Вопросы обеспечения соответствия разрабатываемых систем требованиям информационной безопасности

Валерий Козюминский, IBA

Software Engineering Forum

S·E·F

Вопросы обеспечения соответствия разрабатываемых систем требованиям информационной безопасности

Требования законодательства к защите информации в ИС

Требования ГОСТ к разработке АС

Требования ОК к оценке безопасности систем ИТ

Основные проблемы выполнения разработчиком требований безопасности

Практические рекомендации по выполнению требований информационной безопасности при создании ИС

Требования законодательства по защите информации

ЗАКОН Республики Беларусь от 10.11.2008 г. № 455-з «**Об информации, информатизации и защите информации**»

ПОЛОЖЕНИЕ о порядке защиты информации в государственных информационных системах (Проект постановления Совета Министров Республики Беларусь)

ПОЛОЖЕНИЕ о порядке аттестации систем защиты информации государственных информационных систем (Проект постановления Совета Министров Республики Беларусь)

ПОЛОЖЕНИЕ о порядке проведения государственной экспертизы средств защиты информации(Проект постановления Совета Министров Республики Беларусь)

ЗАКОН Республики Беларусь «Об электронном документе»

Требования законодательства по защите информации

Из ст. 28 ЗАКОНА Республики Беларусь от 10.11.2008 г. № 455-з «**Об информации, информатизации и защите информации**»:

- **Информация**, распространение и (или) предоставление которой ограничено, а также информация, содержащаяся в государственных информационных системах, должна обрабатываться в информационных системах с применением системы защиты информации**,** аттестованной в порядке, установленном Советом Министров Республики Беларусь.
- Не допускается эксплуатация государственных информационных систем без реализации мер по защите информации.

Software Engineering Forum
S·E·F

Требования законодательства по защите информации

Из проекта **ПОЛОЖЕНИЯ о порядке защиты информации в государственных информационных системах:**

- Защита информации в государственных информационных системах осуществляется путем создания систем защиты информации…
- Ответственность за организацию работ по защите информации возлагается на руководителей организаций, которые владеют и (или) пользуются информационными ресурсами информационной системы

Software Engineering Forum
S·E·F

Требования законодательства по защите информации

Из проекта **ПОЛОЖЕНИЯ о порядке защиты информации в государственных информационных системах**

Комплекс мероприятий по созданию СЗИ в ИС включает:

- классификацию хранящихся и обрабатываемых в ИС сведений;
- анализ структуры ИС, порядка организации вычислительных процессов и условий ее функционирования;
- присвоение информационной системе класса типового объекта информатизации;
- разработку или корректировку политики информационной безопасности;
- разработку или корректировку задания по безопасности на ИС;
- реализацию требований задания по безопасности в ИС;
- оценку соответствия системы защиты информации требованиям … путем проведения мероприятий по аттестации системы защиты информации;
- ввод ИС в эксплуатацию.

Software Engineering Forum
S·E·F

Требования законодательства по защите информации

Из проекта **ПОЛОЖЕНИЯ о порядке аттестации систем защиты информации государственных информационных систем**

Аттестация – комплекс организационно-технических мероприятий, в результате которых подтверждается соответствие системы защиты информации требованиям …, что подтверждается выдачей аттестата соответствия.

Аттестация предусматривает комплексную оценку системы защиты информации в реальных условиях эксплуатации ИС.

Software Engineering Forum

S·E·F

Требования ГОСТ к разработке АС

Стадия создания АС	Содержание
Формирование требований	**Обследование объекта автоматизации, формирование требований пользователя к АС**
Разработка концепции	**Изучение объекта, разработка концептуальных вариантов АС, выбор варианта концепции АС**
Техническое задание	**Разработка и утверждение ТЗ на АС**
Эскизный проект	**Разработка предварительных проектных решений на АС и ее части**
Технический проект	**Разработка проектных решений на АС и ее части. Разработка документации. Разработка требований на поставку изделий**
Рабочая документация	**Разработка рабочей документации на АС и ее части. Разработка ПО**
Ввод в действие	**Подготовка объекта к вводу АС в действие. Пусконаладочные работы. Предварительные испытания. Опытная эксплуатация. Приемочные испытания**
Сопровождение АС	

(Из ГОСТ 34.601-90)

Software Engineering Forum

S·E·F

Требования ГОСТ к разработке АС

Из **ГОСТ 34.602-89 Техническое задание на создание АС**

2.6.1 В подразделе «Требования к системе в целом» указывают:

….

