Уровень конфиденциальности, категории конфиденциальности и целостность: что есть что, и как с этим работать?

Данная статья не является частью официальной документации и представлена как пояснительный материал.

Данная статья применима к:

- ОС СН Смоленск 1.6;
- ОС СН Ленинград 8.1.

Система защиты информации (далее - СЗИ) ОС СН Смоленск оперирует следующими мандатными атрибутами:

- Иерархический уровень конфиденциальности (далее по тексту- уровень конфиденциальности);
- Неиерархическая категория конфиденциальности (далее по тексту- категории конфиденциальности);
- Неиерархический уровень целостности (далее по тексту - уровень целостности);
- Мандатные атрибуты управления доступом (в данной статье не рассматриваются).

Что есть что в этом списке, в чем сходство, и в чем различие?

«Уровни» и «категории» конфиденциальности, «целостность» — в чем различия?

Первые два атрибута (**уровень конфиденциальности** и **категория конфиденциальности**) отвечают за то , чтобы информация не попадала к тому, кто не уполномочен её получать.

Уровень конфиденциальности

Классический пример **уровней конфиденциальности** - это степени повышающейся секретности документов (сущностей) "Не секретно" - "ДСП" - "Секретно" - "Совершенно секретно",
и соответствующие им уровни доступа к этим документам, назначенные персоналу (субъектам).

Очевидно, что в такой системе персоналу с уровнем доступа, например, "ДСП", разрешено читать только документы уровней "ДСП" и "Не секретно", и запрещено читать документы с более высокими уровнями конфиденциальности ("Секретно" и "Совершенно секретно").

Не столь очевидно, но персоналу с уровнем конфиденциальности, например "Секретно",
запрещено передавать (преднамеренно или случайно) персоналу с более низким уровнем доступа "ДСП" документы уровня "Секретно"
(теоретические подробности можно найти в многочисленных описаниях модели безопасности Белла-ЛаПадулы (англ. Bell-LaPadula).

Категории конфиденциальности

Для более точного управления доступом, в дополнение к разделению по уровням конфиденциальности,
СЗИ предоставляет возможность разделить материалы по **категориям конфиденциальности**.

Простой пример категорий конфиденциальности имеется в Руководстве по СЗИ ОС СН Смоленск 1.6, п. 4.8.10.7: использование двух категорий "Танки" и "Самолёты".
При этом, персонал, работающий с "Танками", и имеющий соответствующую категорию конфиденциальности, не сможет ни получать сведения о "Самолётах", ни передавать сведения о "Танках" тем, кто работает с "Самолётами",
но, в то же время, условному "Руководителю" могут быть предоставлены одновременно обе категории конфиденциальности, чтобы "Руководитель" мог получать полный объём информации.

Итак, с помощью параметров **уровень конфиденциальности** и **категории конфиденциальности** СЗИ обеспечивает защиту от несанкционированной передачи информации:

- Невозможность прочитать информацию, к которой не предоставлен доступ:
  - "нижним" уровням запрещено читать информацию с "верхних" уровней;
  - всем запрещено читать информацию, на которую нет разрешенной категории конфиденциальности;
- Невозможность передать информацию тому, кому не предоставлен доступ:
  - "верхним" уровням запрещено записывать свою информацию на "нижние" уровни;
  - всем запрещено передавать информацию тем, у кого нет соответствующей категории конфиденциальности.

Правила, по которым СЗИ определяет возможность доступа к данным, описаны ниже.

Целостность

Атрибут **уровень целостности** отвечает за то, чтобы информацию не могли изменять те, кому не положено её изменять.

И, в первую очередь, атрибут **уровень целостности** отвечает за безопасность самой информационной системы.

Пример для пояснения:

> Модель контроля целостности с 2007 г. реализуется в механизме MIC (Mandatory Integrity Control) всех ОС семейства Microsoft Windows, где показала свою эффективность при противодействии компьютерным вирусам и атакам, направленным на несанкционированное повышение привилегий.

(теоретические подробности модели контроля целостности можно найти в описаниях модели безопасности Биба (англ. Biba)).

В общем, требование защиты целостности выглядит так:

- Субъект (процесс или пользователь), работающий на некотором уровне целостности, может записывать (изменять) только сущности (объекты) своего, или более низкого уровня (запись "вверх" запрещена).

В СЗИ ОС СН Смоленск начиная с версии 1.5 была реализована двухуровневая модель целостности,
далее, начиная с ОС СН Смоленск версии 1.6 и в ОС СН Ленинград 8.1, модель целостности расширена до многоуровневой.

