Лекция
Оценка и контроль защищенности информационных систем

Основы информационной безопасности

Источники требований

- Законодательство
- Технические нормативные правовые акты (регламенты, кодексы, стандарты)
- Политика безопасности

- **«Обращение к стандартам позволяет в собственной практике учесть чужой опыт работы»**

руководитель консультационной компании

Project Management Partners

Билл Дункан.

Республика Беларусь

http://www.tnpa.by/

технические нормативные правовые акты

ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ О ТЕХНИЧЕСКОМ НОРМИРОВАНИИ И СТАНДАРТИЗАЦИИ

Статья 15. Виды технических нормативных правовых актов

К техническим нормативным правовым актам в области технического нормирования и стандартизации относятся:

- технические регламенты;
- технические кодексы;
- стандарты, в том числе государственные стандарты, стандарты организаций;
- технические условия.

Технические нормативные правовые акты

- **Технические регламенты** разрабатываются в целях защиты жизни, здоровья и наследственности человека, имущества и охраны окружающей среды, а также предупреждения действий, вводящих в заблуждение потребителей продукции и услуг относительно их назначения, качества или безопасности. Разработка технических регламентов в иных целях не допускается.
- Технический регламент применяется одинаковым образом и в равной мере независимо от страны и (или) места происхождения продукции.
- Требования утвержденного технического регламента являются обязательными для соблюдения всеми субъектами технического нормирования и стандартизации.
- Технический регламент не может быть введен в действие, если отсутствуют методики контроля, измерений и испытаний технических требований, установленных в техническом регламенте.

Технические нормативные правовые акты

- **Технические кодексы** разрабатываются с целью реализации требований технических регламентов, повышения качества процессов разработки (проектирования), производства, эксплуатации (использования), хранения, перевозки, реализации и утилизации продукции или оказания услуг.
- Разработка и утверждение технических кодексов осуществляются республиканскими органами государственного управления.
- Требования технических кодексов к процессам разработки (проектирования), производства, эксплуатации (использования), хранения, перевозки, реализации и утилизации продукции или оказанию услуг основываются на результатах установившейся практики.
- Технические кодексы вводятся в действие после их государственной регистрации.

Государственные стандарты

- основываются на современных достижениях науки, техники, международных и межгосударственных (региональных) стандартах, правилах, нормах и рекомендациях по стандартизации, прогрессивных стандартах других государств, за исключением случаев, когда такие документы могут быть непригодными или неэффективными для обеспечения:
- национальной безопасности;
- защиты жизни, здоровья и наследственности человека;
- охраны окружающей среды, рационального использования природных ресурсов и энергосбережения;
- предупреждения действий, вводящих в заблуждение потребителей продукции и услуг относительно их назначения, качества или безопасности.

Государственные стандарты в зависимости от объекта стандартизации содержат:

- требования к продукции, процессам ее разработки, производства, эксплуатации (использования), хранения, перевозки, реализации и утилизации или оказанию услуг;
- требования к правилам приемки и методикам контроля продукции;
- требования к технической и информационной совместимости;
- правила оформления технической документации;
- общие правила обеспечения качества продукции (услуг), сохранения и рационального использования ресурсов;
- требования к энергоэффективности и снижению энерго- и материалоемкости продукции, процессов ее производства, эксплуатации (использования), хранения, перевозки, реализации и утилизации или оказания услуг;
- термины и определения, условные обозначения, метрологические и другие общие технические и организационно-методические правила и нормы.

Технические кодексы установившейся практики

- ТКП 061-2007 Банковские технологии. Порядок применения СТБ ИСО/МЭК 12119-2003 в процессе оценки соответствия программных средств.
- ТКП 062.1-2007 Банковские технологии. Порядок создания и обработки электронных платежных документов, используемых в автоматизированной системе межбанковских расчетов Национального банка Республики Беларусь. Часть 1. Сообщения МТ 103, МТ 202, МТ 204.
- ТКП 062.2-2008 (07040) Банковские технологии. Порядок создания и обработки электронных платежных документов, используемых в автоматизированной системе межбанковских расчетов Национального банка Республики Беларусь. Часть 2. Сообщение МТ 102
- ТКП 063.1-2007 Банковские технологии. Порядок создания и обработки платежных инструкций клиента в форме электронных документов. Часть 1. Платежное поручение, платежное требование.
- ТКП 064-2007 (07040) Банковские пластиковые карточки. Периферийное оборудование. Порядок формирования выходных документов
- ТКП 065-2007 (07040) Банковские пластиковые карточки. Периферийное оборудование. Порядок формирования интерфейса пользователя
- ТКП 075-2007 Банковские технологии. Порядок воспроизведения на бумажном носителе платежных инструкций клиента в форме электронных документов. Ч.1 Платежное поручение, платежное требование.
- ТКП 093-2007 Банковские технологии. Порядок воспроизведения на бумажном носителе электронных платежных документов, используемых в автоматизированной системе межбанковских расчетов Национального банка Республики Беларусь. Часть1. Сообщения МТ 103, МТ 202, МТ 204

Технические кодексы установившейся практики

- ТКП 114–2008 (07040) "Банковские технологии. Оценка соответствия программных средств. Порядок оценки соответствия специальным требованиям"
- ТКП 115–2008 (07040) "Банковские технологии. Оценка соответствия программных средств. Порядок оценки соответствия общим требованиям"
- ТКП 133-2008 (07040) Банковские технологии. Порядок создания электронных платежных документов, используемых в Республиканской централизованной системе обмена межбанковской корреспонденцией в форме электронных документов. Часть 1. Сообщение МТ 104
- ТКП 135-2008 (07040) Банковские технологии. Порядок применения СТБ ИСО/МЭК 14764-2003 в процессе оценки сопровождения программных средств
- ТКП 161-2008 (07040) Банковские технологии. Порядок воспроизведения на бумажном носителе электронных платежных документов, используемых в Республиканской централизованной системе обмена межбанковской корреспонденцией в форме электронных документов. Часть 1. Сообщение МТ 104
- ТКП 167-2009 (07040) Банковские технологии. Порядок воспроизведения на бумажном носителе электронных платежных документов, используемых в автоматизированной системе межбанковских расчетов Национального банка Республики Беларусь. Часть 2. Сообщение МТ 102
- ТКП 168-2009 (07040) Банковские технологии. Порядок архивного хранения электронных документов банка, используемых в автоматизированной системе межбанковских расчетов Национального банка Республики Беларусь

Стандарты Республики Беларусь

- СТБ 1176.1-99 Информационная технология. Защита информации. Функция хэширования.
- СТБ 1176.2-99 Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи.

