**Тема 3: "ОЦЕНОЧНЫЕ СТАНДАРТЫ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ"**

***3.1 Роль стандартов ИБ.***

Зачем нужны стандарты в области ИБ?

В общем случае стандартом принято называть документ, в котором устанавливаются требуемые характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт может задавать и другие требования – например, к символике или терминологии.

**Цель**: 1) обеспечение необходимого уровня *качества* продуктов, товаров и услуг;

2) обеспечения *единых характеристик* продуктов, товаров и услуг.

Причиной необходимости использования стандартов является то, что необходимость соблюдения некоторых из них закреплена законодательно. Реальные причины гораздо глубже – обычно стандарт является обобщением опыта лучших специалистов в той или иной области, и потому представляет собой надёжный источник оптимальных и проверенных решений.

Стандартизация в области ИБ необходима по трем основным причинам:

1) необходимость выработки **единых требований** по ИБ (единый набор требований);

2) необходимость выработки **единых подходов** к решению проблем ИБ;

3) необходимость выработки **единых качественных показателей для оценки безопасности** ИС и средств защиты.

Потребители (заказчики) продуктов информационных технологий бес стандартов не смогут сформулировать свои требования по ИБ производителям информационных систем (нужны какие-то критерии, показатели, единицы измерения ИБ и т.д.).

Производители продукции ИТ и средств защиты (программных, технических) нуждаются в стандартах для того, чтобы можно было бы объективно оценить свою продукцию с точки зрения обеспечения ИБ, то есть СЕРТИФИЦИРОВАТЬ ее. Им также необходим стандартный набор требований для того, чтобы ограничить фантазию заказчика и заставить выбирать конкретные требования из этого набора.

Стандарты нужны экспертам по ИБ и специалистам по сертификации как инструмент для оценки **уровня безопасности**, обеспечиваемого конкретными механизмами и средствами защиты информации (техническими, программными и т.д.) либо комплексами таких средств (КСЗИ).

В настоящее время существует довольно много стандартов, а также других нормативных и руководящих документов в области информационной безопасности. Все их рассмотреть в рамках данного курса не представляется возможным. Поэтому мы будем рассматривать **только базовые** стандарты в области информационной безопасности, которыми руководствуются при создании, сертификации и эксплуатации систем управления информационной безопасностью (СУИБ).

Эти стандарты можно разбить на две группы рис. 1

1 группа – оценочные стандарты. Они предназначены для оценки и классификации информационных систем и средств защиты информации по требованиям безопасности. Ими руководствуются для того, чтобы ответить на вопрос: *Соответствует ли ваша ИС и ваши механизмы и средства защиты требованиям безопасности?* К ним относятся:

1) стандарт «Критерии оценки доверенных компьютерных систем» или разговорное название «Оранжевая книга»;

2) международный стандарт ISO/IEC «Критерии оценки безопасности информационных технологий» или разговорное название «Общие критерии».

2 группа стандартов – это так называемые **спецификации**. Они регламентируют различные вопросы реализации и использования методов и средств защиты информации. Ими руководствуются для того, чтобы ответить на вопрос: *Как обеспечить информационную безопасность, какие подходы, какие методы и какие средства необходимо для этого использовать?* К этим стандартам относятся:

1) рекомендации Х.800, «Архитектура безопасности для взаимодействия открытых систем» - регламентирует методы и средства обеспечения ИБ в компьютерных сетях;

2) международный стандарт ISO/IEC «Практические правила управления информационной безопасностью», разработанный на основе одноименного британского стандарта BS 7799;

3) международный стандарт ISO/IEC 27001:2005 «Системы менеджмента информационной безопасности. Требования».

Далее мы рассмотрим более подробно названные стандарты.

***3.2 «Оранжевая книга» как оценочный стандарт.***

Стандарт «Критерии оценки доверенных компьютерных систем», более известный как «Оранжевая книга», был разработан Министерством обороны США в 1983 г. и стал первым в истории общедоступным оценочным стандартом в области информационной безопасности.

Требования «Оранжевой книги» имеют следующую структуру:

***1. Политика безопасности*** (совокупность управленческих решений по защите информации и ресурсов)

1.1. Система должна поддерживать точно определённую политику безопасности. Возможность доступа субъектов к объектам должна определяться на основании их идентификации и набора правил управления доступом. По мере необходимости должна использоваться политика мандатного управления доступом.

1.2. С объектами должны быть ассоциированы метки безопасности, используемые в качестве исходной информации для процедур контроля доступа. Для реализации мандатного управления доступом система должна обеспечивать каждому объекту набор атрибутов, определяющих степень конфиденциальности объекта и режимы доступа к этому объекту.