Правила, по которым СЗИ определяет возможность доступа к сущностям при работе с контролем целостности, также описаны ниже.

Сущности мандатного управления доступом

Система мандатного управления доступом работает со следующими понятиями:

- Субъекты мандатного доступа (пользователь, процесс) - те, кто выполняет операции, подлежащие мандатному контролю;
- Сущности (объекты) мандатного доступа (файл, каталог и т.д.) - то, с чем выполняются операции, подлежащие мандатному контролю.

и определяет условия, при которых субъектам разрешено выполнять операции с сущностями (создавать, получать доступ к содержимому, изменять).

Каждому субъекту и каждой сущность назначаются определённые мандатные атрибуты (или не назначаются никакие, что приравнивается к минимальным (нулевым) мандатным атрибутам).
Мандатные атрибуты субъекта/сущности объединяются в мандатный контекст этого субъекта/сущности.

Решение о возможности или невозможности выполнения операций доступа автоматически принимается СЗИ на основании сравнения меток безопасности субъекта и сущности.

Мандатный контекст, метка безопасности, мандатные атрибуты управления доступом

См. Метка безопасности: структура и состав

Атрибуты мандатного управления доступом

- **Иерархический уровень конфиденциальности (уровень конфиденциальности)** - единичное (скалярное) числовое значение (иногда называется "уровень секретности" или просто "уровень").
  Каждой метке безопасности (классификационной метке в составе метки безопасности) в каждый момент времени может быть назначен один и только один уровень конфиденциальности.
  Числовые значения уровня конфиденциальности сущности:
  - Все сравнимы между собой;
  - Могут находится в диапазоне 0 до 255, включая границы;
  - Технически реализованы как 8-ми битная беззнаковая величина (uint8_t);
  - В пользовательских интерфейсах представляются десятичным значением или наименованием единичного уровня конфиденциальности;

- **Теоретически,** множество возможных значений уровня конфиденциальности сущности представляет собой **линейное упорядоченное множество относительно операции сравнения.**

- **Неиерархические категории конфиденциальности (категории конфиденциальности)** - маска, состоящая из набора единичных значений категорий конфиденциальности (так же применяются название просто "категория") .
  В ОС СН Astra Linux SE реализовано использование до 64-х единичных категорий конфиденциальности, таким образом, каждой метке безопасности (классификационной метке в составе метки безопасности)
  в каждый момент времени могут быть назначены одновременно до 64-х категорий конфиденциальности. Единичные категории конфиденциальности несравнимы между собой.
  Числовые значения категории конфиденциальности сущности:

  - **Частично** сравнимы между собой;
  - Определяются как суммы значений назначенных единичных категорий конфиденциальности;
  - Могут принимать значения от 0 до 0xFFFF FFFF FFFF FFFF, включая границы;
  - Технически реализованы как 64-х битная маска, беззнаковая величина (unsigned long long);
  - В пользовательских интерфейсах представляются шестнадцатеричным значением или списком наименований единичных категорий конфиденциальности;
  - **Теоретически,** множество возможных значений категорий конфиденциальности сущности представляет собой **полное частично упорядоченное множество относительно операции сравнения.**

- **Неиерархический уровень целостности (уровень целостности)** - маска, состоящая из набора единичных значений уровней целостности (так же применяется название "категория целостности", или просто "целостность").
  В ОС СН Astra Linux SE по умолчанию определены 7 ненулевых и несравнимых между собой единичных значений уровня целостности
  (при настройке ОС СН Astra Linux SE количество единичных значений может быть увеличено до 8):

№ п/п	Значение	Битовая маска	Комментарий
	000	0000 0000	Нулевой уровень. "Низкий", или "Low"
1	001	0000 0001	Уровень задействован как "Сетевые сервисы"
2	002	0000 0010	Уровень задействован как "Виртуализация"
3	004	0000 0100	Уровень задействован как "Специальное ПО"
4	008	0000 1000	Уровень задействован как "Графический сервер"
5	016	0001 0000	Свободен, может быть использован для СУБД
6	032	0010 0000	Свободен, может быть использован для сетевых сервисов
7	064	0100 0000	Зарезервирован, и может быть использован при поднятии max_ilev
8	128	1000 0000	Зарезервирован, и может быть использован при поднятии max_ilev

  Дополнительно зарезервировано специальное наименование уровня целостности "Высокий" ("High").
  Уровень "Высокий" не является единичным уровнем, а представляет собой максимальную сумму единичных уровней, определённых в системе (имеет значение 63 при использовании 6-ти уровней, или значение 255 при использовании 8-ми уровней целостности).

