом регулировании» №184-ФЗ 2002 г. (ред. от 23.07.2013)

Основные цели технического регулирования:

- применение единых правил установления требований к продукции или к продукции и связанным с требованиями к продукции процессам проектирования, производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;
- соответствие технического регулирования уровню развития национальной экономики, развития материально-технической базы, а также уровню научно-технического развития;
- независимость органов по аккредитации, органов по сертификации от изготовителей, продавцов, исполнителей и приобретателей, в том числе потребителей;
- единая система и правила аккредитации;
- недопустимость ограничения конкуренции при осуществлении аккредитации и сертификации;

3.3.Техническое регулирование в области ИБ: ФЗ«О техническом регулировании» №184-ФЗ 2002 г. (ред. от 23.07.2013)

Инструменты технического регулирования:

1. Технический регламент - документ, который принят -

- международным договором РФ, подлежащим ратификации в порядке, установленном законодательством РФ, или в соответствии с международным договором РФ, ратифицированным в порядке, установленном законодательством РФ, или федеральным законом, или указом Президента РФ,
- постановлением Правительства РФ, или нормативным правовым актом федерального органа исполнительной власти по техническому регулированию

Технический регламент устанавливает **обязательные** для применения и исполнения требования к объектам технического регулирования

2.Декларация о соответствии - документ, удостоверяющий соответствие выпускаемой в обращение продукции требованиям технических регламентов;

3.3.Техническое регулирование в области ИБ: ФЗ«О техническом регулировании» №184-ФЗ 2002 г. (ред. от 23.07.2013)

Инструменты технического регулирования:

3.Сандарт - документ, в котором устанавливаются характеристики продукции, правила осуществления и характеристики процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг.

Стандарт также может содержать правила и методы исследований (испытаний) и измерений, правила отбора образцов, требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения;

Стандарт устанавливает добровольное для применения и исполнения требования к объектам стандартизации

3.3.Техническое регулирование в области ИБ: ФЗ«О техническом регулировании» №184-ФЗ 2002 г. (ред. от 23.07.2013)

Инструменты технического регулирования:

Технические регламенты:
являются обязательными

Стандарты:
являются рекомендательными

3.3.Техническое регулирование в области ИБ:
ФЗ«О техническом регулировании» №184-ФЗ 2002 г. (ред. от 23.07.2013)

Технические регламенты принимаются в целях:

- защиты жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества;
- охраны окружающей среды, жизни или здоровья животных и растений;
- предупреждения действий, вводящих в заблуждение приобретателей, в том числе потребителей;
- обеспечения энергетической эффективности и ресурсосбережения.

Принятие технических регламентов в иных целях не допускается

3.3.Техническое регулирование в области ИБ:

ФЗ«О техническом регулировании» №184-ФЗ 2002 г. (ред. от 23.07.2013)

Технические регламенты с учетом степени риска причинения вреда устанавливают минимально необходимые требования, обеспечивающие:

- безопасность излучений; биологическую безопасность;
- взрывобезопасность; механическую безопасность;
- пожарную безопасность;
- безопасность продукции (технических устройств, применяемых на опасном производственном объекте);
- термическую безопасность; химическую безопасность;
- электрическую безопасность;
- радиационную безопасность населения;
- электромагнитную совместимость в части обеспечения безопасности работы приборов и оборудования;
- единство измерений;
- другие виды безопасности, соответствующие целям технического регулирования

(ИБ в этом перечне отсутствует!!!!)

3.3.Техническое регулирование в области ИБ:

ФЗ«О техническом регулировании» №184-ФЗ 2002 г. (ред. от 23.07.2013)

ИБ может рассматриваться как необходимое условие обеспечения приведенных в ФЗ «безопасностей»

Однако для эффективности требований ТР они должны учитывать специфику соответствующих сегментов информационной инфраструктуры (в частности, характер угроз).

- **Следовательно, потребуется разработать и ввести достаточно большое число ТР (сложность процедуры принятия ТР … длительный процесс)**

3.3.Техническое регулирование в области ИБ:

ФЗ«О техническом регулировании» №184-ФЗ 2002 г. (ред. от 23.07.2013)

Документы в области стандартизации

- национальные стандарты;
- правила стандартизации, нормы и рекомендации в области стандартизации;
- применяемые в установленном порядке классификации, общероссийские классификаторы технико-экономической и социальной информации;
- стандарты организаций;
- своды правил;
- международные стандарты, региональные стандарты, региональные своды правил, стандарты иностранных государств и своды правил иностранных государств, зарегистрированные в Федеральном информационном фонде технических регламентов и стандартов;

3.4.Стандартизация обеспечения ИБ

Стандартизация ИБ на международном уровне

- **ISO: International Standardization Organization**
  (ИСО: Международная организация по стандартизации)
- **IEC:International Electro-technical Commission**
  (МЭК : Международная электротехническая комиссия)
- **ITU: International Telecommunications Union**
  МСЭ : Международный союз электросвязи
- **IETF: Internet Engineering Task Force**
  (IETF: Комиссия по технологиям Internet)
- **EMV:Europay, MasterCard и Visa International**
  (EMB:Международная организация пластиковых карт)
- **OECD:Organization for Economic Cooperation and Development**
  (ОЭСР:Организация по экономическому сотрудничеству и развитию)