Стандарты Республики Беларусь

- ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.
- ГОСТ 31078-2002 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

Стандарты Республики Беларусь

- СТБ П ИСО/МЭК 17799-2000/2004 Информационные технологии и безопасность. Правила управления информационной безопасностью.
- СТБ П ISO/IEC 27001-2011 Информационные технологии. Технологии безопасности. Системы управления защитой информации. Требования

Стандарты Республики Беларусь

- СТБ 34.101.1-2004 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
- СТБ 34.101.2-2004 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
- СТБ 34.101.3-2004 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3: Гарантийные требования безопасности.

Стандарты Республики Беларусь

- СТБ 34.101.8-2006 Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования.
- СТБ 34.101.9-2004 Информационные технологии. Требования к защите информации от несанкционированного доступа, устанавливаемые в техническом задании на создание автоматизированной системы.
- СТБ 34.101.10-2004 Информационные технологии. Средства защиты информации от несанкционированного доступа в автоматизированных системах. Общие требования.
- СТБ 34.101.11-2009 Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Профиль защиты операционной системы сервера для использования в доверенной зоне корпоративной сети.
- СТБ 34.101.12-2007 Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Оценка качества.
- СТБ 34.101.13-2009 Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Профиль защиты операционной системы сервера для использования в демилитаризованной зоне корпоративной сети.

Стандарты Республики Беларусь

- СТБ 34.101.14-2009 Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Профиль защиты программных средств маршрутизатора для использования в демилитаризованной зоне корпоративной сети.
- СТБ 34.101.15-2007 Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Типовая программа и методика испытаний.
- СТБ 34.101.16-2009 Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Профиль защиты программных средств коммутатора для использования в доверенной зоне корпоративной сети.
- СТБ 34.101.17-2009 «Информационные технологии. Синтаксис запроса на получение сертификата»;
- СТБ 34.101.18-2009 «Информационные технологии. Синтаксис обмена персональной информацией»;
- СТБ 34.101.19-2009 «Информационные технологии. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»;
- СТБ 34.101.20-2009 «Информационные технологии. Синтаксис криптографической информации для токенов»;
- СТБ 34.101.21-2009 «Информационные технологии. Интерфейс обмена информацией с аппаратно-программным носителем криптографической информации (токеном)»;
- СТБ 34.101.22-2009 Информационные технологии. Криптография на основе алгоритма RSA;

Стандарты Республики Беларусь

- СТБ П 34.101.31-2007 Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности
- СТБ П 34.101.35-2009 Информационные технологии. Методы и средства безопасности. Объекты информатизации. Профиль защиты класса Б3.
- СТБ П 34.101.36-2009 Информационные технологии. Методы и средства безопасности. Объекты информатизации. Профиль защиты класса А2.
- СТБ П 34.101.37-2009 Информационные технологии. Методы и средства безопасности. Объекты информатизации. Профиль защиты программных средств системы управления сайта.
- СТБ П 34.101.38-2009 Информационные технологии и безопасность. Классификация объектов информационных технологий по требованиям информационной безопасности
- СТБ П 34.101.39-2009 Информационные технологии и безопасность. Специальное программное обеспечение. Требования и методы испытаний
- СТБ П 34.101.40-2009 Информационные технологии. Методы и средства безопасности. Методика оценки показателей защищенности и надежности специального программного обеспечения
- СТБ П 34.101.41-2009 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения
- СТБ П 34.101.42-2009 Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Аудит информационной безопасности
- СТБ 34.101.43-2010 Информационная технология. Методы и средства безопасности. Профиль защиты аппаратно-программных устройств криптографической защиты информации.

Стандарты Республики Беларусь

- РД РБ 07040.1201-2003 «Банковские технологии. Средства электронной цифровой подписи программные. Общие требования».
- РД РБ 07040.1202-2003 «Банковские технологии. Процедуры выработки псевдослучайных данных с использованием секретного параметра».
- РД РБ 07040.1203-2004 Банковские технологии. Технология электронной цифровой подписи. Термины и определения.
- РД РБ 07040.1204-2004 Банковские технологии. Формат карточки открытого ключа.
- РД РБ 07040.1205-2004 Автоматизированные банковские системы. Система «Клиент-банк». Профиль защиты.
- РД РБ 07040.1206-2004 Банковские технологии. Формат сертификатов открытых ключей и списков отозванных сертификатов.

ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ ОБ ОЦЕНКЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ТЕХНИЧЕСКИХ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ В ОБЛАСТИ ТЕХНИЧЕСКОГО НОРМИРОВАНИЯ И СТАНДАРТИЗАЦИИ

Статья 6. Объекты оценки соответствия

Объектами оценки соответствия являются:

- продукция;
- процессы разработки, производства, эксплуатации (использования), хранения, перевозки, реализации и утилизации продукции;
- оказание услуг;
- система управления качеством;
- система управления окружающей средой;
- компетентность юридического лица в выполнении работ по подтверждению соответствия и (или) проведении испытаний продукции;
- профессиональная компетентность персонала в выполнении определенных работ, услуг;
- иные объекты, в отношении которых в соответствии с законодательством Республики Беларусь принято решение об оценке соответствия.

ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ ОБ ОЦЕНКЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ТЕХНИЧЕСКИХ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ В ОБЛАСТИ ТЕХНИЧЕСКОГО НОРМИРОВАНИЯ И СТАНДАРТИЗАЦИИ

Статья 8. Виды оценки соответствия

Оценка соответствия осуществляется в виде:

- аккредитации;
- подтверждения соответствия.