***2. Подотчётность***

2.1. Все субъекты должны имеет уникальные идентификаторы. Контроль доступа должен осуществляться на основе идентификации субъекта и объекта доступа, аутентификации и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и должны быть ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично сточки зрения безопасности.

2.2. Для определения степени ответственности пользователя за действия в системе, все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищённом протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность. Протокол событий должен быть надёжно защищен от несанкционированного доступа, модификации и уничтожения.

***3. Гарантии***

3.1. Средства защиты должны содержать независимые аппаратные или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, регистрацию и учёт, должны находиться под контролем средств, проверяющих корректность их функционирования. Средства контроля должны быть полностью независимы от средств защиты.

3.2. Все средства защиты должны быть защищены от несанкционированного вмешательства и отключения, причём эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и информационной системы в целом. Данное требование распространяется на весь жизненный цикл информационной системы.

Напомним, что «Оранжевая книга» является оценочным стандартом а значит, предназначена в первую очередь для проведения анализа защищенности информационных систем. По результатам такого анализа ИС должна быть отнесена к одному из определённых в документе классов защищённости. «Оранжевая книга» определяет четыре группы классов защищённости:

А – содержит единственный класс А1.

В – содержит классы В1, В2 и В3.

С – содержит классы С1 и С2.

D содержит единственный класс D1.

Требуемый уровень защищенности системы возрастает от группы D к группе А, а в пределах одной группы – с увеличением номера класса. Каждый класс характеризуется определённым фиксированным набором требований к подсистеме обеспечения информационной безопасности, реализованной в ИС.

Приведём краткие характеристики каждого из классов защищенности.

1. Группа D – минимальная защита.

К данной категории относятся те системы, которые были представлены для сертификации по требованиям одного из более высоких классов защищенности, но не прошли испытания.

2. Группа С – дискреционная защита.

Данная группа характеризуется наличием дискреционного управления доступом и регистрации действий субъектов.

- Класс С1 дискреционная защита.

Система включает в себя средства контроля и управления доступом, позволяющие задавать ограничения для отдельных пользователей. Класс С1 рассчитан на однопользовательские системы, в которых осуществляется совместная обработка данных одного уровня конфиденциальности.

- Класс С2 управление доступом.

Система обеспечивает более избирательное управление доступом путём применения средств индивидуального контроля за действиями пользователей, регистрации, учёта событий и выделения ресурсов.

3. Группа В – мандатная защита.

Система обеспечивает мандатное управление доступом с использованием меток безопасности, поддержку модели и политики безопасности. Предполагается наличие спецификаций на функции ядра безопасности. Реализуется концепция монитора безопасности обращений, контролирующего все события в системе.

- Класс В1 – защита с применением меток безопасности.

Помимо выполнения всех требований к классу С2, система должна поддерживать маркировку данных и мандатное управление доступом. При экспорте из системы информация должна подвергаться маркировке.

- Класс В2 структурированная защита.

Ядро безопасности должно поддерживать формально определенную и чётко документированную модель безопасности, предусматривающую дискреционное и мандатное управление доступом, которое распространяется на все субъекты. Должен осуществляться контроль скрытых каналов передачи информации. В структуре ядра безопасности должны быть выделены элементы, критичные с точки зрения безопасности. Интерфейс ядра безопасности должен быть чётко определён, а его архитектура и реализация должны быть выполнены с учётом возможности проведения тестовых испытаний. Управление безопасностью должно осуществляться администратором безопасности.

- Класс В3 домены безопасности.

Ядро безопасности должно поддерживать монитор безопасности обращений, который контролирует все типы доступа субъектов к объектам и который невозможно обойти. Ядро безопасности содержит исключительно подсистемы, отвечающие за реализацию функций защиты, и является достаточно компактным для обеспечения возможности эффективного тестирования. Средства аудита должны включать механизмы оповещения администратора о событиях, имеющих значение для безопасности системы. Необходимо наличие средств восстановления работоспособности системы.

4. Группа А – верифицированная защита.

Группа характеризуется применением формальных методов верификации корректности функционирования механизмов управления доступом. Требуется дополнительная документация, демонстрирующая, что архитектура и реализация ядра безопасности отвечает требованиям безопасности. Функциональные требования совпадают с классом В3, однако на всех этапах разработки ИС требуется применение формальных методов верификации систем защиты.

Разработка и публикация «Оранжевой книги» стали важнейшей вехой в становлении теории информационной безопасности. Такие базовые понятия, как «политика безопасности», «монитор безопасности обращений» или «администратор безопасности» впервые в открытой литературе появились именно в «Оранжевой книге».

В то же время с течением времени стали проявляться многочисленные недостатки «Оранжевой книги» и предложенного подхода к классификации ИС в целом. Во многом её устаревание было связано с принципиальными изменениями аппаратной базы средств вычислительной техники, произошедшими с 1983 г. – и прежде всего, с распространением распределённых вычислительных систем и сетей, особенности которых в «Оранжевой книге» никак не учитываются.