3.4.Стандартизация обеспечения ИБ

Стандартизация ИБ на международном уровне

- **ECMA:European computer manufacturers association**
  (ЕАПК:Европейская ассоциация производителей компьютеров)
- **ETSI:European Telecommunications Standards Institute**
  (ЕИСТ:Европейский институт стандартизации телекоммуникаций)

3.4.Стандартизация обеспечения ИБ

Стандартизация ИБ на международном уровне

- **NIST: National Institute of Standards and Technology**
  (НИСТ: Национальный институт стандартов и технологий США)
- **ANSI:American national standard institute**
  (АНСИ:Американский национальный институт стандартизации)
- **BSI:British Standard Institute**
  (БСИ:Британский институт стандартизации)

3.4.Стандартизация обеспечения ИБ

Стандартизация ИБ на международном уровне

•ISO: International Standardization Organization

(ИСО: Международная организация по стандартизации)

создана в 1946 г., содержит около 200 технических комитетов (ТС), свыше15000 стандартов, 156 стран-участниц

ТК 68 ИСО «Банковское дело и связанные с ним финансовые услуги» включает ПК2 «Менеджмент безопасности и общие банковские операции»

IEC:International Electro-technical Commission

(МЭК : Международная электротехническая комиссия)

создана в 1944, содержит более 100 ТС

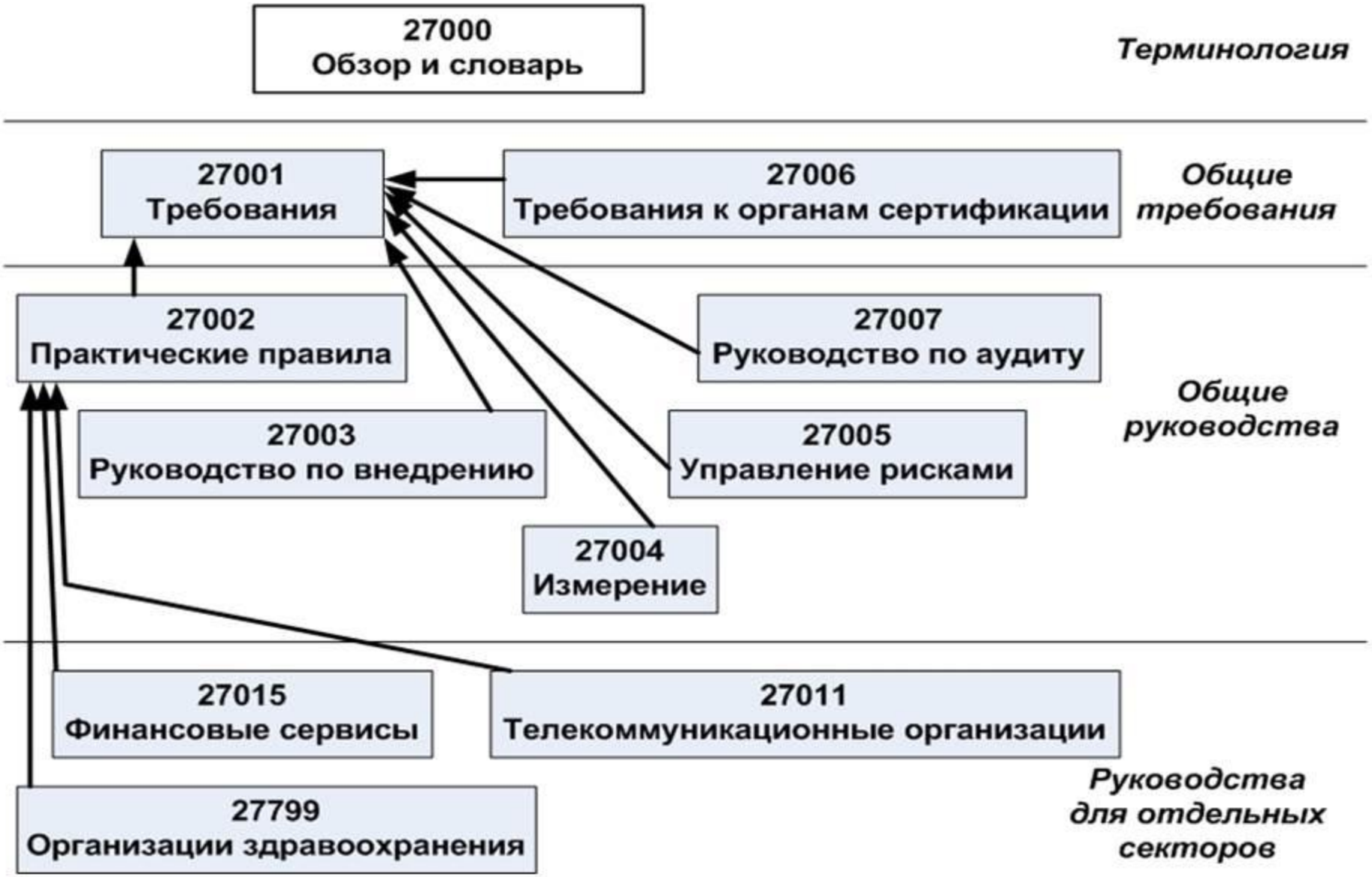
ISO/IEC (ИСО/МЭК):