РАБОТЫ И УСЛУГИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ, В ТОМ ЧИСЛЕ КРИПТОГРАФИЧЕСКИМИ МЕТОДАМИ, ВКЛЮЧАЯ ПРИМЕНЕНИЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

- 13.1. разработка, производство, реализация, монтаж, наладка, сервисное обслуживание (либо выборка из указанного перечня работ) технических средств обработки информации в защищенном исполнении, программных средств обработки информации в защищенном исполнении, технических, программных, программно-аппаратных средств защиты информации и контроля ее защищенности, средств криптографической защиты информации (либо выборка из указанного перечня средств)
- 13.2. проведение испытаний, специальные исследования (либо выборка из указанного перечня работ) технических средств обработки информации, программных средств обработки информации, технических, программных, программно-аппаратных средств защиты информации и контроля ее защищенности, средств криптографической защиты информации (либо выборка из указанного перечня средств) по требованиям безопасности информации
- 13.3. проектирование, создание (либо выборка из указанного перечня работ) систем защиты информации на объектах информатизации
- 13.4. проектирование, создание (либо выборка из указанного перечня работ) систем защиты информации в информационных системах

РАБОТЫ И УСЛУГИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ, В ТОМ ЧИСЛЕ КРИПТОГРАФИЧЕСКИМИ МЕТОДАМИ, ВКЛЮЧАЯ ПРИМЕНЕНИЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

13.5. аттестация объектов информатизации

13.6. аттестация информационных систем

13.7. проведение работ по выявлению специальных технических средств, предназначенных для негласного получения информации

13.8. удостоверение формы внешнего представления электронного документа на бумажном носителе

13.9. оказание услуг по распространению открытых ключей проверки подписи

Указ Президента Республики Беларусь
О лицензировании отдельных видов деятельности
от 01.09.2010 №450

ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ ОБ ОЦЕНКЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ТЕХНИЧЕСКИХ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ В ОБЛАСТИ ТЕХНИЧЕСКОГО НОРМИРОВАНИЯ И СТАНДАРТИЗАЦИИ

Статья 9. Документы об оценке соответствия

К документам об оценке соответствия относятся:

аттестат аккредитации;

- сертификат соответствия;
- декларация о соответствии;
- сертификат компетентности.

Документы об оценке соответствия действуют на всей территории Республики Беларусь.

Статья 33. Права и обязанности аккредитованных испытательных лабораторий (центров)

Аккредитованные испытательные лаборатории (центры) имеют право:

- проводить в своей области аккредитации испытания продукции на соответствие требованиям технических нормативных правовых актов в области технического нормирования и стандартизации;

Оценка соответствия

- Оценка соответствия требованиям ТНПА
  - аккредитация,
  - подтверждение соответствия:
  - сертификация,
  - декларирование.
- Оценка ПЗ, ЗБ и ОО
- Аттестация объектов информатизации
- Аттестация информационных систем
- Государственная экспертиза
- Аудит

Виды оценки соответствия

Оценка соответствия осуществляется в виде:

- аккредитации;
- подтверждения соответствия.

Аккредитация

- **СТБ 50.01-2000**
- Система аккредитации Республики Беларусь. Основные положения

- **ТКП 50.13-2004 (04100)**
- Система аккредитации Республики Беларусь. Порядок аккредитации органов по сертификации персонала

- **ТКП 5.1.06-2004**
- Национальная система подтверждения соответствия Республики Беларусь. Порядок сертификации компетентности персонала. Основные положения

Оценка соответствия

К техническим нормативным правовым актам, на соответствие которым осуществляется оценка соответствия, относятся:

- технические регламенты,
- технические кодексы установившейся практики,
- государственные стандарты РБ,
- технические условия.

Формы подтверждения соответствия

Подтверждение соответствия может носить обязательный или добровольный характер.

Обязательное подтверждение соответствия осуществляется в формах:

- обязательной сертификации;
- декларирования соответствия.

Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации.

Обязательное подтверждение соответствия

- осуществляется в отношении объектов оценки соответствия, включенных в перечень продукции, услуг, персонала и иных объектов оценки соответствия, подлежащих обязательному подтверждению соответствия в Республике Беларусь.

Схемы подтверждения соответствия при декларировании соответствия

- устанавливаются соответствующим техническим регламентом, а в случае, если схемы подтверждения соответствия в нем не установлены либо технический регламент отсутствует, - техническим нормативным правовым актом в области технического нормирования и стандартизации, утвержденным Государственным комитетом по стандартизации Республики Беларусь.

При добровольной сертификации

- заявитель на подтверждение соответствия самостоятельно выбирает технические нормативные правовые акты, на соответствие которым осуществляется добровольная сертификация, и определяет номенклатуру показателей, контролируемых при добровольной сертификации объектов оценки соответствия.

При добровольной сертификации

- В номенклатуру этих показателей в обязательном порядке включаются показатели безопасности, если они установлены в технических нормативных правовых актах на данный объект оценки соответствия.

Документы об оценке соответствия

К документам об оценке соответствия относятся:

- аттестат аккредитации;
- сертификат соответствия;
- декларация о соответствии;
- сертификат компетентности.

ПОЛОЖЕНИЕ
О ПОРЯДКЕ АТТЕСТАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

- УТВЕРЖДЕНО
- Постановлением СМ РБ
- 26.05.2009 N 675

Положение о лицензировании отдельных видов деятельности
Перечень видов деятельности

- аттестация объектов информатизации
- аттестация информационных систем

- Указ Президента Республики Беларусь
- от 1 сентября 2010 г. N 450
- «О ЛИЦЕНЗИРОВАНИИ ОТДЕЛЬНЫХ ВИДОВ ДЕЯТЕЛЬНОСТИ»

аттестация

- - комплекс организационно-технических мероприятий, в результате которых подтверждается соответствие **системы защиты информации** требованиям нормативных правовых актов в области защиты информации, в том числе технических нормативных правовых актов, и оформляется аттестатом соответствия;

система защиты информации

- - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, функционирующих по правилам, установленным соответствующими нормативными правовыми актами в области защиты информации, в том числе техническими нормативными правовыми актами.

