Информационная безопасность

Лекция 6 Жизненный цикл изделия и безопасность

В. М. Куприянов, Национальный центр ИНИС МАГАТЭ, НИЯУ МИФИ

НЦ ИНИС МИФИ

Литература

Основная литература для изучения дисциплины:

- Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности.- М.: Горячая линия – Телеком, 2006.
- Петраков А.В. Основы практической защиты информации.- М.: Радио и связь, 2001.
- Шумский А.А., Шелупанов А.А. Системный анализ в защите информации.- М.: Гелиос АРВ, 2005.
- Герасименко В.А., Малюк А.А. Основы защиты информации.- М.: Инкомбук, 1997.
- Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.- М.: Энергоатомиздат, 1994.
- Семкин С.Н., Семкин А.Н. Основы информационной безопасности объектов обработки информации.- Орел: ОВИПС, 2000.

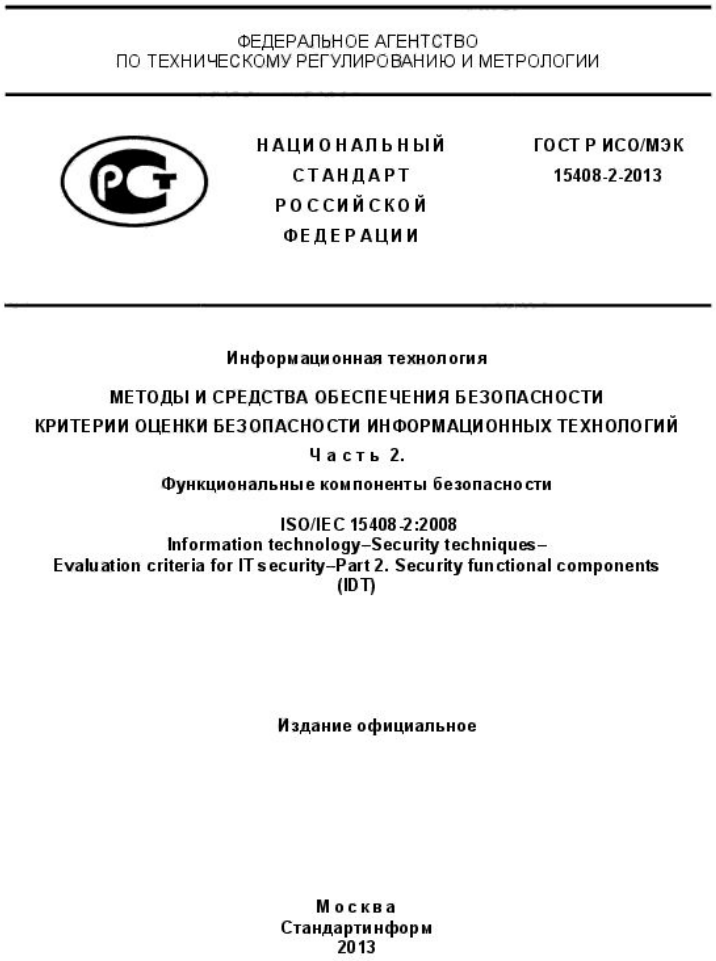
Требования безопасности к информационным системам

- Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий" (издан 1 декабря 1999 года) относится к оценочным стандартам. Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран. Он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба. Именно поэтому этот стандарт очень часто называют "Общими критериями".
- "Общие критерии" являются метастандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования.
- "Общие критерии" содержат два основных вида требований безопасности:
- **функциональные** – соответствуют активному аспекту защиты – предъявляемые к функциям безопасности и реализующим их механизмам;
- **требования доверия** – соответствуют пассивному аспекту – предъявляемые к технологии и процессу разработки и эксплуатации.
- В отличие от "Оранжевой книги", "Общие критерии" не содержат предопределенных "классов безопасности". Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.
- Очень важно, что безопасность в "Общих критериях" рассматривается не статично, а в привязке к жизненному циклу объекта оценки.

Жизненный цикл ПО

Основной стандарт

- Настоящий стандарт устанавливает структуру и содержание компонентов функциональных требований безопасности для оценки безопасности. Он также включает в себя каталог функциональных компонентов, отвечающих общим требованиям к функциональным возможностям безопасности многих продуктов ИТ



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15408-2-2013

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 2.