- **требования безопасности**;

….

- **требования к защите информации от несанкционированного доступа**;
- **требования по защите информации от внешних аварий**;

….

Software Engineering Forum
S·E·F

Требования ОК к оценке безопасности систем ИТ

Базовые стандарты ОК

СТБ 34.101.1-2004 (ИСО/МЭК 15408.1-99)
Информационная технология. Методы и средства безопасности. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.
Часть 1. Введение и общая модель

СТБ 34.101.2-2004 (ИСО/МЭК 15408.2-99)
Часть 2. Функциональные требования безопасности

СТБ 34.101.3-2004 (ИСО/МЭК 15408.3-99)
Часть 3. Гарантийные требования безопасности

Common Criteria

ISO

Software Engineering Forum
S·E·F

Требования ОК к оценке безопасности систем ИТ

Из **СТБ 34.101.3-2004 (ИСО/МЭК 15408.3-99)**

Уровни гарантии оценки:

Базовый уровень доверия	**УГО1**	**Функционально тестированный**
Невысокий-умеренный уровень доверия	**УГО2**	**Структурно тестированный**
Умеренный уровень доверия	**УГО3**	**Методически тестированный и проверенный**
Умеренный- высокий уровень доверия	**УГО4**	**Методически спроектированный, тестированный и пересмотренный**
	УГО5	
	УГО6	
	УГО7	

Software Engineering Forum
S·E·F

Требования ОК к оценке безопасности систем ИТ

Из **СТБ 34.101.3-2004 (ИСО/МЭК 15408.3-99)**

Перечень представляемой документации для оценки ИС по УГО2

Класс ГТБ	Компонент ГТБ	**Документация для оценки**
ASE		**Задание по безопасности**
ACM	ACM_CAP.2	**Документация по управлению конфигурацией**
ADO	ADO_DEL.1 ADO_IGS.1	**Процедуры поставки** **Процедуры установки, генерации и запуска**
ADV	ADV_FSP.1 ADV_HLD.1 ADV_RCR.1	**Неформальная функц. спецификация** **Описательный проект верхнего уровня** **Неформальная демонстрация соответствия**
AGD	AGD_ADM.1 AGD_USR.1	**Руководство администратора** **Руководство пользователя**
ATE	ATE_COV.1 ATE_FUN.1 ATE_IND.2	**Доказательство покрытия** **ПМ и результаты функц. тестирования** **Протокол оценки**
AVA	AVA_SOF.1 AVA_VLA.1	**Оценка стойкости средств безопасности** **Отчет разработчика об анализе уязвимостей**

Software Engineering Forum
S·E·F

Требования ОК к оценке безопасности систем ИТ

Методические документы и стандарты ОК

СТБ П 34.101.5-2003 (CEM-97/017, CEM-99/008)
Информационные технологии и безопасность
ОБЩАЯ МЕТОДОЛОГИЯ ИСПЫТАНИЙ ПРОДУКТОВ И СИСТЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА СООТВЕТСТВИЕ УРОВНЯМ ГАРАНТИЙ

СТБ 34.101.6-2003 (ISO/IEC PDTR 15446, CEM-99/008)
Информационные технологии и безопасность
ЗАДАНИЕ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ
Разработка, обоснование, оценка

СТБ 34.101.7-2003 (ISO/IEC PDTR 15446, CEM-99/008)
Информационные технологии и безопасность
ПРОФИЛЬ ЗАЩИТЫ
Разработка, обоснование, оценка