Аттестация предусматривает комплексную оценку системы защиты информации в реальных условиях эксплуатации информационной системы и включает проведение следующих мероприятий:

- анализ исходных данных по аттестуемой системе защиты информации;
- разработка программы аттестации;
- предварительное ознакомление с информационной системой и системой защиты информации;

- проведение обследования информационной системы и системы защиты информации;
- анализ разработанной документации по защите информации в информационной системе на соответствие требованиям нормативных правовых актов в области защиты информации, в том числе технических нормативных правовых актов;

- проведение испытаний средств защиты информации и оценка системы защиты информации в реальных условиях эксплуатации информационной системы;
- анализ результатов испытаний средств защиты информации, системы защиты информации и принятие решения о выдаче аттестата соответствия;
- выдача аттестата соответствия

Для проведения аттестации разрабатывается программа аттестации,

- которая должна содержать перечень работ и их продолжительность, методики испытаний, перечень используемой контрольной аппаратуры и тестовых средств, перечень привлекаемых аккредитованных испытательных лабораторий по требованиям безопасности информации.

Оценка системы защиты информации включает:

- анализ организационной структуры информационной системы, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения системы защиты информации, разработанной документации и ее соответствия требованиям нормативных правовых актов в области защиты информации, в том числе технических нормативных правовых актов;

Оценка системы защиты информации включает:

- проверку правильности отнесения информационной системы к классу типовых объектов информатизации, выбора и применения средств защиты информации;
- рассмотрение и анализ результатов испытаний средств защиты информации и системы защиты информации;

Оценка системы защиты информации включает:

- проверку уровня подготовки кадров и распределения ответственности персонала за организацию и обеспечение выполнения требований по защите информации;

Оценка системы защиты информации включает:

- оценку системы защиты информации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;
- оформление протоколов испытаний (оценки) и заключения по результатам проверок.

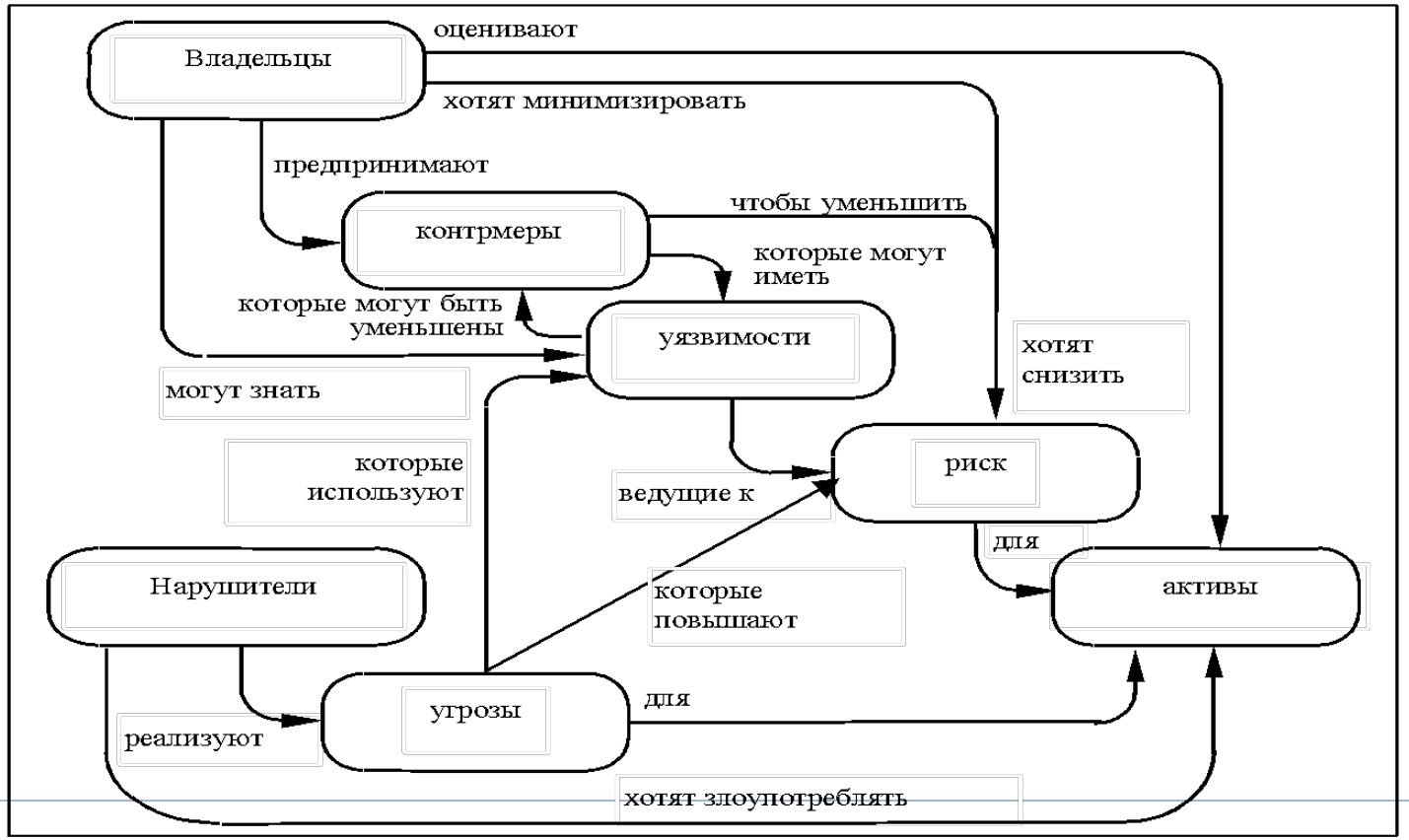
- Приложение

СТБ 34.101.1-2004

- 6 Общая модель
- 6.1 Содержание понятия безопасности
- 6.2 Модель разработки и оценки объекта
- 6.3 Концепции безопасности
- 6.3.1 Среда безопасности
- 6.3.2 Задачи безопасности
- 6.3.3 Требования безопасности информационных технологий
- 6.3.4 Общая спецификация объекта
- 6.3.5 Реализация объекта
- 6.4 Описательные возможности Общих критериев
- 6.4.1 Представление требований безопасности
- 6.4.2 Правила записи требований безопасности
- 6.4.3 Источники требований безопасности
- 6.5 Объекты оценки
- 6.6 Поддержка гарантии безопасности объекта