Объединенный технический комитет (JTC 1)

JTC 1 –разрабатывает стандарты в области ИТ

Подкомитет 27 (SC 27) JTC 1 работает в сфере ИБ

3.4.Стандартизация обеспечения ИБ: серия ISO/IEC 27000



3.4.Стандартизация обеспечения ИБ: серия ISO/IEC 27000

Номер и год принятия	*Название*
27000:2014	СУИБ. Обзор и основные термины
27001:2013/ Cor 1:2014	СУИБ. Требования (на основе BS 7799–2:2005)
27002:2013/ Cor 1:2014	Практические правила управления ИБ (ранее ISO/IEC 17799:2005)
27003:2010	Руководство по внедрению СУИБ *(готовится новая редакция - ГНР)*
27004:2009	Управление ИБ. Оценка СУИБ *(ГНР)*
27005:2011	Управление рисками ИБ (на основе BS 7799–3:2006) *(ГНР)*
27006:2011	Требования к органам, обеспечивающим аудит и сертификацию СУИБ *(ГНР)*
27007:2011	Руководство по аудиту СУИБ *(ГНР)*
27008:2011	Руководство по аудиту средств управления ИБ, реализованных в СУИБ *(ГНР)*
27009	Использование и применение ISO/IEC 27001 при сертификации аккредитованных третьих сторон для отдельного сектора/сервиса
27010:2012	Управление ИБ при коммуникации между секторами (в нескольких частях, предоставляющих руководство по совместному использованию информации о рисках ИБ, средствах управления, проблемах и/или инцидентах ИБ, выходящих за границы отдельных секторов экономики и государств, особенно в части, касающейся критичных инфраструктур) *(ГНР)*
27011:2008	Руководство по управлению ИБ для телекоммуникационных компаний на основе ISO/IEC 27002 *(ГНР)*
27013:2012	Руководство по интегрированному внедрению ISO 27000 и ISO 20000-1 *(ГНР)*
27014:2013	Руководство ИБ
27015:2012	Руководство по внедрению СУИБ для финансовых сервисов (банков, страховых компаний, кредитных организаций и т.д.)
27016:2014	Управление ИБ. Экономика организации
27017	Практические правила для средств управления ИБ для сервисов облачных вычислений на основе ISO/IEC 27002

3.4.Стандартизация обеспечения ИБ: серия ISO/IEC 27000

27018:2014	Практические правила для средств управления защитой данных в общедоступных сервисах облачных вычислений
27019:2013	Руководство по управлению ИБ на базе ISO/IEC 27002 для систем управления процессами, характерными для энергетической промышленности
27021	Компетентностные требования к профессионалам в области СУИБ
27023	Соответствие пересмотренных редакций ISO/IEC 27001 и ISO/IEC 27002
27031:2011	Руководство по готовности информационных и телекоммуникационных технологий для обеспечения непрерывности бизнеса (на основе BS 25699:2006/2007)
27032:2012	Руководство по обеспечению кибербезопасности
27033	27033–1:2009 Безопасность сетей. Часть 1. Общие положения и концепции *(ГНР)*
	27033–2:2012 Руководство по проектированию и внедрению системы обеспечения безопасности сетей
	27033–3:2010 Базовые сетевые сценарии – угрозы, методы проектирования и средства управления
	27033–4:2014 Обеспечение безопасности межсетевых взаимодействий при помощи шлюзов безопасности
	27033–5:2013 Обеспечение безопасности связи в сетях на основе использования виртуальных частных сетей
	27033–6 Защита беспроводного доступа к IP-сетям
27034	27034–1:2011/Cor1:2014 Безопасность приложений. Часть 1. Обзор и основные концепции в области обеспечения безопасности приложений
	27034–2 Нормативная база организации
	27034–3 Процесс управления безопасностью приложений
	27034–4 Оценка безопасности приложений
	27034–5 Протоколы и структура управляющей информации для обеспечения безопасности приложений (отдельно 5-1 для XML-схем)
	27034–6 Руководство по обеспечению безопасности конкретных приложений

3.4.Стандартизация обеспечения ИБ: серия ISO/IEC 27000

27035:2011	Управление инцидентами безопасности (заменил ISO/IEC TR 18044) *(готовится 3 новых части)*
27036	27036-1:2014 ОИБ при взаимоотношениях с другими организациями (поставщиками). Часть 1: Обзор и концепции 27036-2:2014 Требования 27036-3:2013 Руководство по защите цепи поставок информационных и коммуникационных технологий 27036 Руководство по защите облачных сервисов
27037:2012	Руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в цифровой форме (на основе BS 10008:2008)
27038:2014	Спецификация для изданий, представленных в цифровой форме
27039:2015	Выбор, размещение и функционирование систем обнаружения и предотвращения вторжений *(вместо 18043:2006)*
27040:2015	Безопасность хранения данных
27041	Руководство по обеспечению применимости и адекватности методов исследования свидетельств, представленных в цифровой форме
27042	Руководство по анализу и интерпретации свидетельств, представленных в цифровой форме
27043:2015	Принципы и процессы исследования свидетельств, представленных в цифровой форме
27044	Руководство по управлению информацией и событиями безопасности (SIEM)
27050	27050-1 Обнаружение с помощью электронных средств. Часть 1. Обзор и концепции 27050-2 Рекомендации по руководству и управлению обнаружением с помощью электронных средств 27050-3 Процессуальный кодекс обнаружения с помощью электронных средств 27050-4 Готовность ИТТ для обнаружения с помощью электронных средств

