**Основные критерии защищенности АС.**

**1. Классификация систем защиты АС.**

**1.1. Руководящие документы государственной технической комиссии России**

В 1992 г. Гостехкомиссия (ГТК) при Президенте Российской Федерации разработала и опубликовала пять руководящих документов, посвященных вопросам защиты информации в автоматизированных системах ее обработки. Основой этих документов является концепция защиты средств вычислительной техники (СВТ) и АС от несанкционированного доступа к информации, содержащая систему взглядов ГТК на проблему информационной безопасности и основные принципы защиты компьютерных систем. С точки зрения разработчиков данных документов, основная задача средств безопасности - это обеспечение защиты от несанкционированного доступа к информации. Определенный уклон в сторону поддержания секретности информации объясняется тем, что данные документы были разработаны в расчете на применение в информационных системах силовых структур РФ.

**1.1.1 Структура требований безопасности**

Руководящие документы ГТК состоят из пяти частей:

1. Защита от несанкционированного доступа к информации. Термины и определения.

2. Концепция защиты СВТ и АС от несанкционированного доступа (НСД) к информации.

3. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

4. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации.

5. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники.

Наибольший интерес представляют вторая, третья и четвертая части. Во второй части излагается система взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от НСД. Руководящие документы ГТК предлагают две группы требований к безопасности - показатели защищенности СВТ от НСД и критерии защищенности АС обработки данных. Первая группа позволяет оценить степень защищенности отдельно поставляемых потребителю компонентов АС и рассматривается в четвертой части, а вторая рассчитана на более сложные комплексы, включающие несколько единиц СВТ, и представлена в третьей части руководящих документов.

**1.1.2. Основные положения концепции защиты СВТ и АС от НСД к информации**

Концепция предназначена для заказчиков, разработчиков и пользователей СВТ и АС, используемых для обработки, хранения и передачи требующей защиты информации. Она является методологической базой нормативно-технических и методических документов, направленных на решение следующих задач:

• выработка требований по защите СВТ и АС от НСД к информации;

• создание защищенных СВТ и АС, т.е. защищенных от НСД к информации;

• сертификация защищенных СВТ и АС.

Как уже было сказано выше, концепция предусматривает существование двух относительно самостоятельных направлений в проблеме защиты информации от НСД: направления, связанного с СВТ, и направления, связанного с АС. Различие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации. В случае СВТ можно говорить лишь о защищенности (защите) СВТ от НСД к информации, для обработки, хранения и передачи которой СВТ предназначено. Примером СВТ можно считать специализированную плату расширения с соответствующим аппаратным и программным интерфейсом, реализующую функции аутентификации пользователя по его биометрическим характеристикам. Или к СВТ можно отнести программу прозрачного шифрования данных, сохраняемых на жестком диске.

При создании АС появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации. Типичным примером АС является многопользовательская, многозадачная ОС.

Для определения принципов защиты информации в руководящих документах ГТК дается понятие НСД к информации: НСД – доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. В данном определении под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

Понятие НСД является чрезвычайно важным, так как оно определяет, от чего сертифицированные по руководящим документам ГТК системы защиты АС и СВТ должны защищать информацию. Например, к НСД не отнесены разрушительные последствия стихийных бедствий, хотя они и представляют угрозу информации, в частности ее целостности и доступности.

К основным способам НСД относятся:

непосредственное обращение к объектам доступа (например, через получение программой, управляемой пользователем, доступа на чтение или запись, в файл);

создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты (например, используя люки, оставленные разработчиками системы защиты);

модификация средств защиты, позволяющая осуществить НСД (например, путем внедрения в систему защиты программных закладок или модулей, выполняющих функции "троянского коня");

внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД (например, путем загрузки на компьютер в обход штатной ОС иной ОС, не имеющей функций защиты).

Далее в руководящих документах ГТК представлены семь принципов защиты информации:

защита СВТ и АС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации;

защита СВТ обеспечивается комплексом программно-технических средств;

защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер;.

защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ;

программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС);

неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты;

защита АС должна предусматривать контроль эффективности средств защиты от НСД, который либо может быть периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

Несмотря на то, что угрозы информации могут реализовываться широким спектром способов, так или иначе изначальным источником всех угроз является человек или нарушитель. В качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ и являющийся специалистом высшей квалификации, знающим все о АС и, в частности, о системе и средствах ее защиты.

В руководящих документах ГТК дается классификация нарушителя по уровню возможностей, предоставляемых ему штатными средствами АС и СВТ Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего. Выделяется четыре уровня этих возможностей.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в AC - запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации (в качестве примера АС, предоставляющей нарушителю описанный круг возможностей, можно привести систему обработки формализованных почтовых сообщений).