СТБ 34.101.1-2004

- **Концептуальные понятия безопасности и их взаимосвязь**



СТБ 34.101.1-2004

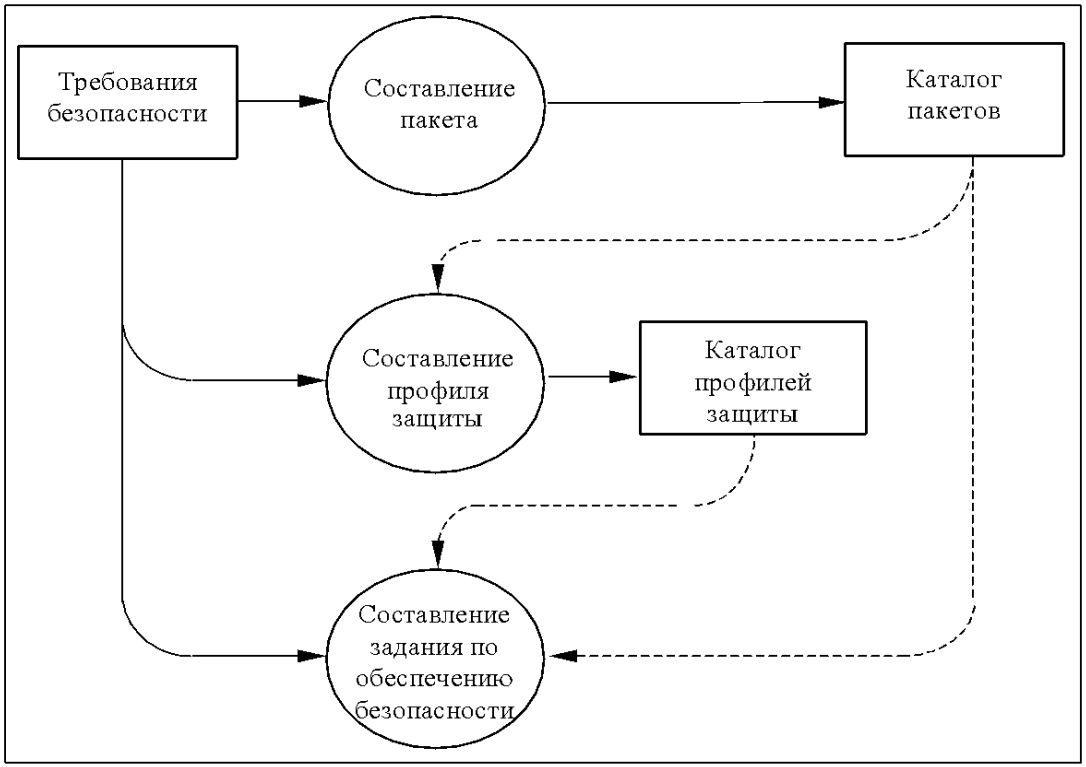
- **Профиль защиты** содержит совокупность требований безопасности для типового объекта информационных технологий. Эти требования выбираются из СТБ 34.101.2 и СТБ 34.101.3 или определяются разработчиком ПЗ самостоятельно. Эта совокупность требований включает УГО, который может быть усилен дополнительными гарантийными компонентами. ПЗ позволяет формулировать требования безопасности для объекта, которые полностью согласуются с совокупностью задач безопасности.
- ПЗ является документом многократного использования и определяет функциональные и гарантийные требования безопасности для типового объекта ИТ. Эти требования необходимы и эффективны при решении задач безопасности. ПЗ содержит также обоснования задач и требований безопасности.
- ПЗ могут разрабатываться заказчиками, разработчиками, пользователями продуктов или систем ИТ или другими субъектами, заинтересованными в создании такого набора требований.

СТБ 34.101.1-2004

- **Задание по безопасности** содержит совокупность требований безопасности, которые могут быть взяты из ПЗ или непосредственно из перечня функциональных или гарантийных требований, представленных в СТБ 34.101.2 и СТБ 34.101. 3, а также могут быть заданы самостоятельно. ЗБ содержит требования безопасности для конкретной реализации объекта оценки. Эти требования по результатам оценки признаны необходимыми и эффективными для решения установленных задач безопасности.
- ЗБ содержит общую спецификацию объекта вместе с требованиями безопасности, задачами безопасности и их обоснованиями. ЗБ является основой для соглашения между заказчиками (потребителями), разработчиками и экспертами (испытателями) объекта относительно его безопасности.

СТБ 34.101.1-2004

- стандарт определяет три вида структур для записи требований безопасности



Среда безопасности объекта

Описание среды безопасности объекта должно содержать связанные с безопасностью характеристики среды, в которой будет использоваться объект, и предполагаемый способ эксплуатации объекта. Оно включает:

- а) **предположения**, которые должны содержать следующие связанные с безопасностью характеристики среды объекта:

  1) информацию о предполагаемом порядке использовании объекта, в том числе о прикладной области применения, предполагаемой стоимости активов и о возможных ограничениях на использование;

  2) информацию о среде, в которой будет использоваться объект, включая вопросы, связанные с КСБО, подбором персонала и внешними связями с другими объектами;

- б) **угрозы активам**, которые исходят из окружающей среды объекта и создают опасность для его работы и против которых требуется защита средствами объекта или его среды.

  Угрозы должны быть описаны в понятиях: **источник угроз (нарушитель), атака и актив**, который подвергается атакам; источники угроз – в понятиях: **квалификация, используемый ресурс и мотивация;** атаки – в понятиях: **методы атак, используемые уязвимые места и возможности для атаки.**

  Если задачи безопасности объекта выводятся только из политики безопасности организации и предположений, то структурный элемент "угрозы" в ЗБ можно опустить;

- в) **политику безопасности организации**, которая должна определять и при необходимости объяснять разделы политики безопасности или правила, которым должен соответствовать объект. Каждый раздел политики следует представлять в форме, позволяющей использовать ее для формулирования четких задач безопасности ИТ.

Если задачи безопасности объекта выводятся только из угроз и предположений, то структурный элемент "политика безопасности организации" в ЗБ можно опустить.

предположения

ПС.1 Безопасное изготовление

На всех этапах жизненного цикла процессы разработки, изготовления и испытаний изделия X осуществляют квалифицированные специалисты организации-производителя

ПС.2 Безопасный монтаж

Монтаж и наладку изделия X, контроль состояния и техническое обслуживание изделия X осуществляет квалифицированный персонал в строгом соответствии с установленными правилами и указаниями эксплуатационной документации

ПС.3 Безопасный ввод в эксплуатацию

В момент ввода в эксплуатацию изделие X находится в безопасном состоянии

ПС.4 Надежный оператор

Эксплуатация изделия X осуществляется специально подобранным и подготовленным, квалифицированным администратором и пользователем. Операторы законопослушны и не имеют намерений снизить безопасность изделия X.