Функциональные компоненты безопасности

ISO/IEC 15408-2:2008
Information technology–Security techniques–
Evaluation criteria for IT security–Part 2. Security functional components
(IDT)

Издание официальное

Москва
Стандартинформ
2013

Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

- **Основные понятия**
- Самый полный и современный среди них Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба.
- По историческим причинам данный стандарт часто называют "*Общими критериями*" (или даже ОК). Мы также будем использовать это сокращение.
- **"Общие критерии"** на самом деле являются метастандартом, определяющим инструменты *оценки безопасности* ИС и порядок их использования. В отличие от "*Оранжевой книги*", ОК не содержат предопределенных *"классов безопасности"*. Такие классы можно строить, исходя из **требований безопасности**, существующих для конкретной организации и/или конкретной информационной системы.
- С программистской точки зрения ОК можно считать набором библиотек, помогающих писать содержательные "программы" -**задания по безопасности**, типовые **профили защиты** и т.п. Программисты знают, насколько хорошая библиотека упрощает разработку программ, повышает их качество. Без библиотек, "с нуля", программы не пишут уже очень давно; оценка безопасности тоже вышла на сопоставимый уровень сложности, и "*Общие критерии*" предоставили соответствующий инструментарий.
- Важно отметить, что **требования могут быть параметризованы**, как и полагается библиотечным функциям.

Поддержка жизни изделия

. Принцип иерархии: класс – семейство – компонент – элемент

- Для структуризации пространства требований, в "Общих критериях" введена иерархия класс – семейство – компонент – элемент.
- **Классы** определяют наиболее общую, "предметную" группировку требований (например, функциональные требования подотчетности).
- **Семейства** в пределах класса различаются по строгости и другим тонкостям требований.
- **Компонент** – минимальный набор требований, фигурирующий как целое.
- **Элемент** – неделимое требование.
- Между компонентами могут существовать зависимости, которые возникают, когда компонент сам по себе недостаточен для достижения цели безопасности.
- Подобный принцип организации защиты напоминает принцип программирования с использованием библиотек, в которых содержатся стандартные (часто используемые) функции, из комбинаций которых формируется алгоритм решения.
- "Общие критерии" позволяют с помощью подобных библиотек (компонент) формировать два вида нормативных документов: профиль защиты и задание по безопасности.
- **Профиль защиты** представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Угрозы и уязвимость

Угрозы безопасности в стандарте характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Планировавние обеспечения безопасности

- **Задание по безопасности** содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.
- Функциональный пакет – это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности.
- **Базовый профиль защиты** должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

Функциональные требования

- Все **функциональные требования** объединены в группы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в "Общих критериях" представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это гораздо больше, чем число аналогичных понятий в "Оранжевой книге".
- "Общие критерии" включают следующие классы функциональных требований:
- Идентификация и аутентификация.
- Защита данных пользователя.
- Защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов).
- Управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности).
- Аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности).
- Доступ к объекту оценки.
- Приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных).
- Использование ресурсов (требования к доступности информации).
- Криптографическая поддержка (управление ключами).
- Связь (аутентификация сторон, участвующих в обмене данными).
- Доверенный маршрут/канал (для связи с сервисами безопасности).

Требования к ресурсам

- Класс функциональных требований "Использование ресурсов" включает три семейства.
- **Отказоустойчивость**. Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В стандарте различаются активная и пассивная отказоустойчивость. Активный механизм содержит специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.
- **Обслуживание по приоритетам**. Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.
- **Распределение ресурсов**. Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.
- Аналогично и другие классы включают наборы семейств требований, которые используются для формулировки требований к системе безопасности.
- "Общие критерии" – достаточно продуманный и полный документ с точки зрения функциональных требований и именно на этот стандарт безопасности ориентируются соответствующие организации в нашей стране и в первую очередь Гостехкомиссия РФ.

Жизненный цикл защиты

Доверие к средствам защиты

- **1.5.5. Требования доверия**
- Вторая форма требований безопасности в "Общих критериях" – требования доверия безопасности.
- Установление доверия безопасности основывается на активном исследовании объекта оценки.
- Форма представления требований доверия, та же, что и для функциональных требований (класс – семейство – компонент).
- Всего в "Общих критериях" 10 классов, 44 семейства, 93 компонента требований доверия безопасности.

Доверие

- Применительно к требованиям доверия (для функциональных требований не предусмотрены) в "Общих критериях" введены оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.
- Степень доверия возрастает от первого к седьмому уровню. Так, оценочный уровень доверия 1 (начальный) применяется, когда угрозы не рассматриваются как серьезные, а оценочный уровень 7 применяется к ситуациям чрезвычайно высокого риска.

Классы требований

- **Классы требований доверия безопасности:**
- Разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации).
- Поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки).
- Тестирование.
- Оценка уязвимостей (включая оценку стойкости функций безопасности).
- Поставка и эксплуатация.
- Управление конфигурацией.
- Руководства (требования к эксплуатационной документации).
- Поддержка доверия (для поддержки этапов жизненного цикла после сертификации).
- Оценка профиля защиты.
- Оценка задания по безопасности.