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации (например, в данном случае предполагается, что нарушитель может выступать в роли "обычного" пользователя ОС).

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования (например, к данному классу относится нарушитель, внедривший в систему безопасности АС программную закладку).

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации (например, известны случаи, когда в АС внедрялись "временные бомбы", выводящие систему из строя по истечении срока гарантийного ремонта).

Кроме перечисленных выше понятий во второй части руководящих документов ГТК рассматриваются:

основные направления обеспечения защиты от НСД, в частности основные функции средств разграничения доступа (СРД) и обеспечивающих СРД средств;

основные характеристики технических средств защиты от НСД;

порядок организации работ по защите.

**1.1.3. Показатели защищенности средств вычислительной техники от НСД**

В ч.2 руководящих документов ГТК устанавливается классификация СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Под СВТ понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Показатели защищенности содержат требования защищенности СВТ от НСД к информации и применяются к общесистемным программным средствам и операционным системам (с учетом архитектуры компьютера). Конкретные перечни показателей определяют классы защищенности СВТ и описываются совокупностью требований. Совокупность всех средств защиты составляет комплекс средств защиты (КСЗ).

По аналогии с критерием TCSEC, который будет рассмотрен далее. установлено семь классов защищенности СВТ от НСД к информации. Самый низкий класс - седьмой, самый высокий - первый. Показатели защищенности и требования к классам приведены в табл.1.

Таблица 1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Показатель защищенности | Класс защищенности | | | | | |
| 6 | 5 | 4 | 3 | 2 | 1 |
| Дискреционный принцип контроля доступа | + | + | + | = | + | = |
| Мандатный принцип контроля доступа | - | - | + | = | = | = |
| Очистка памяти | - | + | + | + | = | = |
| Изоляция модулей | - | - | + | = | + | = |
| Маркировка документов | - | - | + | = | = | = |
| Защита ввода и вывода на отчужденный физический носитель информации | - | - | + | = | = | = |
| Сопоставление пользователя с устройством | - | - | + | = | = | = |
| Идентификация и аутентификация | + | = | + | = | = | = |
| Гарантии проектирования | - | + | + | + | + | + |
| Регистрация | - | + | + | + | = | = |
| Взаимодействие пользователя с КСЗ | - | - | - | + | = | = |
| Надежное восстановление | - | - | - | + | = | = |
| Целостность КСЗ | - | + | + | + | = | = |
| Контроль модификации | - | - | - | - | + | = |
| Контроль дистрибуции | - | - | - | - | + | = |
| Гарантии архитектуры | - | - | - | - | - | + |
| Тестирование | + | + | + | + | + | = |
| Руководство пользователя | + | = | = | = | = | = |
| Руководство по КСЗ | + | + | = | + | + | = |
| Текстовая документация | + | + | + | + | + | = |
| Конструкторская (проектная) документация | + | + | + | + | + | + |
| Примечания. "-" – нет требований к данному классу; "+" – новые или дополнительные требования; "=" – требования совпадают с требованиями к СВТ предыдущего класса. | | | | | | |

Важно отметить, что требования являются классическим примером применения необходимых условий оценки качества защиты, т.е. если какой-либо механизм присутствует, то это является основанием для отнесения СВТ к некоторому классу.

Интересно, что защищенные СВТ содержат разделение только по двум классам политик безопасности: дискреционной и мандатной.

Невлияние субъектов друг на друга описывается требованием "изоляция модулей" (требуется с 4-го класса). Гарантии выполнения политики безопасности коррелированны с требованием "целостность КСЗ" (требуется с 5-го класса) и "гарантии проектирования" (требуется также с 5-го класса).

**1.1.4. Классы защищенности АС**

В ч.З руководящих документов ГТК дается классификация АС и требований по защите информации в АС различных классов. При этом определяются:

1. Основные этапы классификации АС:

разработка и анализ исходных данных;

выявление основных признаков АС, необходимых для классификации;

сравнение выявленных признаков АС с классифицируемыми;

присвоение АС соответствующего класса защиты информации от НСД.

2. Необходимые исходные данные для классификации конкретной АС:

перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;

перечень лиц, имеющих доступ к штатным средствам АС с указанием их уровня полномочий;

матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

режим обработки данных в АС.

3. Признаки, по которым производится группировка АС в различные классы:

наличие в АС информации различного уровня конфиденциальности;

уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации,

режим обработки данных в АС: коллективный или индивидуальный.