3.4.Стандартизация обеспечения ИБ: серия ISO/IEC 27000

Российский стандарт	*Международный стандарт*	*Британский стандарт*
ГОСТ Р ИСО/МЭК 27000-2012	ISO/IEC 27000:2009	
ГОСТ Р ИСО/МЭК 27001-2006	ISO/IEC 27001:2005	BS 7799-2:2002
ГОСТ Р ИСО/МЭК 27002-2012	ISO/IEC 27002:2005	BS 7799-1:2002
ГОСТ Р ИСО/МЭК 27003-2012	ISO/IEC 27003:2010	
ГОСТ Р ИСО/МЭК 27004-2011	ISO/IEC 27004:2009	
ГОСТ Р ИСО/МЭК 27005-2010	ISO/IEC 27005:2008	BS 7799-3:2005
ГОСТ Р ИСО/МЭК 27006-2008	ISO/IEC 27006:2007	
ГОСТ Р ИСО/МЭК 27007-2014	ISO/IEC 27007:2011	
ГОСТ Р ИСО/МЭК 27011-2012	ISO/IEC 27011:2008	
ГОСТ Р ИСО/МЭК 27013-2014	ISO/IEC 27013:2012	
ГОСТ Р ИСО/МЭК 27031-2012	ISO/IEC 27031:2011	
ГОСТ Р ИСО/МЭК 27033-1-2011	ISO/IEC 27033-1:2009	
ГОСТ Р ИСО/МЭК 27033-3-2014	ISO/IEC 27033-3:2010	
ГОСТ Р ИСО/МЭК 27034-1-2014	ISO/IEC 27034-1:2011	
ГОСТ Р ИСО/МЭК 27037-2014	ISO/IEC 27037:2012	
ГОСТ Р ИСО/МЭК 18045-2013	ISO/IEC 18045:2008	
ГОСТ Р ИСО/МЭК 15408-1-2008	ISO/IEC 15408-1:2005	
ГОСТ Р ИСО/МЭК 15408-2-2013	ISO/IEC 15408-2:2008	
ГОСТ Р ИСО/МЭК 15408-3-2013	ISO/IEC 15408-3:2008	

3.4.Стандартизация обеспечения ИБ: серия Р ИСО/МЭК 27000

- ГОСТ Р ИСО/МЭК 27000-2012 ИТ. Методы и средства обеспечения безопасности. Системы менеджмента ИБ. Общий обзор и терминология.
- ГОСТ Р ИСО/МЭК 27001-2012 ИТ. Методы и средства обеспечения безопасности. Системы менеджмента ИБ. Требования.
- ГОСТ Р ИСО/МЭК 27002-2012 ИТ. Практические правила менеджмента ИБ.
- ГОСТ Р ИСО/МЭК 27003-2012 ИТ. Методы и средства обеспечения безопасности. Системы менеджмента ИБ. Руководство по реализации системы менеджмента ИБ.
- ГОСТ Р ИСО/МЭК 27011-2012 ИТ. Методы и средства обеспечения безопасности. Руководства по менеджменту ИБ для телекоммуникационных организаций на основе ИСО/МЭК 27002.
- ГОСТ Р ИСО/МЭК 27033-1-2011 ИТ. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.

3.4.Стандартизация обеспечения ИБ - Национальные стандарты РФ

Группы стандартов - количество стандартов в группе

1.Стандарты основополагающие
1.1.Организационно-методические и общетехнические - 10
1.2.Защищенные автоматизированные системы (АС) - 5
1.3.Оценка безопасности информационных систем (ИТ) - 5
2.Стандарты по криптографии - 3
3.Стандарты на термины и определения -6
4.Стандарты на продукцию (средства и системы безопасности)- 3
5.Стандарты на услуги - 2
6.Стандарты на методы контроля - 3
7.Стандарты на процессы управления ИБ - 13

ВСЕГО – 50

3.4.Стандартизация обеспечения ИБ - Национальные стандарты РФ

Группа: «Стандарты основополагающие» (организационно-методические и общетехнические)

1. ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты
2. ГОСТ Р 52069.0-2003 ЗИ. Система стандартов. Основные положения.
3. ГОСТ Р 51275-2006 ЗИ. Объекты информатизации. Факторы, воздействующие на информацию. Общие положения.
4. ГОСТ Р ИСО 9594-8-98 Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации.
5. ГОСТ Р 52448-2005 ЗИ. Обеспечение безопасности сетей электросвязи. Общие положения.
6. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
7. ГОСТ Р 53109-2008 Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности.
8. ГОСТ Р ИСО 7498-2-99 ИТ. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.
9. ГОСТ Р 54581-2011 ИТ. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы.
10. ГОСТ Р 51901.4-2005 Менеджмент риска. Руководство при применению и проектированию.