ПОНЯТИЕ И ФОРМЫ УЯЗВИМОСТИ ИНФОРМАЦИИ. ЕЕ ПРОЯВЛЕНИЯ И ВИДЫ

Согласно определению, уязвимость информации – есть мера изменения информации под воздействием различных факторов. С таким определением можно не согласиться хотя бы потому, что информация не обязательно в этом случае будет изменена, она может быть просто скопирована или уничтожена. Уязвимость любой информации заключается в нарушении ее физической сохранности вообще либо у данного собственника (в полном или частичном объеме), структурной целостности, доступности для правомочных пользователей. Уязвимость конфиденциальной информации, в том числе составляющей государственную тайну, дополнительно включает в себя нарушение ее конфиденциальности (закрытости для посторонних лиц).

Возможность изменения или нарушения действующего статуса информации обусловлено в первую очередь ее уязвимостью, которая означает неспособность информации самостоятельно противостоять дестабилизирующим воздействиям, сохранять при таких воздействиях свой статус.

Но уязвимость информации не существует как самостоятельное явление, а проявляется (выражается) в различных формах. Сегодня в научной литературе и нормативных документах не сформировался термин форма проявления уязвимости информации, но самих конкретных форм называется достаточно много. При этом значительное количество перечисляемых форм являются синонимами или разновидностями одних и тех же явлений, некоторые не могут быть отнесены к формам по своей сущности.

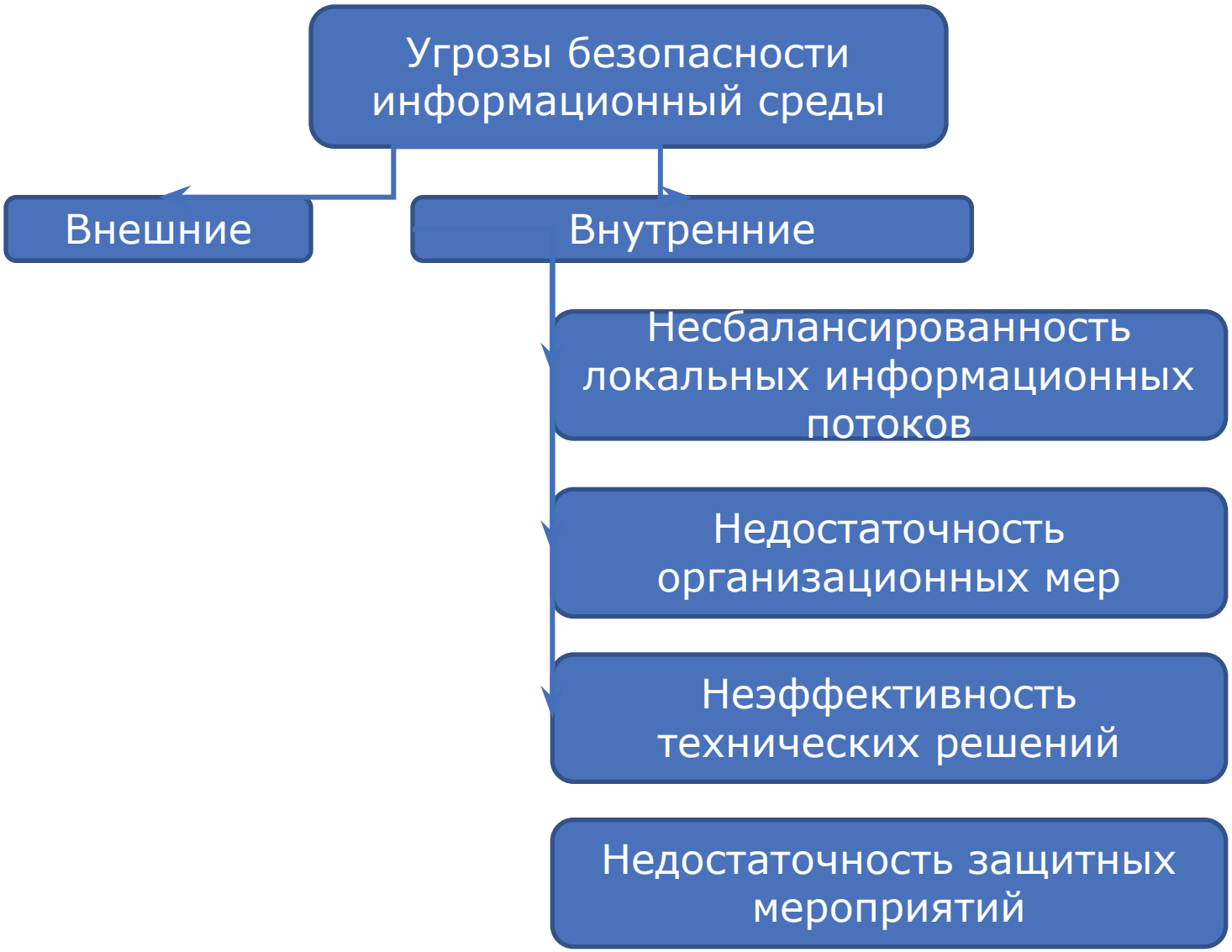
ОБЩИЕ ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