Документы ГТК устанавливают девять классов защищенности АС от НСД, распределенных по трем группам. Каждый класс характеризуется определенной совокупностью требований к средствам защиты. В пределах каждой группы соблюдается иерархия классов защищенности АС. Класс, соответствующий высшей степени защищенности для данной группы, обозначается индексом NА, где N - номер группы (от 1 до 3). Следующий класс обозначается NB и т.д.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - ЗБ и ЗА.

Вторая группа включает АС, в которых пользователи имеют одинаковые полномочия доступа ко всей информации, обрабатываемой и хранимой в АС на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и хранится информация разных уровней конфиденциальности. Не все пользователи имеют равные права доступа. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

В табл. 2 приведены требования к подсистемам защиты для каждого класса защищенности.

Таблица 2

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Подсистемы защиты и требования к ним | | Классы защищенности | | | | | | | | | | | | | | | |
| ЗБ | ЗА | 2Б | | 2А | | 1Д | | 1Г | | 1В | | 1Б | | 1А | |
| 1. Подсистема управления  доступом | |  |  |  | |  | |  | |  | |  | |  | |  | |
| 1.1. Идентификация. Проверка подлинности и контроль доступа субъектов: | |  |  |  | |  | |  | |  | |  | |  | |  | |
| в систему | | + | + | + | | + | | + | | + | | + | | + | | + | |
| к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ | |  |  |  | | ++ | |  | | ++ | | ++ | | ++ | | ++ | |
| к программам | |  |  |  | | + | |  | | + | | + | | + | | + | |
| к томам, каталогам, файлам, записям, полям записей | |  |  |  | | ++ | |  | | ++ | | ++ | | ++ | | ++ | |
| 1.2. Управление потоками информации | |  |  |  | | + | |  | |  | | + | | + | | + | |
| 2. Подсистема регистрации и учета | |  |  |  | |  | |  | |  | |  | |  | |  | |
| 2.1. Регистрация и учет: | |  |  |  | |  | |  | |  | |  | |  | |  | |
| входа/выхода субъектов доступа в/из системы (узла сети) | | + | + | + | | + | | + | | + | | + | | + | | + | |
|  | |  |  |  | |  | |  | |  | |  | |  | |  | |
| Подсистемы защиты и требования к ним | | Классы защищенности | | | | | | | | | | | | | | | |
| ЗБ | ЗА | 2Б | | 2А | | 1Д | | 1Г | | 1В | | 1Б | | 1А | |
| выдачи печатных (графических) выходных документов | |  | + |  | | + | |  | | + | | + | | + | | + | |
| запуска/завершения программ и процессов (заданий, задач) | |  |  |  | | + | |  | | + | | + | | + | | + | |
| доступа программ субъектов к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи | |  |  |  | | ++ | |  | | ++ | | ++ | | ++ | | ++ | |
| доступа программ субъектов, доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, каталогам, файлам, записям, полям записей | |  |  |  | | + | |  | | + | | + | | + | | + | |
| изменения полномочий субъектов доступа | |  |  |  | |  | |  | |  | | + | | + | | + | |
| создаваемых защищаемых объектов доступа | |  |  |  | | + | |  | |  | | + | | + | | + | |
| 2.2. Учет носителей информации | | + | + | + | | + | | + | | + | | + | | + | | + | |
| 2.3. Очистка (обнуление, обезличивание) освобождаемых областей, оперативной памяти ЭВМ и внешних накопителей | |  | + |  | | + | |  | | + | | + | | + | | + | |
| 2.4. Сигнализация попыток нарушения защиты | |  |  |  | |  | |  | |  | | + | | + | | + | |
| 3. Криптографическая подсистема | | | |  | |  | |  | |  | |  | |  | |  | |  |  |
| 3.1. Шифрование конфиденциальной информации | | | |  | |  | |  | | + | |  | |  | |  | | + | + |
| 3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах | | | |  | |  | |  | |  | |  | |  | |  | |  | + |
| 3.3. Использование аттестованных (сертифицированных) криптографических средств | | | |  | |  | |  | | + | |  | |  | |  | | + | + |
| 4. Подсистема обеспечения целостности | | | |  | |  | |  | |  | |  | |  | |  | |  |  |
| 4.1. Обеспечение целостности программных средств и обрабатываемой информации | | | | + | | + | | + | | + | | + | | + | | + | | + | + |
| 4.2. Физическая охрана средств вычислительной техники и носителей информации | | | | + | | + | | + | | + | | + | | + | | + | | + | + |
| 4.3. Наличие администратора (службы) защиты информации в АС | | | |  | |  | |  | | + | |  | |  | | + | | + | + |
| 4.4. Периодическое тестирование СЗИ НСД | | | | + | | + | | + | | + | | + | | + | | + | | + | + |
| 4.5. Наличие средств восстановления СЗИ НСД | | | | + | | + | | + | | + | | + | | + | | + | | + | + |
| 4.6. Использование сертифицированных средств защиты | | | |  | | + | |  | | + | |  | |  | | + | | + | + |
| Примечания: "+" – требование к данному классу присутствует, в остальных случаях данное требование необязательно. | | | | | | | | | | | | | | | | | | | |