3.4.Стандартизация обеспечения ИБ - Национальные стандарты РФ

Группа: «Стандарты основополагающие» (защищенные АС)

1. ГОСТ Р 51624-2000 ЗИ. АС в защищенном исполнении. Общие требования.
2. ГОСТ Р 51583-2000 ЗИ. Порядок создания АС в защищенном исполнении. Общие положения.
3. ГОСТ Р 53113.1-2008 Защита информационных технологий и АС от угроз ИБ, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.
4. ГОСТ Р 53113.2-2009 Рекомендации по организации ЗИ, информационных технологий и АС от атак с использованием скрытых каналов.
5. ГОСТ Р ИСО/МЭК ТО 19791-2008 ИТ. Методы и средства обеспечения безопасности. Оценка безопасности АС.

3.4.Стандартизация обеспечения ИБ - Национальные стандарты РФ

Группа: «Стандарты основополагающие» (оценка безопасности ИТ)

1. ГОСТ Р ИСО/МЭК 15408-1-2008 ИТ. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
2. ГОСТ Р ИСО/МЭК 15408-2-2008 - ИТ. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
3. ГОСТ Р ИСО/МЭК 15408-3-2008 ИТ. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
4. ГОСТ Р ИСО/МЭК 18045-2008 ИТ. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.
5. ГОСТ Р ИСО/МЭК ТО 15446-2008 Руководство по разработке профилей защиты и заданий по безопасности.

3.4.Стандартизация обеспечения ИБ - Национальные стандарты РФ

Группа: «Стандарты по криптографии»

1. **ГОСТ 28147-89 Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.**

2. **ГОСТ Р 34.11-2012 ИТ. Криптографическая защита информации. Функция хеширования.** (Создан взамен ГОСТ 34.11-94).

3. **ГОСТ 34.10-2012 ИТ. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.** (Создан взамен ГОСТ Р 34.10-2001. До ГОСТ Р 34.10-2001 действовал стандарт ГОСТ Р 34.10-94).

Приняты и введены в действие Приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 года № 215-ст

3.4.Стандартизация обеспечения ИБ - Национальные стандарты РФ

Группа: «Стандарты на термины и определения»

1. ГОСТ Р 50922-2006. ЗИ. Основные термины и определения.
2. ГОСТ Р 53114-2008 ЗИ. Обеспечение информационной безопасности в организации. Основные термины и определения.
3. Р 50.1.053-2005 Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации.
4. Р 50.1.056-2005 Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения.
5. ГОСТ 15971-90 Системы обработки информации. Термины и определения.
6. ГОСТ 34.003-90 ИТ. Комплекс стандартов на АС. Автоматизированные системы. Термины и определения.

3.4.Стандартизация обеспечения ИБ - Национальные стандарты РФ

Группа: «Стандарты на услуги»

1. ГОСТ Р ИСО/МЭК 13569-2007 Финансовые услуги. Рекомендации по информационной безопасности.
2. ГОСТ Р 53131-2008 ЗИ. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения.

Группа: «Стандарты на методы контроля»

1. ГОСТ Р 51188-98 ЗИ. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.
2. ГОСТ Р 53112-2008 ЗИ. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний.
3. ГОСТ Р 53115-2008 ЗИ. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства.

3.4.Стандартизация обеспечения ИБ - Национальные стандарты РФ

Группа «Стандарты на продукцию (средства и системы безопасности)»

1. ГОСТ Р 52633-2006 ЗИ. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.
2. ГОСТ Р 51839.3-2001 Защитные технологии. Средства защиты. Защита противокопировальная. Общие технические требования.
3. ГОСТ Р 50543-93 Конструкции базовые несущие СВТ. Требования по обеспечению ЗИ и ЭМС методом экранирования.

Группа: «Стандарты на процессы (ИТ-ЗИ)»

1. ГОСТ 29339-92 ИТ. ЗИ от утечки за счет ПЭМИН при ее обработке СВТ. ОТТ.
2. ГОСТ Р 50752-95 ИТ. ЗИ от утечки за счет ПЭМИН при ее обработке СВТ. Методы испытаний.

3.4.Стандартизация обеспечения ИБ - Национальные стандарты РФ

Группа: «Стандарты на процессы (менеджмент – ИТ)»

1. ГОСТ Р ИСО/МЭК 13335-1-2006 ИТ. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.
2. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 ИТ. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий.
3. ГОСТ Р ИСО/МЭК 13335-4-2006 ИТ. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер.
4. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 ИТ. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети.
5. ГОСТ Р ИСО/МЭК ТО 18044 – 2007 ИТ. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

3.4.Стандартизация обеспечения ИБ - Национальные стандарты РФ

Группа: «Стандарты на процессы (менеджмент – ИТ/27000)»

1. ГОСТ Р ИСО/МЭК 27001-2012 ИТ. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
2. ГОСТ Р ИСО/МЭК 27002-2012 ИТ. Методы и средства обеспечения безопасности. Практические правила менеджмента информационной безопасности.
3. ГОСТ Р ИСО/МЭК 27004-2011 ИТ. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.
4. ГОСТ Р ИСО/МЭК 27005-2010 ИТ. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
5. ГОСТ Р ИСО/МЭК 27006-2008 ИТ. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.
6. ГОСТ Р ИСО/МЭК 27033-1-2011 ИТ. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.