ПС.5 Физическая защита

Обеспечивается физическая защита изделия X от доступа посторонних лиц в соответствии с требованиями Инструкцией по работе в сети. Помещения, в которых расположено изделие X, физически защищены от НСД и размещаются в пределах действия средств контроля физического доступа

ПС.6 Проверенное ПО

В изделие X устанавливается ПО, проверенное на наличие недекларированных возможностей (НДВ), отсутствие вредоносных программ и/или компьютерных вирусов и все компоненты изделия X инсталлируются и конфигурируются в соответствии с технической и эксплуатационной документацией

ПС.7 Контроль функционирования

Регулярно осуществляется регламентный и периодический контроль безопасного функционирования изделия X в том числе и посредством внутреннего тестирования. Все инциденты безопасности, связанные с функционированием изделия X и несоблюдением установленных требований регистрируются, своевременно анализируются и по результатам анализа принимаются управленческие решения.

угрозы

- УО.7Потеря конфиденциальности/целостности данных вследствие ошибки пользователя
- УО.8Уничтожение оборудования или данных по небрежности
- УО.9Неправильное использование изделия X
- УО.10Ошибки при администрировании изделия X
- УО.11Отключение электроэнергии
- УО.12Скачки напряжения / повышение напряжения / снижение напряжения
- УО.13Уязвимости и ошибки в стандартном программном обеспечении
- УО.14Ошибка (отказ) при доставке сообщения
- УО.15Отказ от факта получения или отправления сообщения
- УО.16Небезопасные криптографические алгоритмы
- УО.17Манипуляции с данными или с программным обеспечением
- УО.18Манипуляции с линиями связи
- УО.19Неавторизованное использование изделия X
- УО.20Угроза использования уязвимостей внутренним штатом во время обслуживания / администрирования

ПБ.1 Целевое использование

- Изделие X используется операторами только для совершения санкционированных действий с использованием возможностей изделия X в рамках установленных для соответствующей роли полномочий и в соответствии с ЭД на изделие X

ПБ.2 Администратор

В организации в качестве администратора изделия X назначается квалифицированное лицо, в компетенцию которого входит обеспечение обслуживания и эксплуатации изделия X, организация и проведение мероприятий по обеспечению безопасности активов изделия X

ПБ.3 Учет активов

Все активы изделия X учитываются и контролируются. Не допускается несанкционированное изменение состава и конфигурации оборудования изделия X, системного и прикладного ПО

Задачи безопасности

- Задачи безопасности должны отражать намерение противостоять всем установленным угрозам и/или поддерживать принятую политику безопасности и предположения. Различают следующие типы задач безопасности:
- а) **задачи безопасности для объекта**, которые должны быть четко сформулированы для того, чтобы их решение позволило противостоять угрозам средствами безопасности объекта и/или поддерживать политику безопасности организации, которой должен следовать объект;
- б) **задачи безопасности для среды**, которые должны быть четко сформулированы для того, чтобы их решение позволило противостоять угрозам средствами безопасности объекта и среды и/или поддерживать политику безопасности организации, которой должен следовать объект. Формулировки задач безопасности для среды могут повторять (частично или полностью) предположения в описании среды безопасности объекта.

задачи

ЗО.2 Управление

Изделие X должно управляться администратором АП и удаленно, в рамках установленных полномочий, администратором ЦПУ.

ЗО.3 Регистрация событий.

Сведения о произведенных действиях, запущенных процессах и других событиях могущих привести к переходу изделия X в потенциально небезопасное состояние должны регистрироваться в журналах аудита.

ЗО.4 Защита данных аудита

КСБ изделия X должен обеспечивать защиту журналов аудита от удаления, модификации и просмотра неавторизованным пользователем и возможность удобной работы с ними уполномоченному пользователю.

ЗО.5 Разграничение доступа

КСБ изделия X должен обеспечивать доступ пользователей к активам изделия X в соответствии с их ролями.

СТБ 34.101.1-2004

- Требования безопасности представляются в форме, отражающей иерархию понятий: **класс-семейство-компонент-элемент**. Такая форма представления поможет заказчику (потребителю) правильно выбрать собственные требования безопасности.
- Как функциональные, так и гарантийные требования имеют общую форму представления и единую иерархию понятий.
- Понятие **класс** используется для формулирования наиболее общей группы требований безопасности, объединенных общими задачами безопасности.
- Членами класса являются семейства. Все члены класса имеют общую область применения, но различаются по задачам безопасности.
- Понятие **семейство** используется для обозначения совокупности требований безопасности, относящихся к одинаковым задачам безопасности, но различающихся детализацией или строгостью формулировок.
- Членами семейства являются компоненты.
- Понятие **компонент** используется для обозначения наименьшей совокупности требований безопасности, которую можно включить в ПЗ, ЗБ или в пакет. В большинстве случаев совокупности компонентов, входящих в семейство, упорядочены по усилению требований безопасности, объединенных общей задачей безопасности. Они также частично упорядочены в виде иерархических совокупностей. В тех случаях, когда семейство состоит из одного компонента, упорядочение не применяется.
- Членами компонента являются элементы.
- Понятие **элемент** используется для обозначения неделимого требования безопасности, которое можно проверить в процессе оценки. Уровень элемента – самый низкий уровень представления требований.

СТБ 34.101.1-2004

- Разрешенными являются следующие четыре операции:
- а) **итерация** позволяет многократно использовать компонент в различных операциях;
- б) **назначение** позволяет устанавливать определенный параметр элемента в компоненте требований безопасности;
- в) **выбор** позволяет выделить один или несколько элементов из перечня требований в компоненте;
- г) **уточнение** позволяет более детально описать компонент.

СТБ 34.101.2-2004

- Функциональные требования

СТБ 34.101.2-2004

Семейство FAU_GEN "Формирование данных аудита безопасности"

Компонент FAU_GEN.1 "Формирование данных аудита"

Иерархичен к: нет других компонентов

FAU_GEN.1.1 КСБО должен генерировать запись аудита следующих событий:

– запуск и отключение средств аудита;

– всех подлежащих аудиту событий для [выбор: *минимального, основного, детального, неопределенного*] уровня аудита;

– [назначение: *другие специально определенные события, подлежащие аудиту*].