Рассмотренные выше документы ГТК необходимо воспринимать как первую стадию формирования отечественных стандартов в области информационной безопасности. На разработку этих документов наибольшее влияние оказал критерий TCSEC ("Оранжевая книга"), который будет рассмотрен ниже, однако это влияние в основном отражается в ориентированности этих документов на защищенные системы силовых структур и в использовании единой универсальной шкалы оценки степени защищенности.

К недостаткам руководящих документов ГТК относятся: ориентация на противодействие НСД и отсутствие требований к адекватности реализации политики безопасности. Понятие "политика безопасности" трактуется исключительно как поддержание режима секретности и отсутствие НСД. Из-за этого средства защиты ориентируются только на противодействие внешним угрозам, а к структуре самой системы и ее функционированию не предъявляется четких требований. Ранжирование требований по классам защищенности по сравнению с остальными стандартами информационной безопасности максимально упрощено и сведено до определения наличия или отсутствия заданного набора механизмов защиты, что существенно снижает гибкость требований и возможность их практического применения.

**1.2. Критерии оценки безопасности компьютерных систем Министерства обороны США ("Оранжевая книга")**

"Критерии оценки безопасности компьютерных систем" (Trusted Computer System Evaluation Criteria-TCSEC), получившие неформальное, но прочно закрепившееся название "Оранжевая книга", были разработаны и опубликованы Министерством обороны США в 1983 г. с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному программному и информационному обеспечению компьютерных систем, и выработки методологии и технологии анализа степени поддержки политики безопасности в компьютерных системах в основном военного назначения.

В данном документе были впервые формально (хотя и не вполне строго) определены такие понятия, как "политика безопасности", "корректность" и др. Согласно "Оранжевой книге" безопасная компьютерная система – это система, поддерживающая управление доступом к обрабатываемой в ней информации так, что только соответствующим образом авторизованные пользователи или процессы (субъекты), действующие от их имени, получают возможность читать, записывать, создавать и удалять информацию. Предложенные в этом документе концепции защиты и набор функциональных требований послужили основой для формирования всех появившихся впоследствии стандартов безопасности.

**1.2.1. Общая структура требований TCSEC**

В "Оранжевой книге" предложены три категории требований безопасности: политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены непосредственно на обеспечение безопасности информации, а два последних на качество средств защиты.

**Политика безопасности**

Требование 1. Политика безопасности. Система должна поддерживать точно определенную политику безопасности. Возможность доступа субъектов к объектам должна определяться на основании их идентификации и набора правил управления доступом. Там, где это необходимо, должна использоваться политика мандатного управления доступом, позволяющая эффективно реализовать разграничение доступа к информации различного уровня конфиденциальности.

Требование 2. Метки. С объектами должны быть ассоциированы метки безопасности, используемые в качестве исходной информации для процедур контроля доступа. Для реализации мандатного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объекта и режимы доступа к этому объекту.

Подотчетность

Требование 3. Идентификация и аутентификация. Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (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 с точки зрения безопасности.

Требование 4. Регистрация и учет. Для определения степени ответственности пользователей за действия в системе, все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе (т. е. должен существовать объект компьютерной системы, потоки от которого и к которому доступны только субъекту администрирования). Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективности его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

Гарантии (корректность)

Требование 5. Контроль корректности функционирования средств защиты. Средства защиты должны содержать независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учет, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

Требование 6. Непрерывность защиты. Все средства защиты (в том числе и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одной из ключевых аксиом, используемых для формального доказательства безопасности системы.

**1.2.2. Классы защищенности компьютерных систем по TCSEC**

"Оранжевая книга" предусматривает четыре группы критериев, которые соответствуют различной степени защищенности: от минимальной (группа D) до формально доказанной (группа А). Каждая группа включает один или несколько классов. Группы D и А содержат по одному классу (классы D и А соответственно), группа С – классы С1, С2, а группа В три класса – В1, В2, ВЗ, характеризующиеся различными наборами требований защищенности. Уровень защищенности возрастает от группы D к группе А, а внутри группы - с увеличением номера класса. Усиление требований осуществляется с постепенным смещением акцентов от положений, определяющих наличие в системе каких-то определенных механизмов защиты, к положениям обеспечивающих высокий уровень гарантий того, что система функционирует в соответствии требованиям политики безопасности (табл. 3). Например, по реализованным механизмам защиты классы ВЗ и А1 идентичны.

