**СМ 4/5 КСЗ (рестарт)**

Используемые сокращения:

* АС – автоматизированная система
* ГИС – государственная информационная система
* ИСПДн – информационная система персональных данных
* КСЗ – комплекс средств защиты
* НДВ – недекларированные возможности
* НПА – нормативно-правовой акт
* ПДн – персональные данные
* ПО – программное обеспечение
* ПОит – ПО, разрабатываемое ИнтерТраст
* ПЭП – подсистема электронной подписи в СМ4/5
* РД – руководящий документ
* СВТ – средство вычислительной техники
* ФСБ – Федеральная служба безопасности
* ФСТЭК – Федеральная служба по техническому и экспортному контролю
* ЭП – электронная подпись

1. ПЭП.

Предлагаю руководствоваться «CM45-Информационное письмо по Локер.doc», но если возможно изучить следующие документы:

1. InterTrust\_CM4-210-(Архитектура подсистемы Локер Веб).doc
2. InterTrust\_CM4-220-(Спецификация подсистемы Локер Веб)\_luxoft.doc
3. Locker 4.0.X (для CM 4.0m6) Низкоуровневые сценарии работы 2012\_07\_16.doc
4. Locker4. Видение.doc
5. Локер 4. Конверт ЭЦП.doc

с целью

а). минимальная – учет в архитектуре серверной и клиентской части функций по подготовке подписываемой информации.

б). максимальная – проектирование архитектуры СМ 4/5 с учетом подписания информации и проверки электронной подписи на разных типах рабочих мест (подписываемая информация – совокупность полей и вложения (файлы)).

Ps. Скорее всего путь а)., б). для размышлений.

1. Управление доверием

Предлагается не рассматривать, так как идеолог данной темы (М. Кравченко).

1. Спецификация КСЗ (SRS)

Это документ в большей мере не закончен, в части проведения а). анализа с учетом других требований и б). анализа требований и определения места их реализации (скажем в АС или ПО, ИСПДн или ПО).

Появились новые факторы:

1. в виде принятых и готовящихся к принятию НПА:

а). в части требований к информационным системам персональных данных (приказ ФСТЭК № 21 от 18.2.2013 г. – вступил в силу 2.6.2013 г.);

б). в части требований к государственным информационным системам (ГИС) (приказ ФСТЭК № 17 от 12.2.2013 г. – на согласовании в Минюсте). Требования по защите информации относятся к ГИС, но в п. 6 данного приказа говорится, что их можно применять и не для ГИС. Зная ситуацию в гос. органах, эти требования будут использоваться для многих систем и не являющихся ГИС.

в). требования приказа № 17 (см. п. б.) не относятся к информационным системам высших органов власти и ФСБ.

г). введены в действие в действие профили защиты. Пока не разобрался в какой мере их требования могут затрагивать ПО (обеспечить совместимость и т.д.).

2. ожидается информационное письмо ФСТЭК, суть которого, заключается в том, что сертификация по требованиям безопасности будет проводится строго по требованиям национальных стандартов и методических документов (руководящих документов). Технические условия не должны трактовать национальные стандарты и методические документы.

Ps. Наши конкуренты Директум уже испытала это в хоте сертификации 20-ти экземпляров своего ПО. Получили только соответствие по НДВ 4 уровня. По НСД как СВТ по 5 классу – забраковали (очитка памяти и т.д.).

3. Не понятен статус существующих РД для СВТ и АС.

Ссылка из новых документов (приказ 21 и 17) на них есть, что необходимо использовать СВТ не ниже 5 класса.

*РД понимает под СВТ совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем. Показатели защищенности СВТ применяются к* ***общесистемным программным средствам и операционным системам*** *(с учетом архитектуры ЭВМ).*

Выводы

1. ЭП заниматься надо
2. Разработка ПО с учетом требований РД по НДВ 4 уровня. Чтобы можно было пройти испытания и получить сертификат соответствия (Требования Приложение № 1 – что должно быть указано в п.3.2.1 данного приложения).
3. Провести анализ требований для реализации в рамках создания ИСПДн и при необходимости прохождения аттестации (нужен перечень ПО, используемого при создании системы[[1]](#footnote-2) с использованием СМ 4/5).
4. Взять за основу требования приказа ФСТЭК № 21 от 18.2.2013 г. (??? ФСТЭК № 17 от 12.2.2013 г.)
5. В ходе совещания обсудить реализуемость мер по обеспечению безопасности ПДн (по критериям – ПОит, ПО?, ИСПДн). Для этого необходим перечень ПО, используемый при создании СМ 4/5).
6. Привлечение аналитика предмет обсуждения на совещании.

Приложение № 1

**3.2. ТРЕБОВАНИЯ К ЧЕТВЕРТОМУ УРОВНЮ КОНТРОЛЯ**

**3.2.1.Контроль состава и содержания документации**

В состав документации, представляемой заявителем, должны входить:

* Спецификация (ГОСТ 19.202-78), содержащая сведения о составе ПО и документации на него;
* Описание программы (ГОСТ 19.402-78), содержащее основные сведения о составе (с указанием контрольных сумм файлов, входящих в состав ПО), логической структуре и среде функционирования ПО, а также описание методов, приемов и правил эксплуатации средств технологического оснащения при создании ПО;
* Описание применения (ГОСТ 19.502-78), содержащее сведения о назначении ПО, области применения, применяемых методах, классе решаемых задач, ограничениях при применении, минимальной конфигурации технических средств, среде функционирования и порядке работы.
* Исходные тексты программ (ГОСТ 19.401-78), входящих в состав ПО.

Для ПО импортного производства состав документации может отличаться от требуемого, однако содержание должно соответствовать требованиям указанных ГОСТ.

**3.2.2. Контроль исходного состояния ПО**

Контроль заключается в фиксации исходного состояния ПО и сравнении полученных результатов с приведенными в документации.

Результатами контроля исходного состояния ПО должны быть рассчитанные уникальные значения контрольных сумм загрузочных модулей и исходных текстов программ, входящих в состав ПО.

Контрольные суммы должны рассчитываться для каждого файла, входящего в состав ПО.

**3.2.3. Статический анализ исходных текстов программ**

Статический анализ исходных текстов программ должен включать следующие технологические операции:

- контроль полноты и отсутствия избыточности исходных текстов ПО на уровне файлов;

- контроль соответствия исходных текстов ПО его объектному (загрузочному) коду.

**3.2.4. Отчетность**

По окончании испытаний оформляется отчет (протокол), содержащий результаты:

- контроля исходного состояния ПО;

- контроля полноты и отсутствия избыточности исходных текстов контролируемого ПО на уровне файлов;

- контроля соответствия исходных текстов ПО его объектному (загрузочному) коду.

1. Надо понимать под системой ИСПДн, ГИС или АС. [↑](#footnote-ref-2)