Software Engineering Forum
S·E·F

Основные проблемы выполнения требований ИБ

Требования законодательства к защите информации в ИС

Разработка СЗИ:
Разработка ЗБ;
Оценка ЗБ;
Создание СЗИ ИС

Аттестация СЗИ:
Оценка док. СЗИ;
Оценка среды СЗИ;
Испытания СЗИ

Требования ГОСТ к разработке АС

Разработка ТЗ на ИС

Технический проект
Пояснительная записка к ТП

Рабочее Проектирование
Рабочая документация АС

Ввод в действие
Поставка и инсталляция
Предварительные испытания
Опытная эксплуатация
Приемочные испытания

Требования ОК к оценке безопасности систем ИТ

Разработка и оценка ЗБ

Оценка ИС по УГО2
Представление доказательств соответствия:
Управление конфигурацией
Процедуры поставки…
Описание архитектуры
Функц-ная спецификация
Руководящие документы
ПМ тестирования СЗИ
Результаты тестирования
Оценка документации
Независим. тестирование

Согласование процессов создания ИС и СЗИ

Согласование документации на ИС и СЗИ для соответствия ГОСТ и ОК

Вопросы согласования процессов создания ИС и СЗИ

Этапы создания СЗИ
(Проект постановления СМ)

1. Классификация информации
2. Анализ ИС как объекта защиты
3. Присвоение ИС категории
4. Разработка политики
5. Разработка ЗБ
6. Оценка ЗБ
7. Реализация требований ЗБ
8. Оценка СЗИ на соотв. треб. (аттестация)
9. Ввод ИС в эксплуатацию

Стадии создани ИС по ЕСКД

Разработка ТЗ на ИС

Технический проект
Пояснительная записка к ТП

Рабочее Проектирование
Рабочая документация АС

Ввод в действие
Поставка и инсталляция
Предварительные испытания
Опытная эксплуатация
Приемочные испытания

Требования ОК к ЗБ
(СТБ 34.101.6)

1. Общее описание ИС
2. Описание среды (предположений об условиях эксплуатации, активов, угроз)
3. Описание задач безопасности
4. Описание требований
5. Общая спецификация реализации ТБ
6. Обоснование

Согласно СТБ 34.101.1
разработка ЗБ осуществляется итерационно одновременно с созданием объекта

Оценка СЗИ по УГО СТБ 34.101.3

Варианты решения:
1) ТЗ - ЧТЗ - ЗБ 2) ПЗ – ЗБ 3) ЗБ (без ОС) – ЗБ ….

Software Engineering Forum
S·E·F

Вопросы согласования документации на ИС и СЗИ

Документация для аттестации СЗИ
(Проект постановления СМ)

1. **Перечень ОД ИС**
2. Оргструктура ИС
3. Политики ИБ
4. **Структура ПТК**
5. **Структура ПО**
6. **Ф. сх. ИС**
7. **Структура СЗИ**
8. **ЗБ**
9. Сертификаты СБ
10. **Проектная и эксп. Документация СЗИ**
11. Оргструктура ИБ
12. Инструкции по ИБ
13. **ПМ испытаний СЗИ**
14. **Протоколы испытаний СЗИ**
15. **Протокол оценки ЗБ**

Стадии создания ИС по ГОСТ

Разработка ТЗ на ИС

Технический проект
Пояснительная записка к ТП

Рабочее Проектирование
Рабочая документация АС

Ввод в действие
Поставка и инсталляция
Предварительные испытания
Опытная эксплуатация
Приемочные испытания

Требования ОК к СЗИ
(СТБ 34.101.3 для УГО2)

1. ЗБ
2. Управление конфигурацией
3. Процедуры поставки, установки, генерации и запуска
4. Функц. спецификация
5. Описание архитектуры СЗИ
6. Руковдства (админ. И пользователя)
7. ПМ тестирования СЗИ, результаты тестирования
8. Анализ уязвимостей

Варианты подготовки документации СИБ:
1) в соотв с. ОК 2) в соотв с. ЕСКД 3) Совмещение док. ЕСКД и ОК

Software Engineering Forum

S·E·F

СПАСИБО ЗА ВНИМАНИЕ

?????? Вопросы?????

E-mail: vkazjuminski@iba.by