Таблица 3

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Базовые требования "Оранжевой книги" | | Классы защищенности | | | | | |
| С1 | С2 | В1 | В2 | ВЗ | А1 |
| Политика безопасности | | | | | | | |
| 1. | Дискреционная политика безопасности | + | + | + | = | = | = |
| 2. | Мандатная политика безопасности | - | - | + | + | = | = |
| 3. | Метки секретности | - | - | + | + | = | = |
| 4. | Целостность меток | - | - | + | = | = | = |
| 5. | Рабочие метки | - | - | - | + | = | = |
| 6. | Повторение меток | - | - | + | = | = | = |
| 7. | Освобождение ресурсов при повторном использовании объектов | - | + | = | + | = | = |
| 8. | Изолирование модулей | - | + | = | = | = | = |
| 9. | Пометка устройств ввода/вывода | - | - | + | = | = | = |
| 10. | Пометка читаемого вывода | - | - | + | = | = | = |
| Подотчетность | | | | | | | |
| 11. | Идентификация и аутентификация | + | + | = | = | = | = |
| 12. | Аудит | - | + | + | + | + | = |
| 13. | Защищенный канал (доверенный путь) | - | - | - | + | = | = |
| Гарантии | | | | | | | |
| 14. | Проектная спецификация и верификация | - | - | + | + | + | + |
| 15. | Системная архитектура | + | = | = | + | + | = |
| 16. | Целостность системы | + | = | = | = | = | = |
| 17. | Тестирование системы безопасности | + | + | + | + | + | = |
| 18. | Доверенное восстановление после сбоев | - | - | - | - | + | = |
| 19. | Управление конфигурацией системы | - | - | - | + | + | + |
| 20. | Доверенное дооснащение системы | - | - | - | + | + | = |
| 21. | Доверенное распространение | - | - | - | - | + | = |
| 22. | Анализ скрытых каналов | - | - | - | + | + | + |
| Документация | | | | | | | |
| 23 | Руководство пользователя | + | = | = | = | = | = |
| 24 | Руководство по конфигурированию системы защиты | + | + | + | + | + | = |
| 25 | Документация по тестированию | + | = | = | = | = | + |
| 26 | Проектная документация | + | = | + | + | = | + |
| Примечания. "-" – нет требований к данному классу; "+" – новые или дополнительные требования; "=" – требования совпадают с требованиями к СВТ предыдущего класса | | | | | | | |

Рассмотрим основные требования классов защищенности по указанным выше четырем категориям:

• политика безопасности;

• подотчетность;

• гарантии;

• документация.

Центральным объектом исследования и оценки по TCSEC является доверительная база вычислений (ТСВ).

Группа D. Минимальная защита

Класс D. Минимальная защита. Класс D зарезервирован для тех систем, которые были представлены на сертификацию (оценку), но по какой-либо причине ее не прошли.

Группа С. Дискреционная защита

Группа С характеризуется наличием дискреционного управления доступом и аудитом действий субъектов.

Класс С1. Системы на основе дискреционного разграничения доступа. ТСВ систем, соответствующих этому классу защиты, удовлетворяет неким минимальным требованиям безопасного разделения пользователей и данных. Она определяет некоторые формы разграничения доступа на индивидуальной основе, т.е. пользователь должен иметь возможность защитить свою информацию от ее случайного чтения или уничтожения. Пользователи могут обрабатывать данные как по отдельности, так и от имени группы пользователей.

Политика безопасности. ТСВ должна определять и управлять доступом между поименованными объектами и субъектами (пользователями или их группами) в компьютерной системе (например, при помощи матрицы доступа). Механизм защиты должен позволять пользователям определять и контролировать распределение доступа к объектам по поименованным пользователям, их группам или по тем и другим.

Подотчетность. Пользователи должны идентифицировать себя перед ТСВ в случае выполнения ими любых действий, ею контролируемых, при этом должен быть использован хотя бы один из механизмов аутентификации (например, пароль). Данные аутентификации должны быть защищены от доступа неавторизованного пользователя.

Гарантии. ТСВ обеспечивает ее собственную работу и защиту от внешнего воздействия. Ресурсы системы, контролируемые ТСВ, являются подмножеством множества всех ресурсов. Должны быть предоставлены АО и ПО для периодической проверки правильности работы ТСВ. Тестирование ТСВ должно выполняться согласно документации для обеспечения гарантии того, что нет явных путей обхода системы защиты неавторизованным пользователем или иного расстройства системы защиты.