3.4.Стандартизация обеспечения ИБ - Отраслевые стандарты

Основные цели такой стандартизации:

- повышение доверия к организациям отрасли;
- повышение стабильности функционирования организаций отрасли и на этой основе – стабильности функционирования отрасли в целом;
- достижение адекватности мер по защите от реальных угроз ИБ;
- предотвращение и/или снижение ущерба от инцидентов ИБ.
- **Основные задачи стандартизации в отрасли:**
- установление для организаций отрасли единых требований по обеспечению ИБ;
- повышение эффективности мероприятий по обеспечению и поддержанию ИБ организаций отрасли.

3.4.Стандартизация обеспечения ИБ - Отраслевые стандарты

Стандарты Банка России:

- **СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» – пятая редакция введена в действие с 1 июня 2014 г.**

- **СТО БР ИББС-1.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности» – первая редакция введена в действие с 1 мая 2007 г.**

- **СТО БР ИББС-1.2 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций БС РФ требованиям СТО БР ИББС-1.0» – четвертая редакция введена в действие с 1 июня 2014 г.**

3.4.Стандартизация обеспечения ИБ - Отраслевые стандарты

Рекомендации в области стандартизации Банка России:

- РС БР ИББС-2.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0» – с 1 мая 2007 г.
- РС БР ИББС-2.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций БС РФ требованиям СТО БР ИББС-1.0» – с 1 мая 2007 г.
- РС БР ИББС-2.2 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» – с 1 января 2010 г.
- РС БР ИББС-2.5 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности» - с 1 июня 2014 г.
- РС БР ИББС-2.6 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем» - с 1 сентября 2014 г.
- РС БР ИББС-2.7 «Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем. Ресурсное обеспечение деятельности службы информационной безопасности»- 1 мая 2015 г.
- РС БР ИББС-2.8 «Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем. Обеспечение информационной безопасности при использовании технологии виртуализации» 1 мая 2015 г.

3.4.Стандартизация обеспечения ИБ - Отраслевые стандарты

Проекты документов

- **СТО БР ИБНФО Б-1.0 201х** «Обеспечение информационной безопасности некредитных финансовых организаций. Общие положения» - Проект 2016 г.
- **СТО БР ИБНФО М-1.0 201х** «Обеспечение информационной безопасности некредитных финансовых организаций, соответствующих критериям отнесения к малым предприятиям и микропредприятиям. Общие положения» - Проект 2016г.
- **РС БР ИББС-2.ХХ** «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение совершения переводов денежных средств без согласия клиента (антифрод)» - Проект 2016г.
- **РС БР ИББС-2.ХХ** «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Квалификационные требования к специалистам по информационной безопасности организаций кредитно-финансовой сферы Российской Федерации » - Проект 2016 г.
- **РС БР ИББС-2.ХХ** «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение длительного архивного хранения электронных юридически значимых документов с сохранением свойств аутентичности, целостности, достоверности, пригодности для использования и юридической значимости» - Проект 2016 г.
- **РС БР ИББС-2.ХХ** «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечки информации» - Проект 2016 г.

3.4.Стандартизация обеспечения ИБ - Отраслевые стандарты

3.4.Стандартизация обеспечения ИБ - Отраслевые стандарты

Корпоративная система нормативно-методических документов в области комплексных систем безопасности объектов ОАО «Газпром».

Система обеспечения информационной безопасности ОАО «Газпром»:

Стандарты основополагающие (организационно-методические и общетехнические (код 0)

- **СТО Газпром 4.2-0-001-2009 «Документы системы».**
- **СТО Газпром 4.2-0-002-2009 «Правила изложения, оформления, обозначения документов в области стандартизации».**
- **СТО Газпром 4.2-0-003-2009 «Общие положения».**
- **СТО Газпром 4.2-0-004-2009 «Базовая модель угроз ИБ корпоративным информационно-управляющим системам».**

Стандарты на термины и определения (код 1)

- **СТО Газпром 4.2-1-001-2009 «Основные термины и определения».**

Стандарты на продукцию (средства и системы безопасности) (код 2)

- **СТО Газпром 4.2-2-001-2009 «Требования к информационно-управляющим системам предприятия».**
- **СТО Газпром 4.2-2-002-2010 «Требования к АС управления технологическими процессами».**
- **СТО Газпром 4.2-2-003-2010 «Требования по защите от подделок документов на бумажных носителях».**

3.4.Стандартизация обеспечения ИБ - Отраслевые стандарты

Корпоративная система нормативно-методических документов в области комплексных систем безопасности объектов ОАО «Газпром».

Система обеспечения информационной безопасности ОАО «Газпром»:

Стандарты на процессы (код 3)

- СТО Газпром 4.2-3-001-2009 «Руководство по разработке требований к объектам защиты».
- СТО Газпром 4.2-3-002-2009 «Требования по защите информации при использовании информационных технологий».
- СТО Газпром 4.2-3-003-2009 «Анализ и оценка рисков».
- СТО Газпром 4.2-3-004-2009 «Классификация объектов защиты.

Стандарты на услуги (код 4)

Стандарты на методы контроля (код 5)

- СТО Газпром 4.2-5-001-2009 «Оценка соответствия объектов защиты».