Стараясь не отстать от развивающихся информационных технологий, разработчики «Оранжевой книги» вплоть до 1995 г. выпустили целый ряд вспомогательных документов, известных как «Радужная серия». Эти документы содержали рекомендации по применению положений «Оранжевой книги» для различных категорий информационных систем, а также вводили ряд дополнительных требований. Наибольший интерес в «Радужной серии» представляют три документа: «Интерпретация для защищённых сетей», «Интерпретация для защищённых СУБД» и «Руководство по управлению паролями».

В настоящее время «Оранжевая книга» не используется для оценки информационных систем и представляет интерес исключительно с исторической точки зрения.

***3.3 Международный стандарт ISO/IEC Критерии оценки безопасности информационных систем.***

Как для «Оранжевой книги», так и для аналогичных ей руководящих документов, характерны многочисленные недостатки. Перечислим наиболее существенные из них:

- Документы ориентированы на обеспечение защиты информации от угроз нарушения конфиденциальности и, в определенной степени, целостности. Угрозы нарушения доступности практически не рассматриваются.

- Используемый «табличный» подход не позволяет учесть специфику конкретных систем или продуктов, в том числе порядок обработки информации в информационной системе.

- Документы содержат перечень механизмов, наличие которых необходимо для отнесения ИС к тому или иному классу защищенности. При этом совершенно не оговорены методы проверки корректности и адекватности реализации функциональных требований.

- Формулировки ряда требований чрезвычайно туманны и допускают неоднозначную интерпретацию.

В целом, «Оранжевая книга», как и все другие оценочные стандарты первого поколения, создавались для давно ушедшей в прошлое материально-технической базы и по целому ряду аспектов являются морально устаревшими.

Стандарт ISО/IЕС был разработан совместными усилиями специалистов Канады, США, Великобритании, Германии, Нидерландов и Франции в период с 1990 по 1999 год, развитие стандарта непрерывно продолжается. Исторически за стандартом закрепилось разговорное название «Общие критерии».

В России перевод «Общих критериев» версии 2.0 принят в качестве ГОСТа в 2002 году и введён в действие с 1 января 2004 г.

«Общие критерии» предназначены служить основой при оценке характеристик безопасности продуктов и систем ИТ. Заложенные в стандарте наборы требований позволяют сравнивать результаты независимых оценок безопасности. На основании этих результатов потребитель может принимать решение о том, ***достаточно ли безопасны ИТ-продукты или системы для их применения с заданным уровнем риска***.

Стандарт ГОСТ Р ИСО/МЭК состоит из трех частей.

В первой части (ГОСТ Р ИСО/МЭК «Введение и общая модель») устанавливается общий подход к формированию требований безопасности и оценке безопасности, на их основе разрабатываются основные конструкции (профиль защиты и задание по безопасности) представления требований безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ. Требования безопасности объекта оценки (ОО) по методологии «Общих критериев» определяются исходя из целей безопасности, которые основываются на анализе назначения ОО и условий среды его использования (угроз, предположений, политики безопасности).

Часть вторая (ГОСТ Р ИСО/МЭК «Функциональные требования безопасности») содержит универсальный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам.

Третья часть (ГОСТ Р ИСО/МЭК «Требования доверия к безопасности») включает в себя систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты **на всех этапах жизненного цикла продукта или системы ИТ** для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям. Здесь же содержатся оценочные уровни доверия (ОУД), определяющие шкалу требований, которые позволяют с возрастающей степенью полноты и строгости оценить проектную, тестовую и эксплуатационную документацию, правильность реализации функций безопасности ОО, уязвимости продукта или системы ИТ, стойкость механизмов защиты и сделать заключение об уровне доверия к безопасности объекта оценки.

Обобщая вышесказанное, можно отметить, что каркас безопасности, заложенный частью 1 стандарта ГОСТ Р ИСО/МЭК 15408, заполняется содержимым из классов, семейств и компонентов в части 2, а третья часть определяет, как оценить прочность всего «строения».

Стандарт «Общие критерии безопасности информационных технологий» отражает достижения последних лет в области информационной безопасности. Впервые документ такого уровня содержит разделы, адресованные потребителям, производителям и экспертам по оценке безопасности ИТ-продуктов.

В перспективе «Общие критерии» должны заменить руководящие документы во всех системах сертификации средств защиты информации. В настоящий момент в России «Общие критерии» используются одновременно с РД Гостехкомиссии, причём «Общие критерии» применяются исключительно при проведении сертификации продуктов, не предназначенных для обработки информации, составляющей государственную тайну.