Документация должна включать:

описание реализованных в ТСВ механизмов защиты, их взаимодействия и руководство пользователя по их использованию;

руководство для администратора системы на гарантирование системы защиты;

документацию по тестам, включающую описание того, как механизмы безопасности должны тестироваться и как интерпретировать результаты тестов;

документацию по проекту, описывающую философию системы защиты и того, как эта философия реализована в ТСВ (если ТСВ состоит из нескольких модулей, то должен быть описан интерфейс между ними).

Класс С1 рассчитан на многопользовательские системы, в которых осуществляется совместная обработка данных одного уровня конфиденциальности.

Класс С2. Системы, построенные на основе управляемого дискреционного разграничения доступа.

Системы, сертифицированные по данному классу, должны удовлетворять всем требованиям, изложенным в классе С1. Однако, системы класса С2 поддерживают более тонкую, чем в классе С1, политику дискреционного разграничения доступа, делающую пользователя индивидуально ответственным за свои действия после процедуры аутентификации в системе, а также аудит событий, связанных с безопасностью системы.

Политика безопасности. ТСВ должна осуществлять контроль за распространением прав доступа. Механизм дискреционного контроля доступа должен при каждом действии пользователя или его отсутствии обеспечивать защиту объектов от неавторизованного воздействия. При этом должен определяться доступ для каждого отдельного пользователя. Наделять пользователей правом доступа к объекту могут только авторизованные для этого пользователи. Никакая информация (в том числе шифрованная) о предшествующих действиях субъекта не может быть получена субъектом, получившим после первого доступ к системе. Реализация этого требования обеспечивает очищение ресурсов после освобождения их процессами системы.

Подотчетность. ТСВ должна обеспечивать индивидуальную ответственность пользователей за осуществляемые ими действия, обеспечивая возможность ассоциировать пользователя с любым событием аудита. При этом должен поддерживаться и защищаться журнал аудита, доступ к нему разрешаться только тем, кто специально для этого авторизован. Аудиту подлежит следующий стандартный набор событий, среди которых:

идентификация и аутентификация пользователя;

размещение объектов в адресном пространстве процессов пользователей (например, чтение информации из файлов);

уничтожение объектов;

действия, осуществляемые администраторами системы.

При этом запись журнала аудита должна снабжаться необходимым набором атрибутов:

дата и время события;

идентификатор пользователя, инициировавшего событие;

тип события (например, вход в систему, получение доступа к файлу на чтение и т.д.);

результат: успех или неуспех выполнения события.

Если требуется, надо указывать дополнительные сведения, например имя объекта, к которому происходит обращение. Для удобства изучения данных журнала аудита должны быть предусмотрены средства фильтрации записей по заданным признакам.

Гарантии. ТСВ должна изолировать подлежащие защите ресурсы так, чтобы выполнялись требования контроля доступа и аудита.

Тестирование должно включать поиск и просмотр очевидных брешей системы защиты, позволяющих нарушить изолированность ресурсов или допустить неавторизованный доступ к данным аутентификации или журнала аудита.

Документация должна дополнительно (по сравнению с классом С1) включать описание событий, заносимых в журнал аудита.

Группа В. Мандатное управление доступом

Основные требования этой группы - мандатное (полномочное) управление доступом с использованием меток безопасности, реализация некоторой формальной модели политики безопасности, а также наличие спецификаций на функции ТСВ. В системах этой группы постепенно к классу ВЗ должен быть реализован монитор ссылок, который должен контролировать все доступы субъектов к объектам системы.

Класс В1. Системы класса В1 должны удовлетворять требованиям класса С2. Кроме того, должны быть выполнены следующие дополнительные требования.

Политика безопасности. ТСВ должна обеспечивать пометку каждого субъекта и объекта системы. Метки секретности должны представлять уровень доступа субъекта и уровень секретности объекта, которым они соответствуют. Именно эти метки должны служить основой для принятия решения ТСВ при запросе субъекта доступа к объекту. При передаче информации по каналам ввода/вывода ТСВ должна снабжаться соответствующими метками секретности. ТСВ должна также соответствующе маркировать метками секретности весь читаемый вывод. Доступ на чтение от субъекта к объекту может быть разрешен, только если уровень допуска субъекта не ниже уровня секретности объекта, а неиерархические категории первого включают все неиерархические категории второго. Доступ на запись от субъекта к объекту, контролируемый ТСВ, может быть разрешен, только если уровень допуска субъекта не выше уровня секретности объекта, а все неиерархические категории первого входят в неиерархические категории второго.

Подотчетность. Аудиту подлежат любые изменения меток секретности читаемого вывода.