3.4.Стандартизация обеспечения ИБ - Отраслевые стандарты

Корпоративная система нормативно-методических документов в области комплексных систем безопасности объектов ОАО «Газпром».

Система обеспечения информационной безопасности ОАО «Газпром»:

Рекомендации организации (организационно-методические и общетехнические

- **Р Газпром 4.2-0-001-2009 «Типовая политика ИБ дочернего общества (организации)».**
- **Р Газпром 4.2-0-002-2009 «Типовая политика ИБ информационно-управляющей системы производственно-хозяйственной деятельности».**
- **Р Газпром 4.2-0-003-2009 «Типовая политика ИБ автоматизированной системы управления технологическими процессами».**
- **Р Газпром 4.2-0-004-2009 «Типовая политика ИБ региональной сети передачи данных (локальной вычислительной сети)».**
- **Р Газпром 4.2-0-005-2010 «Модель угроз персональных данных при обработке в информационных системах персональных данных ОАО «Газпром», его дочерних обществ и организаций».**

3.4.Стандартизация обеспечения ИБ - Отраслевые стандарты

Корпоративная система нормативно-методических документов в области комплексных систем безопасности объектов ОАО «Газпром».

Система обеспечения информационной безопасности ОАО «Газпром»:

Рекомендации организации (организационно-методические и общетехнические)

- **Р Газпром 4.2-2-001-2009 «Технические требования к обеспечению ИБ в беспроводных сетях, развертываемых на объектах ОАО «Газпром», его дочерних обществ и организаций».**
- **Р Газпром 4.2-2-002-2009 «Технические требования к системе защиты информации центрального вычислительного комплекса информационно-вычислительной сети администрации ОАО «Газпром».**

Рекомендации организации (на процессы)

- **Р Газпром 4.2-3-001-2010 «Методика проведения классификации информационных систем персональных данных ОАО «Газпром», его дочерних обществ и организаций».**
- *Рекомендации организации (на методы контроля)*
- **Р Газпром 4.2-5-001-2009 «Методика сертификационных испытаний информационно-управляющих систем предприятия».**
- **Р Газпром 4.2-5-002-2009 «Методика сертификационных испытаний автоматизированных систем управления технологическими процессами».**
- **Р Газпром 4.2-5-003-2009 «Методика испытаний средств и систем обеспечения безопасности информационных технологий».**

3.5.Нормативно-правовое обеспечение безопасности КВО

Основные нормативные правовые акты государств-членов ОДКБ:

В Республике Беларусь:

- Закон Республики Беларусь от 10 января 2000 года № 363-З «О промышленной безопасности опасных производственных объектов»,
- Указ Президента Республики Беларусь от 25 октября 2011 года № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»;
- Постановление Совета министров Республики Беларусь от 30 марта 2012 года «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации».

В Республике Казахстан:

- Закон Республики Казахстан от 11 апреля 2014 года № 188-V «О гражданской защите».

В Республике Таджикистан:

- Закон Республики Таджикистан от 28 февраля 2004 года № 14 «О промышленной безопасности опасных
- производственных объектов».

3.5.Нормативно-правовое обеспечение безопасности КВО

Основные нормативные правовые акты государств-членов ОДКБ:

В Российской Федерации:

- Федеральный закон РФ от 21 июля 1997 года № 116-ФЗ «О промышленной безопасности опасных производственных объектов».
- «Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года», утвержденная распоряжением Правительства РФ от 17 ноября 2008 года № 1662-р.
- Указ Президента РФ от 12 мая 2009 года № 537 «О Стратегии национальной безопасности РФ до 2020 года».
- Концепция противодействия терроризму в Российской Федерации, утвержденная Президентом РФ 5 октября 2009 года.
- Федеральный закон РФ от 28 декабря 2010 года № 390 «О безопасности».

3.5.Нормативно-правовое обеспечение безопасности КВО

Основные нормативные правовые акты государств-членов ОДКБ:

В Российской Федерации:

- **Указ Президента РФ от 6 мая 2011 года № 590 «Вопросы Совета Безопасности РФ».**
- **Федеральная целевая программа «Снижение рисков и смягчение последствий чрезвычайных ситуаций природного и техногенного характера в РФ до 2015 года», утвержденная Постановлением Правительства РФ от 7 июля 2011 года № 555.**
- **«Основы государственной политики в области обеспечения безопасности населения РФ и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов на период до 2020 года», утверждены Президентом РФ 15 ноября 2011 года № Пр-3400.**
- **«Концепция федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры РФ и опасных грузов», одобрена Распоряжением Правительства Российской Федерации от 27 августа 2005 года № 1314-р).**

3.5.Нормативно-правовое обеспечение безопасности КВО

Основные нормативные правовые акты государств-членов ОДКБ:

- **В Кыргызской Республике:**
- **Конституционный закон «О чрезвычайном положении» от 24 октября 1998 года № 135.**
- **Уголовный кодекс от 1 октября 1997 года № 68.**
- **Кодекс об административной ответственности от 4 августа 1998 года № 114.**
- **Закон «О пожарной безопасности» от 17 июня 1996 года № 22.**
- **Закон «Об аварийно-спасательных службах и статусе спасателей» от 21 января 2000 года № 35.**
- **Закон «О национальной безопасности» от 26 февраля 2003 года № 44.**
- **Закон «О противодействии терроризму» от 8 ноября 2006 года № 178.**
- **Закон «О стратегических объектах Кыргызской Республики» от 23 мая 2008 года № 94.**
- **Закон «О гражданской защите» от 20 июля 2009 года № 239.**
- **Закон «Об обороне и Вооруженных Силах Кыргызской Республики» от 24 июля**
- **2009 года № 242.**
- **Закон «О Совете обороны Кыргызской Республики» от 15 июля 2011 года № 102;**
- **Закон «Технический регламент «О радиационной безопасности» от 29 ноября 2011 года № 224**
- **Закон «Технический регламент «О промышленной безопасности» от 16 ноября 2013 года № 202.**

3.5.Нормативно-правовое обеспечение безопасности КВО

Основные нормативные правовые акты государств-членов ОДКБ:

В Республике Армения:

- Закон Республики Армения от 24 октября 2005 года ЗР-204-Н «О государственном регулировании обеспечения технической
- безопасности».
- Закон Республики Армения от 2 декабря 1998 ЗР-265 «О защите
- населения при чрезвычайных ситуациях».
- Закон Республики Армения от 5 марта 2002 ЗР-309 «О гражданской обороне».
- Закон Республики Армения от 1 февраля 1999 ЗР-285 «О безопасном использовании атомной энергии в мирных целях».
- Закон Республики Армения ЗР-376-Н «О сейсмической защите».
- Закон Республики Армения ЗР-176 «О пожарной безопасности».
- Постановление Правительства Республики Армения от 13 декабря 1999 года № 746 «О порядке переселения населения из опасных территорий».

3.5.Нормативно-правовое обеспечение безопасности КВО

Основные нормативные правовые акты государств-членов ОДКБ:

В Республике Армения:

- **Постановление Правительства Республики Армения от 28 сентября 2000 года № 679 «О порядке обеспечения населения средствами индивидуальной защиты».**
- **Постановление Правительства Республики Армения от 29 июля 2004 года № 1064-Н «Об утверждении порядка создания и обеспечения деятельности постоянной контролирующей системы за радиационной, химической и биологической обстановкой».**
- **Постановление Правительства Республики Армения от 18 августа 2006 года №**
- **1219-Н «О нормах радиационной безопасности».**
- **Постановление Правительства Республики Армения от 18 августа 2006 года № 1489-Н «О правилах радиационной безопасности».**
- **Постановление Правительства Республики Армения от 30 января 2003 года № 134-Н «О порядке просвещения общественности и подготовки органов государственного управления и местного самоуправления и организаций в области чрезвычайных ситуаций и гражданской обороны».**

3.5.Нормативно-правовое обеспечение безопасности КВО

Проблемы нормативно-правового обеспечения КВО (на примере государств-членов ОДКБ):

Рекомендации по гармонизации законодательства государств – членов Организации Договора о коллективной безопасности (ОДКБ) в сфере обеспечения безопасности критически важных объектов

(Приняты Постановление Парламентской Ассамблеи ОДКБ 27.11.2014 года № 7-5):

Государства – члены ОДКБ: Российская Федерация, Республика Белорусь, Республика Казахстан, Республика Таджикистан, Кыргызская Республика, Республика Армения.

1.Гармонизации законодательства государств - членов ОДКБ в области обеспечения безопасности КВО направлена на формирование общего и единообразного подхода к правовому регулированию данных общественных отношений.

2.Анализ национальных нормативных правовых актов государств - членов ОДКБ выявил отсутствие единых подходов к принятию нормативных правовых актов в области обеспечения безопасности КВО.

3.5.Нормативно-правовое обеспечение безопасности КВО

Проблемы нормативно-правового обеспечения КВО (на примере государств-членов ОДКБ):

Рекомендации по гармонизации законодательства государств – членов Организации Договора о коллективной безопасности (ОДКБ) в сфере обеспечения безопасности критически важных объектов

3.В законодательстве государств — членов ОДКБ отмечается отсутствие единых подходов к пониманию критически важных объектов. В законодательстве некоторых государств такой термин не используется. Поэтому при разработке нормативного правового акта, регулирующего обеспечение безопасности КВО, целесообразно использовать единый Глоссарий терминов в области КВО государств - членов ОДКБ.

4.Особенности национального регулирования общественных отношений по обеспечению безопасности КВО предполагают различные подходы к формированию понятийного аппарата. Определенные трудности для практической деятельности создают также многоязычие и отсутствие на сегодняшний день поверенного аутентичного перевода национальных правовых актов и соответствующих информационных баз.

3.5.Нормативно-правовое обеспечение безопасности КВО

Проблемы нормативно-правового обеспечения КВО (на примере государств-членов ОДКБ):

Рекомендации по гармонизации законодательства государств – членов Организации Договора о коллективной безопасности (ОДКБ) в сфере обеспечения безопасности критически важных объектов

5.Анализ нормативных правовых актов государств - членов ОДКБ позволил выявить отсутствие единообразия в подходах к определению видов и субъектов ответственности.

6.Отсутствует единая классификация КВО.

7.Отсутствует единая методика отнесения государственной и негосударственной собственности к КВО (имеется только у РФ)

Благодарю за внимание!

Толстой Александр Иванович

AlTolstoj@mephi.ru