**Защита от НСД к информации. Часть первая.**

**Программное обеспечение средств защиты информации.**

**Классификация по уровню контроля отсутствия не декларированных возможностей.**

1. Документ устанавливает классификацию программного обеспечения по уровню контроля отсутствия в нем не декларированных возможностей. Под не декларированными возможностями подразумевается возможность ПО, не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности информации.

Одной из возможной реализаций НВ является программные закладки - преднамеренно внесенные в ПО функциональные объекты, которые при определенных условиях инициируют выполнение не описанных в документации функций ПО, приводящие к нарушению конфиденциальности, целостности или доступности информации. Устанавливаются 4 уровня контроля, каждый из которых характеризуется совокупностью минимальных требования – они структурированы: 1) требования к документации, 2) требования к содержанию испытаний.

Испытания, проводимые в соответствии с данным документом, должны содержать проверки, которые относятся к 2 категориям – статическому и динамическому анализу. **Статический** представляет собой совокупность методов контроля, соответствия, реализованных и декларированных в документации функциональных возможностей ПО, основанных на структурном анализе и декомпозиции исходных текстовых программ. **Динамический** – это идентификация фактических маршрутов выполнения функциональных объектов с последующим сопоставлением маршрута, построенного в процессе проведения статического анализа. Оба метода дополняют друг друга.

2. ГОСТ-Р ИСО\МЭК 15408-2002. Информационные технологии. Методы и средства обеспечения информации. Критерии оценки безопасности ИТ. – общие критерии ( он государственный, утвержден, остальные – нет).

Одним из важнейших свойств – его универсальность. Документ состоит из 3 частей: 1 – введение и общая модель. 2 – функциональные требования безопасности, 3 – требования доверия к безопасности.

В стандарте приведены понятия: объекта оценки (оо), продукта и системы.

**ОО** – произвольный продукт ИТ или система с руководствами администратора и пользователя.

**ПРОДУКТ** – совокупность программных, программно-аппаратных или аппаратных средств ИТ, представляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в состав различных систем.

**СИСТЕМА** – специфическое воплощение ИТ с конкретными назначением и условиями эксплуатации. Определены категории пользователей – потребители, разработчики и эксперты. Объект оценки рассматривается с точки зрения среды безопасности – законодательная, административная, процедурная и программно-техническая.

При подготовке к оценке необходимо проанализировать 1) предположение безопасности, 2) угроза безопасности, 3) политика безопасности. Для достижения поставленных целей к ОО и его среде формулируются требования по безопасности. 2 и 3 часть общих критериев представляют собой каталоги требований безопасности двух видов: 1 – функциональные требования (ч2), 2 – требования доверия (ч3). При формулировании требований к объекту оценки предполагается разработка двух документов: 1 – профили защиты, 2 – задания по безопасности.

Недостатки общих критерием: 1 – отсутствие критериев оценки, касающихся администрирования безопасности, непосредственно не относящихся к мерам безопасности ИТ (управление персоналом в вопросах физической безопасности и ряд других мер), 2 – не затрагиваются механизмы контроля ПМИН – противодействие эл.магн излучениям и наводкам, 3 – не рассматривается методология оценки и административно-правовая структура, 4 – процедуры использования результатов оценки при аттестации продукта и систем в данном стандарте не рассматриваются, 5 – в стандарт не сходят критерии оценки специфических свойств криптографических алгоритмов.

3.СТРУКТУРА И СОДЕРЖАНИЕ ПРОФИЛЯ ЗАЩИТЫ. (на слайде)

Введение профиля защиты должно содержать информацию управления документооборотом и обзорную информацию, которая необходима для работы с реестром профиля защиты. 2 раздела. 1 – идентификация профиля защиты, которая должна обеспечить маркировку и описательную информацию, предназначенную для идентифицирования каталогизирования, регистрирования профиля защиты и ссылок на него. 2 – аннотация профиля защиты. Применяется для размещения в виду самостоятельного реферата в каталогах и реестрах профиля защиты. Изложение среды безопасности объекта оценки должно содержать описание аспектов безопасности среды, в которой предполагается использовать объект оценки, и ожидаемый способ его применения. В состав этого изложения входит: описание предположений (информация относительно предполагаемого использования объекта оценки и информация относительно среды применения объекта оценки), описание угроз, описание политики безопасности организации.

Цели безопасности для ОО – должны быть четко изложены и сопоставлены с аспектами установленных угроз, которым необходимо противостоять средствами ОО или с политикой безопасности организации.

Краткая спецификация ОО должна определить отображение требований безопасности для ОО. Данная спецификация представляет собой описание функций безопасности и мер доверия к ОО, которые отвечают требованиям безопасности ОО. В состав краткой спецификации входит: 1 – изложение функций безопасности, 2 – изложение мер доверия. Если сделано утверждение о соответствии 1 или нескольким профилям защиты, то изложение утверждений о соответствии должно содержать 1 – ссылка на профиль защиты, 2 – конкретизация ПЗ, 3 – дополнения ПЗ.

Логическое обоснование краткой спецификации ОО показывает, что функции безопасности и меры доверия к ОО пригодны для того, чтобы отвечать требованиям безопасности ОО.

4. ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ БЕЗОПАСНОСТИ.

Систематизированный каталог функциональных требований безопасности сосредоточен во 2ч общих критериях (этого стандарта). Функциональные требования разбиты на 11 классов, 66 семейств и 135 компонентов. Структура на слайде (отправят). Имя класса содержит информацию, которая необходима для идентификации функционального класса и отнесения его к определенной категории. Каждый ФК имеет уникальное имя. Информация о категории представлена кратким именем, которое состоит из 3 букв латинского алфавита. Представление класса содержит рисунок, который показывает все семейства этого класса и иерархию компонентов в каждом семействе (на слайде структура). Каждое функциональное семейство имеет уникальное имя. Первые 3 символа идентичны краткому имени класса ХХХ, далее \_ и краткое имя семейства YYY (ХХХ\_YYY).

Характеристика семейства – описание функционального семейства, в котором излагаются его цели безопасности и общее описание функциональных требований.

Цели безопасности семейства характеризуют задачу безопасности, которая должна быть решена с помощью ОО, который включает компонент из этого семейства.

Цель ранжирования компонентов – предоставить пользователям информацию для выбора подходящего функционального компонента из семейства.

Требования управления – содержится информация для разработчиков ПЗ и ЗБ (профиль защиты и задание по безопасности), которая учитывается при определении действий по управлению для данного компонента.

Требования аудита - содержат события, которые подвергаются аудиту. Выбираются требования из класса (аудит безопасности FAU). Запись аудита может включаться на разных уровнях детализации, которые характеризуются следующими терминами: минимальный, базовый и детализированный. Структура функционального компонента на слайде.