Гарантии. ТСВ должна обеспечивать изоляцию процессов системы, через выделение им соответствующего адресного пространства.

Целью тестирования является:

поиск всех каналов проникновения внешних субъектов с целью получения несанкционированного доступа к информации;

получение гарантии того, что никакой неавторизованный для этого специально пользователь не может ввести ТСВ в состояние, в котором она не способна отвечать на запросы других субъектов.

ТСВ должна быть построена на основе неформальной или формальной политики безопасности, которая должна поддерживаться на протяжении всего жизненного цикла системы.

Класс В2. Структурированная защита. Выполняются все требования класса защиты В1. Кроме того, в системах класса В2 ТСВ основывается на четко определенной и хорошо документированной формальной модели политики безопасности, требующей, чтобы мандатная и дискреционная системы разграничения доступа были распространены на все субъекты и объекты компьютерной системы. ТСВ должна быть четко структурирована на элементы, критичные с точки зрения безопасности и некритичные. Интерфейс ТСВ должен быть хорошо определен и ее проект и конечный результат должны быть подвергнуты полной проверке и тестированию. Механизм аудита должен быть усилен, введен контроль за конфигурацией системы. Система должна быть устойчива к внешнему проникновению.

Политика безопасности. ТСВ должна уведомлять каждого работающего в системе пользователя о любых изменениях его уровня секретности, а последний должен иметь возможность запрашивать у системы полную информацию о своей метке секретности. ТСВ должна поддерживать минимальные и максимальные метки секретности любого присоединенного физического устройства, которые должны определять непосредственное физическое окружение этого устройства.

Подотчетность. ТСВ должна обеспечить защищенный канал между собой и пользователем, осуществляющим вход в систему и аутентификацию. Инициатором осуществления соединения через такой защищенный канал может выступать только пользователь.

Гарантии. ТСВ должна быть внутренне структурирована на хорошо определенные, в большой степени независимые модули. Это достигается с помощью эффективного использования имеющегося в системе АО с целью разделения критичных и некритичных с точки зрения защиты модулей ТСВ. Все элементы ТСВ должны быть идентифицированы, а интерфейс между ними полностью определен. ТСВ должна обеспечить разделение функций оператора и администратора системы.

Разработчики системы должны полностью выявить скрытые каналы утечки и провести их инженерное обследование с целью измерения информационного потока для каждого канала. ТСВ должна быть рассмотрена по всем положениям, относящимся к ее устойчивости к проникновению. Тестирование ТСВ должно показать, что она функционирует согласно представленной в описании высокоуровневой спецификации.

Формальная модель политики безопасности должна поддерживаться ТСВ на протяжении всего жизненного цикла компьютерной системы. Должна существовать служба управления конфигурацией системы и должны быть предоставлены средства для создания новых версий ТСВ.

Класс ВЗ. Домены безопасности. В системах класса ВЗ ТСВ должна удовлетворять всем требованиям предыдущего класса и дополнительно требованиям монитора ссылок, который должен быть:

защищен от несанкционированного изменения или порчи;

обрабатывать все обращения;

прост для анализа и тестирования.

ТСВ должна быть структурирована таким образом, чтобы исключить код, не имеющий отношения к безопасности системы.

Дополнительно должно быть обеспечено:

поддержка администратора безопасности;

расширение механизма аудита с целью сигнализации о любых событиях, связанных с безопасностью;

поддержка процедуры восстановления системы.

Политика безопасности. Не включает существенных дополнительных требований по сравнению с предыдущим классом защиты.

Подотчетность. Должно быть обеспечено создание защищенного канала для любого соединения пользователя с ТСВ (вход в систему, аутентификация, изменение секретных свойств объектов). Должен быть реализован механизм, осуществляющий анализ и накопление данных о событиях, имеющих отношения к безопасности и могущих послужить причиной нарушения политики безопасности. Этот механизм должен уведомлять администратора безопасности, когда превышается некоторый порог срабатывания. Если это событие или последовательность событий продолжается, то система должна предпринять наименее разрушительное действие для их блокирования.

Гарантии. ТСВ должна быть разработана и структурирована с использованием полного, концептуально-целостного механизма защиты с точно определенной семантикой. Сложность ТСВ должна быть минимизирована. Должен быть исключен код, не имеющий отношения к безопасности системы.

Функции, не связанные с управлением безопасностью и выполняемые пользователем, выступающим в роли администратора безопасности системы, должны быть ограничены набором только тех функций, которые делают более эффективным выполнение этой роли. Должен быть обеспечен механизм восстановления при сбоях компьютерной системы без нарушения ее безопасности. На этапе тестирования не должно быть найдено проектных брешей в системе защиты. Должно быть четко показано, что высокоуровневая спецификация ТСВ соответствует модели политики безопасности.