  Таким образом, каждой метке безопасности (метке целостности в составе метки безопасности) в каждый момент времени могут быть назначены одновременно до 6-ти (8-ми) единичных уровней целостности.
  Числовые значения уровня целостности сущности:

  - **Частично** сравнимы между собой;
  - Определяются как суммы значений назначенных единичных уровней целостности;
  - Могут принимать значения от 0 до 63 (255), включая границы;
  - Технически реализованы как 8-ми битная маска, беззнаковая величина (uint8_t);
  - В пользовательских интерфейсах представляются десятичным значением или наименованием единичного уровня целостности;
  - **Теоретически,** множество возможных значений уровня целостности сущности представляет собой **полное частично упорядоченное множество относительно операции сравнения.**

Далее в тексте под терминами "уровень целостности" и "категория конфиденциальности" будут пониматься значения соответствующих мандатных атрибутов,
являющиеся суммами соответствующих единичных значений.

Сравнение мандатных атрибутов

Операции сравнения уровней конфиденциальности, категорий конфиденциальности уровней целостности определяются следующим образом:

- Уровень конфиденциальности cL_0 больше или равен уровню конфиденциальности cL_1 ($cL_0 >= cL_1$),
  если численное значение cL_0 больше или равно численному значению cL_1;

- Категории конфиденциальности C_0 больше или равны категориям конфиденциальности C_1 ($C_0 >= C_1$),
  если все биты набора C_1 являются подмножеством набора бит C_0 или наборы совпадают.
  В терминах побитовых операций: `(C0 & C1) == C1`;
- Уровень целостности iL_0 больше или равен уровню целостности iL_1 ($iL_0 >= iL_1$),
  если все биты набора iL_1 являются подмножеством набора бит iL_0 или наборы совпадают.
  В терминах побитовых операций: `(iL0 & iL1) == iL1`.

Разрешения на доступ

Пусть метка безопасности субъекта содержит следующие атрибуты:

- Классификационная метка:
  - Уровень конфиденциальности $cL_{суб}$;
  - Категории конфиденциальности $C_{суб}$;
- Метка целостности:
  - Уровень целостности $iL_{суб}$.

а метка безопасности сущности содержит атрибуты:

- Метка конфиденциальности:
  - Уровень конфиденциальности $cL_{об}$;
  - Категории конфиденциальности $C_{об}$;
- Метка целостности
  - Уровень целостности $iL_{об}$.

Тогда:

- Операция записи разрешена, если
  $cL_{суб} = cL_{об}$, $C_{суб} = C_{об}$ и $iL_{суб} >= iL_{об}$,
  то есть: уровни конфиденциальности и категории конфиденциальности субъекта и сущности совпадают,
  и уровень целостности субъекта не ниже уровня целостности сущности
  (теоретически - значение $iL_{суб}$ принадлежит верхнему множеству $iL_{об}$);

- Операции чтения и исполнения разрешены, если
  $cL_{суб} >= cL_{об}$ и $C_{суб} >= C_{об}$,
  то есть: уровень конфиденциальности субъекта не ниже уровня конфиденциальности сущности,
  единичные категории конфиденциальности сущности входят в единичные категории конфиденциальности субъекта,
  и разрешение не зависит от значений уровней целостности $iL_{суб}$ и $iL_{об}$
  (теоретически - значения $cL_{суб}$ и $C_{суб}$ принадлежат верхним множествам $cL_{об}$ и $C_{об}$ соответственно) .

Правила наследования и изменения

- Если субъект создаёт другого **субъекта** (например, процесс создаёт процесс)**,**
  то созданный субъект **полностью наследует метку безопасности** родителя,
  т.е. наследует и уровень конфиденциальности, и категории конфиденциальности, и уровень целостности **;**

- Если субъект создаёт **сущность** (например, процесс создаёт файл)**,**
  то созданная сущность **наследует только классификационную метку** родителя,
  т.е. наследует только уровень конфиденциальности и категории конфиденциальности,
  и, независимо от уровня целостности родителя, всегда **получает нулевой уровень целостности**;

- Изменять метку конфиденциальности сущности (т.е. изменять уровень конфиденциальности *и/или* категории конфиденциальности)
  могут только субъекты с наличием привилегии PARSEC_CAP_CHMAC;

- Изменять метку целостности сущности (т.е. изменять уровень целостности сущности)
  могут только субъекты с наличием привилегии PARSEC_CAP_CHMAC и с максимальным ("Высоким") уровнем целостности.