FAU_GEN.1.2 Записи аудита КСБО должны содержать следующую информацию:

а) дату и время события, тип события, идентификатор субъекта и результат (успех или неудача) события;

б) для каждого типа событий, подлежащих аудиту, из числа определенных в функциональных компонентах, которые включены в ПЗ/ЗБ [назначение: *другая связанная с аудитом информация*].

Зависимости: **FPT_STM.1 "Надежные метки времени"**

СТБ П ИСО/МЭК 17799

- **Информационные технологии и безопасность**
- **ПРАВИЛА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ**
- **БЕЗОПАСНОСТЬЮ**

- **СТБ ISO/IEC 27001-2011** Информационные технологии. Технологии безопасности. СИСТЕМЫ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ. Требования.

  - ISO/IEC 27001:2005 Information technology. - Security techniques. Information security management systems. Requirements.

Система управления защитой информации

- **Общие требования**
  - **Учреждение и реализация СУЗИ**
    - **Учреждение СУЗИ**
    - **Реализация и управление СУЗИ**
    - **Мониторинг и пересмотр СУЗИ**
    - **Поддержание и совершенствование СУЗИ**
  - **Требования к документации**
    - **Общие положения**
    - **Контроль над документацией**
    - **Средства контроля записей**
- **Ответственность руководства**
  - **Обязательства руководства**
  - **Управление ресурсами**
    - **Предоставление ресурсов**
    - **Обучение, осведомленность и компетентность**
- **Внутренний контроль СУЗИ**
- **Административный контроль СУЗИ**
  - **Общие положения**
  - **Проведение контроля**
  - **Результат контроля**
- **Совершенствование СУЗИ**
  - **Постоянное совершенствование**

Учреждение и реализация СУЗИ

Учреждение СУЗИ

Организация должна выполнить следующее:

a) определить область действия и границы СУЗИ в рамках характеристик деятельности, организации, ее местоположения, активов и технологии с включением деталей и обоснований любых исключений из области действия (см. 1.2);

b) определить политику применения СУЗИ в рамках характеристик деятельности организации, ее местоположения, активов и технологии, которая:

1) включает структуру для постановки целей и устанавливает общий смысл направления и принципов для деятельности в отношении информационной безопасности;

2) принимает в расчет управленческие, правовые или распорядительные требования и контрактные обязательства по обеспечению безопасности;

3) присоединяется к контексту стратегического управления риском организации, в котором проходит учреждение и реализация СУЗИ;

4) устанавливает критерии, по которым оценивается риск (см. 4.2.1c);

5) утверждена руководством.

c) определить подход организации к оценке риска:

1) установить методику оценки риска, которая подходит для СУЗИ, установленной деловой информационной безопасности, правовых и распорядительных требований;

2) разработать критерии для принятия риска и установить приемлемые уровни риска (см. 5.1, перечисление f).

Выбранная методика оценки риска гарантирует, что оценки риска приносят сопоставимые и воспроизводимые результаты.

d) идентифицировать риски:

идентифицировать активы в рамках СУЗИ и касательно владельцев данных активов;

идентифицировать угрозы для данных активов;

идентифицировать слабые места в системе защиты, которые могут быть использованы при угрозах;

идентифицировать воздействия, к которым может привести потеря конфиденциальности, целостности и доступности активов;

e) анализировать и оценивать риски:

оценить воздействие на организацию, которое может стать результатом сбоев в безопасности, принимая во внимание последствия потери конфиденциальности, целостности или доступности активов;

оценить реальную вероятность сбоев безопасности, случающихся в связи с преобладающими угрозами и слабыми местами в системе защиты, воздействия, связанного с данными активами и используемыми системами контроля;

установить уровни риска;

определить, приемлемы ли риски или они требуют принятия мер с использованием критериев принятия рисков, установленных в 4.2.1, перечисление c)2).

f) установить и оценить возможные варианты обработки рисков.

Возможные действия включают:

1) применение соответствующих средств контроля;

2) сознательное и объективное принятие рисков при условии, что они четко удовлетворяют политикам организации и критериям принятия рисков (см. 4.2.1, перечисление c)2);

3) избегание рисков;

4) передачу сопутствующих деловых рисков другим сторонам, например страховым компаниям, поставщикам.

g) Выбрать цели и средства контроля для обработки рисков.

Цели и средства контроля выбираются и реализуются для удовлетворения требований, установленных оценкой и процессом обработки риска. При данном выборе принимают во внимание критерии принятия риска, а также распорядительные, законодательные и контрактные требования.

Цели и средства контроля, перечисленные в приложении А, выбираются как часть данного процесса в качестве подходящих для удовлетворения установленных требований.

Цели и средства контроля, перечисленные в приложении А, не являются исчерпывающими. Могут выбираться дополнительные цели и средства контроля.

Примечание - В приложении А содержится полный список цепей и средств контроля, которые в большинстве случаев были определены как существенные для организаций. Пользователи настоящего предстандарта должны обращаться к приложению А как к отправной точке для выбора способа контроля и гарантирования того, что никакие основные варианты контроля не упущены.

h) получить одобрение руководства по предложенным остаточным рискам.

i) получить санкцию руководства на реализацию и управление СУЗИ.

j) подготовить заявление о применимости.

Заявление о применимости должно включать следующее:

1) выбранные в соответствии с 4.2.1 (перечисление g) цели и средства контроля и причины их
выбора;

2) реализуемые (см. 4.2.1, перечисление e)2) в настоящее время цели и средства контроля;

3) исключение каких-либо целей и средств контроля по приложению А и обоснование их исключения.