Группа А. Верифицированная защита

Данная группа характеризуется применением формальных методов верификации корректности работы механизмов управления доступом (дискреционного и мандатного). Требуется, чтобы было формально показано соответствие архитектуры и реализации ТСВ требованиям безопасности.

Класс А1. Формальная верификация. Критерий защиты класса А1 не определяет дополнительные по сравнению с классом ВЗ требования к архитектуре или политике безопасности компьютерной системы. Дополнительным свойством систем, отнесенных к классу А1, является проведенный анализ ТСВ на соответствие формальным высокоуровневым спецификациям и использование технологий проверки с целью получения высоких гарантий того, что ТСВ функционирует корректно.

Наиболее важные требования к классу А1 можно объединить в пять групп:

формальная модель политики безопасности должна быть четко определена и документирована, должно быть дано математическое доказательство того, что модель соответствует своим аксиомам и что их достаточно для поддержания заданной политики безопасности;

формальная высокоуровневая спецификация должна включать абстрактное определение выполняемых ТСВ функций и аппаратный и(или) встроенный программный механизм для обеспечения разделения доменов;

формальная высокоуровневая спецификация ТСВ должна демонстрировать соответствие модели политики безопасности с использованием, где это возможно, формальной технологии (например, где имеются проверочные средства) и неформальной во всех остальных случаях;

должно быть неформально показано и обратное соответствие элементов ТСВ формальной высокоуровневой спецификации, формальная высокоуровневая спецификация должна представлять собой универсальный механизм защиты, реализующий политику безопасности, элементы этого механизма должны быть отображены на элементы ТСВ;

должны быть использованы формальные технологии для выявления и анализа скрытых каналов, неформальная технология может быть использована для анализа скрытых временных каналов, существование оставшихся в системе скрытых каналов должно быть оправдано.

Более строгие требования предъявляются к управлению конфигурацией системы и конкретному месту дислокации (развертывания) системы.

Перечисленные требования не затрагивают группы Политика безопасности и Подотчетность и сконцентрированы в группе Гарантии с соответствующим описанием в группе Документация.

1.2.3 Интерпретация и развитие TCSEC

Опубликование TCSEC стало важным этапом как в постановке основных теоретических проблем компьютерной безопасности, так и в указании направления их решения. Тем не менее, в ходе применения ее основных положений выяснилось, что часть практически важных вопросов осталась за рамками данного стандарта. Кроме того, с течением времени ряд положений устарел и потребовал пересмотра.

Круг специфических вопросов по обеспечению безопасности компьютерных сетей и систем управления базами данных нашел отражение в отдельных документах, изданных Национальным центром компьютерной безопасности США в виде дополнений к "Оранжевой книге":

"Интерпретация TCSEC для компьютерных сетей" (Trusted Network Interpretation).

"Интерпретация TCSEC для систем управления базами данных" (Trusted Database Management System Interpretation).

Устаревание ряда положений TCSEC обусловлено прежде всего интенсивным развитием компьютерных технологий и переходом с вычислительных комплексов типа IBM-360/370 к рабочим станциям, высокопроизводительным персональным компьютерам и сетевой модели вычислений. Именно для того, чтобы исключить возникшую в связи с изменением аппаратной платформы некорректность некоторых положений "Оранжевой книги", адаптировать их к современным условиям и сделать адекватными нуждам разработчиков и пользователей программного обеспечения, и была проделана значительная работа по интерпретации и развитию положений этого стандарта. В результате возник целый ряд сопутствующих "Оранжевой книге" документов, многие из которых стали ее неотъемлемой частью. К наиболее часто упоминаемым относятся:

"Руководство по произвольному управлению доступом в безопасных системах" (A guide to understanding discretionary access control in trusted systems );

"Руководство по управлению паролями" (Password management guideline);

"Руководство по применению "Критериев безопасности компьютерных систем" в специфических средах" (Guidance for applying the Department Of Defence Trusted Computer System Evaluation Criteria in specific environment);

"Руководство по аудиту в безопасных системах" (A Guide to Understanding Audit in Trusted Systems).

"Руководство по управлению конфигурацией в безопасных системах" (Guide to understanding configuration management in trusted systems).

Количество подобных вспомогательных документов, комментариев и интерпретаций значительно превысило, объем первоначального документа, и в 1995 г. Национальным центром компьютерной безопасности США был опубликован документ под названием "Интерпретация критериев безопасности компьютерных систем", объединяющий все дополнения и разъяснения.