Если в результате проведенной оценки выясняется, что та или иная информация нуждается в защите, — необходимо принять меры по ее защите. Для этого необходимо предотвратить или значительно усложнить хищение информации и довести до сведения всех лиц, имеющих к ней доступ сведения о важности конкретной информации и мерах наказания за ее разглашение.

Целями защиты информации являются :

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

Оценка уязвимостей (включая оценку стойкости функций безопасности)



ОЦЕНКА УЯЗВИМОСТИ ИНФОРМАЦИИ

Для того чтобы обеспечить эффективную защиту интеллектуальной собственности, необходимо провести ее анализ. Требуется, во-первых, определить потенциальную ценность информационной собственности, во-вторых, оценить ее уязвимость (устойчивость к средствам разведки или поражения) и, в-третьих, спрогнозировать возможные угрозы. Определение потенциальной ценности информации обезопасит наиболее важные секреты, утечка которых способна нанести ущерб, значительно превышающий возможные затраты на их защиту.

При этом важно установить :

- какая информация нуждается в защите?
- кого она может заинтересовать?
- какие элементы информации наиболее ценны?
- каков “срок жизни” этих средств?
- во что обойдется их защита?

Оценка уязвимости информации дает возможность выявить характерные особенности и недостатки объекта защиты, которые могут облегчить проникновение противника к секретам компании. Главный результат такой работы — выявление возможных источников и каналов утечки информации.

Угрозы безопасности

- **Основные:**

- Галатенко В. А. Стандарты информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2004.
- Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: Издательство Молгачева С. В., 2001.
- www.infotecs.ru/gts/ – Сервер Государственной технической комиссии при Президенте Российской Федерации.
- Галатенко В. А. Основы информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2003.
- Карпов Е. А., Котенко И. В., Котухов М. М., Марков А. С., Парр Г. А., Рунеев А. Ю. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Под редакцией И. В. Котенко. – СПб.: ВУС, 2000.
- www.jetinfo.ru.

- **Аутентификация**. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. **Аутентификация партнеров по общению** используется при установлении соединения и периодически во время сеанса. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).
- **Управление доступом** обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.
- **Конфиденциальность данных** обеспечивает защиту от несанкционированного получения информации. Отдельно выделяется **конфиденциальность трафика** – это защита информации, которую можно получить, анализируя сетевые потоки данных.
- **Целостность данных** подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры – с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.
- **Неотказуемость** (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки.

Механизмы управления безопасностью

Администрирование информационной системы в целом включает *обеспечение* актуальности политики безопасности, *взаимодействие* с другими административными службами, реагирование на происходящие события, *аудит* и *безопасное восстановление*.

Администрирование сервисов безопасности включает в себя *определение* защищаемых объектов, *выработку правил* подбора механизмов безопасности (при наличии альтернатив), *комбинирование механизмов* для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Администрирование механизмов безопасности включает:

1. управление криптографическими ключами (генерация и распределение);
2. управление шифрованием (установка и синхронизация криптографических параметров);
3. администрирование управления доступом (распределение информации, необходимой для управления – паролей, списков доступа и т. п.);
4. управление аутентификацией (распределение информации, необходимой для аутентификации – паролей, ключей и т. п.);
5. управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений – частоту отправки, размер и т. п.);
6. управление маршрутизацией (выделение доверенных путей);
7. управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ

Федеральная служба по техническому и экспортному контролю:

В Российской Федерации информационная безопасность обеспечивается соблюдение указов Президента, федеральных законов, постановлений Правительства Российской Федерации, руководящих документов Гостехкомиссии России и других нормативных документов.

Наиболее общие документы были рассмотрены ранее при изучении правовых основ информационной безопасности. В РФ с точки зрения стандартизации положений в сфере информационной безопасности первостепенное значение имеют руководящие документы (РД) Гостехкомиссии России, одной из задач которой является "проведение единой государственной политики в области технической защиты информации".

Гостехкомиссия России ведет весьма активную нормотворческую деятельность, выпуская руководящие документы, играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления Гостехкомиссия России выбрала ориентацию на "Общие критерии".

Экспортный контроль

- В соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:
- 1) обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;
- 2) противодействия иностранным техническим разведкам на территории Российской Федерации;
- 3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;
- 4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
- 5) осуществления экспортного контроля.