Ответственность руководства

Обязательства руководства

Руководство обеспечивает подтверждение своих обязательств по учреждению, реализации, управлению, мониторингу, пересмотру, поддержанию и усовершенствованию СУЗИ посредством:

- учреждения политики применения СУЗИ;
- гарантирования того, что цели и планы СУЗИ установлены;
- назначение ролей и ответственности за информационную безопасность;
- сообщения организации важности удовлетворения целей информационной безопасности и соответствия политике применения информационной безопасности, ее ответственности перед законом и необходимости постоянного совершенствования;
- предоставления достаточных ресурсов для учреждения, осуществления, управления, мониторинга, пересмотра, поддержания и совершенствования СУЗИ (см. 5.2.1);
- выбора критериев принятия риска и приемлемых уровней риска;
- гарантирования проведения внутренних проверок СУЗИ (см. раздел 6); проведения административных пересмотров СУЗИ (см. раздел 7).

Управление ресурсами

Предоставление ресурсов

Организация должна установить и обеспечить ресурсы, необходимые для:

- учреждения, осуществления, управления, мониторинга, пересмотра, поддержания и совершенствования СУЗИ;
- гарантирования того, что процедуры информационной безопасности соответствуют требованиям деятельности;
- установления и обращения к юридическим и распорядительным требованиям и контрактным обязательствам по обеспечению безопасности;
- поддержания соответствующей безопасности за счет надлежащего применения всех реализуемых средств контроля;
- проведения при необходимости проверок и соответствующего реагирования на результаты данных проверок;
- усовершенствования при необходимости эффективности СУЗИ.

Обучение, осведомленность и компетентность

Организация гарантирует, что весь персонал, который наделен ответственностью, определенной в СУЗИ, компетентен в выполнении требуемых задач с помощью:

- определения необходимых знаний у персонала для эффективной работы с СУЗИ;
- обеспечения обучения или принятия других мер (например, принятия на работу компетентного персонала) для удовлетворения этих нужд;
- оценки эффективности принятых мер;
- поддержания учета образования, тренировки, навыков, опыта и квалификаций (см. 4.3.3).

Организация должна также гарантировать, что весь соответствующий персонал сознает значимость своей деятельности по обеспечению информационной безопасности и то, какой вклад они вносят в достижение целей СУЗИ.

4.3.3 Средства контроля записей

Control of records

- Для обеспечения подтверждения соответствия требованиям и эффективной работы СУЗИ должны быть произведены и реализованы записи, которые защищаются и контролируются. СУЗИ принимает во внимание любые соответствующие юридические и распорядительные требования и контрактные обязательства. Записи должны оставаться удобочитаемыми, легко идентифицируемыми и восстановимыми. Элементы управления, необходимые для идентификации, хранения, защиты, восстановления, максимального времени хранения и ликвидации записей, документально подтверждаются и приводятся в исполнение.
- Записи защищены от действий процессов, указанных в 4.2, и всех случаев значимых инцидентов нарушения безопасности, относящихся к СУЗИ.
- *Пример - Примерами записей являются книга посетителей, отчеты проверки, санкции на полный доступ.*

ISO/IEC TR 19791-2006

- Основная цель проекта 19791 — расширить международный стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий" (Evaluation Criteria for IT Security), чтобы сделать возможной оценку безопасности **систем, находящихся в производственной эксплуатации**. Подобное расширение необходимо, поскольку стандарт ISO/IEC 15408 в его нынешнем виде хотя и позволяет специфицировать программно-техническую функциональность безопасности как для продуктов, так и для систем информационных технологий (ИТ), но не охватывает ряд критически важных аспектов действующих, эксплуатируемых (автоматизированных) систем, точные спецификации которых необходимы для эффективного оценивания.
- 19791 содержит расширенные критерии оценки и рекомендации по оцениванию как программно-технических, так и административных и процедурных аспектов автоматизированных систем (АС). Применение комплексного подхода, охват мер всех уровней, направленных на обеспечение информационной безопасности, равно как и всех этапов жизненного цикла АС — еще одна цель проекта.

ISO/IEC TR 19791-2006

- 19791 содержит расширенные критерии оценки и рекомендации по оцениванию как программно-технических, так и административных и процедурных аспектов автоматизированных систем (АС). Применение комплексного подхода, охват мер всех уровней, направленных на обеспечение информационной безопасности, равно как и всех этапов жизненного цикла АС

ISO/IEC TR 19791-2006

- 19791 ориентирован не только на оценщиков, но и на разработчиков, системных интеграторов и эксплуатационников АС, поскольку эти специалисты должны понимать, что требуется для получения положительной оценки.

ISO/IEC TR 19791-2006

- **Развитие ОК идет по четырем основным направлениям**:
- ориентация на оценку действующих автоматизированных систем;
- реализация комплексного подхода к информационной безопасности, охват мер административного и процедурного уровней;
- охват всех этапов жизненного цикла автоматизированных систем;
- декомпозиция сложных систем на домены безопасности.

ISO/IEC TR 19791-2006

- Международный стандарт ISO/IEC 15408 ориентирован в первую очередь на оценку продуктов информационных технологий. Среда, в которой функционируют или должны функционировать подобные продукты, специфицируется в общем виде, в форме предположений о среде. Действующие автоматизированные системы окружены вполне определенной, конкретной средой, которую можно и нужно учитывать в процессе оценивания безопасности.

ISO/IEC TR 19791-2006

- Международный стандарт ISO/IEC 15408 ограничен рамками программно-технического уровня информационной безопасности. Для оценки продуктов информационных технологий этого, в принципе, достаточно; для систем, находящихся в производственной эксплуатации, — нет.
- В 19791 фигурируют функциональные требования и требования доверия к безопасности, относящиеся прежде всего к процедурному, а также к административному уровням информационной безопасности. Считается, что меры программно-технического уровня заимствуются из стандарта ISO/IEC 15408.

ISO/IEC TR 19791-2006

- В международном стандарте ISO/IEC 15408 объект оценки рассматривается как единое целое, с единым набором требований и единой оценкой. Для сложных автоматизированных систем это может оказаться неприемлемым. Целесообразно структурировать сложную систему на домены с разными рисками, требованиями и разной политикой безопасности, что и сделано в рассматриваемом проекте.

ISO/IEC TR 19791-2006

- Меры безопасности административного и процедурного уровней, включенные в 19791, в значительной степени заимствованы из международного стандарта 27001. Важное отличие, однако, состоит в том, что упомянутый стандарт ориентирован на разработчиков и эксплуатационщиков, а 19791 — в первую очередь на оценщиков. Соответственно, положения стандарта 27001 переформулированы так, чтобы служить критериями оценки безопасности.