**Основные идеи «Общих критериев»**

Основное свойство «Общих критериев» (ОК) – это максимально возможная универсальность: под объектом оценки (ОО) понимается произвольный продукт информационных технологий или система с руководствами администратора и пользователя.

**Продукт** рассматривается как совокупность программных, программно-аппаратных или аппаратных средств информационных технологий, предоставляющая определённые функциональные возможности и предназначенная для непосредственного использования или включения в состав различных систем.

В свою очередь, **система** – это специфическое воплощение информационных технологий с конкретным назначением и условиями эксплуатации.

Предполагается, что общие критерии могут быть использованы следующими категориями пользователей:

***1. Потребители***.

ОК позволяют определить, вполне ли оцениваемый продукт или система удовлетворяют нх потребностям в безопасности.

***2. Разработчики***

ОК могут быть использованы для формирования утверждения о соответствии объекта оценки установленным требованиям.

***З. Оценщики***

Стандарт может быть использован при формировании заключения о соответствии ОО предъявляемым к ним требованиям безопасности.

Объект оценки рассматривается в контексте среды безопасности, в которую включаются:

- ***законодательная среда*** – законы и нормативны акты, затрагивающие ОО;

- ***административная среда*** – положения политик безопасности, затрагивающих ОО и учитывающих его особенности;

- ***процедурная среда*** – меры физической защиты, персонал и его специфика;

- ***программно-техническая среда*** – назначение ОО, предполагаемые области его применения.

При подготовке к оценке формализуются следующие **аспекты среды ОО**:

***1. Предположения безопасности***

Предположения выделяют ОО из общего контекста и задают границы его рассмотрения. Предполагается, что среда ОО удовлетворяет данным предположениям. Иными словами предполагается, что объект оценки будет использоваться в нормальных условиях (а не в условиях боевых действий) и требования относительно среды безопасности соблюдены. При проведении оценки предположения безопасности принимаются без доказательств.

***2. Угрозы безопасности***

Выделяются угрозы, наличие которых в рассматриваемой среде установлено или предполагается. Угроза характеризуется следующими параметрами:

- источник угрозы;

- предполагаемый способ реализации угрозы;

- уязвимости, которые являются предпосылкой для реализации угрозы;

- активы, которые являются целью нападения;

- нарушаемые свойства безопасности активов;

- возможные последствия реализации угрозы.

***З. Политика безопасности***

Излагаются положения политики безопасности, применяемые в организации, которые имеют непосредственное отношение к ОО.

На основании сформулированных предположений безопасности, при учёте угроз и политик формулируются цели безопасности для ОО, направленные на обеспечение противостояния угрозам и выполнение положений политики безопасности.

Для достижения поставленных целей к ОО и его среде предъявляются требования безопасности.

Вторая и третья части «Общих критериев» представляют собой каталоги требований безопасности двух типов: функциональных и доверия.

- ***Функциональные требования безопасности*** (Часть 2) предъявляются к функциям безопасности ОО и реализующим их механизмам. Функциональные требования относятся к сервисам безопасности, таким как идентификация, аутентификация, управление доступом, аудит и т.д.

- ***Требования доверия*** (Часть 3) предъявляются к технологии разработки, тестированию, анализу уязвимостей, поставке, сопровождению, эксплуатационной документации и т.д.

Описание обоих типов требований выполнено в едином стиле: они организованы в иерархию "класс - семейство - компонент - элемент". Термин "класс" используется для наиболее общей группировки требований безопасности, а элемент - самый нижний, неделимый уровень требований безопасности.

При формулировании требований к ОО могут быть разработаны два документа:

***1. Профиль защиты*** – типовой набор требований для некоторой категории ОО. Профиль защиты определяется как "независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя".

Профиль защиты (ПЗ) не привязан к конкретному 00 и представляет собой обобщенный стандартный набор функциональных требований и требований доверия для определенного класса продуктов или систем. Например, может быть разработан профиль защиты на межсетевой экран корпоративного уровня, на операционную систему для правительственных организаций, и т.д.

***2. Задание по безопасности*** – документ, содержащий требования безопасности для конкретной разработки, выполнение которых обеспечивает достижение поставленных целей безопасности. В задании по безопасности (ЗБ) может быть заявлено соответствие одному или нескольким профилям защиты.

**ЗБ можно рассматривать как техническое задание на подсистему обеспечения информационной безопасности для ОО.**

Задание по безопасности служит основой для проведения оценки 00 с целью демонстрации соответствия его требованиям безопасности.

При проведении оценки изделия ИТ главными являются следующие вопросы:

1) отвечают ли функции безопасности ОО функциональным требованиям?

2) корректна ли реализация функций безопасности?

Если оба ответа положительны, можно говорить о достижении целей.