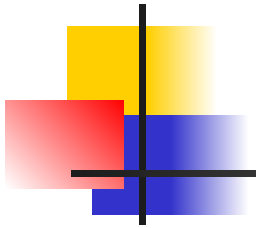
СТРАТЕГИИ, МОДЕЛИ И СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ИНФОРМАЦИОННУЮ СИСТЕМУ ФИРМЫ

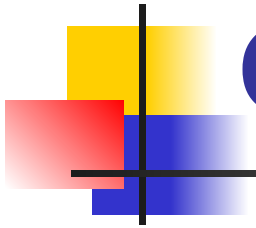
Борисов В.А.
КАСК – филиал ФГБОУ ВПО РАНХ и ГС
Красноармейск 2011 г.



Стратегии обеспечения ИБ фирм

Стратегия безопасности

- Подразумевает множество условий, при которых пользователи системы могут получить доступ к информации и ресурсам, и определяет требования, которые должны быть выполнены при разработке конкретной системы.

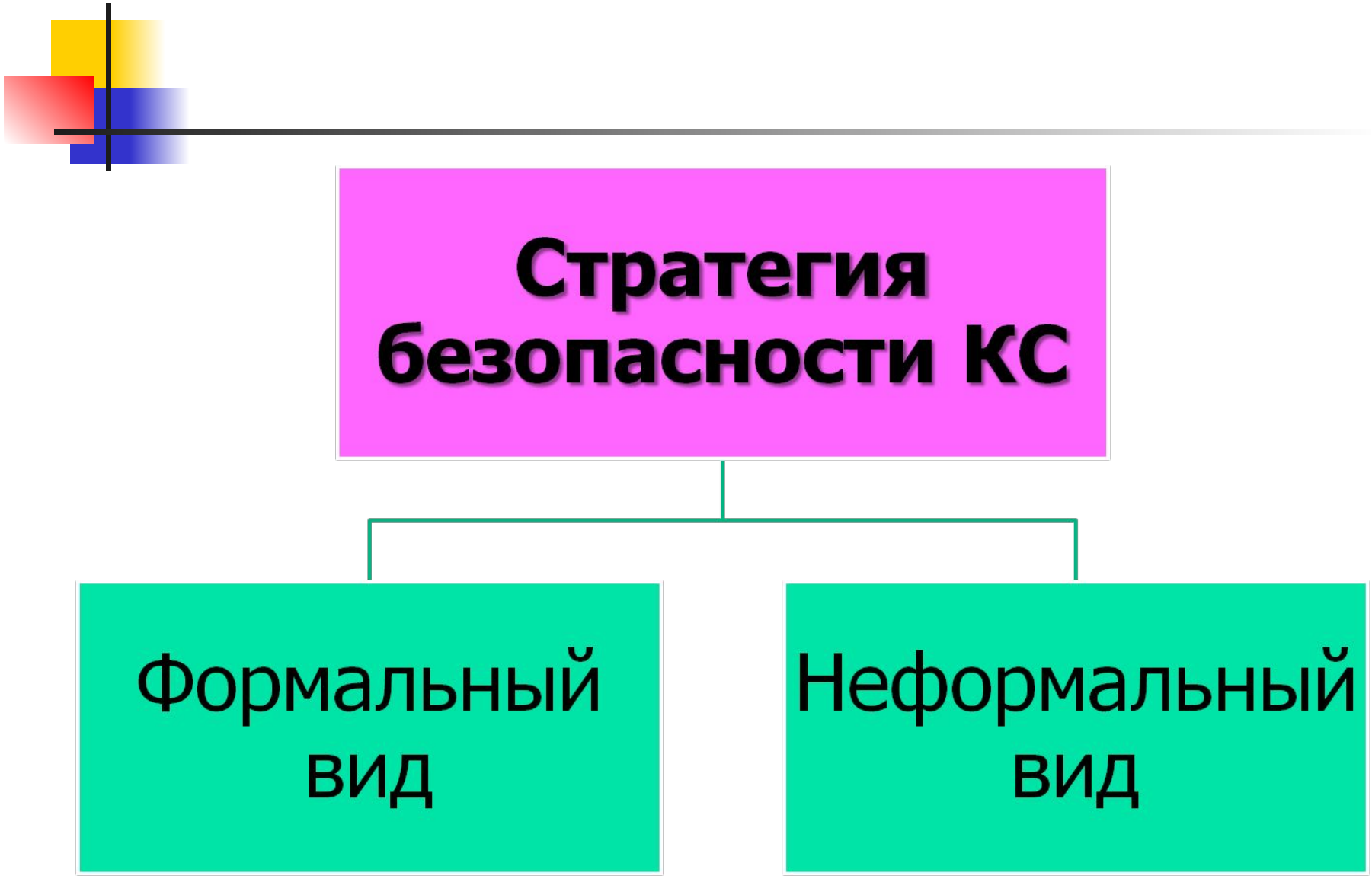


Стратегия безопасности

- Множество процедур, технологий и требований к конкретной системе.

Модель безопасности (МБ)

- Абстрактное описание поведения целого класса систем без рассмотрения конкретных деталей их реализации.


Стратегия безопасности КС
Формальный вид
Неформальный вид

Неформальные СБ

- Описание правил доступа субъектов к объектам в виде таблиц.

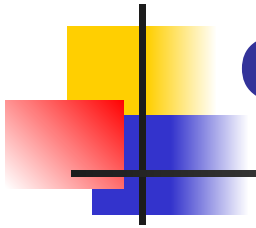
Неформальные СБ

Преимущества

- Легче для понимания малоквалифицированными пользователями и разработчиками.

Недостатки

- Легче допустить логические ошибки, а более сложные выражения будет затруднительно представить в табличной форме.



Формальные СБ

- В их основе лежат модели безопасности.

Преимущества формальной СБ

- Отсутствие противоречий в СБ и возможность теоретического доказательства безопасности системы при соблюдении всех условий СБ.

Группы моделей безопасности

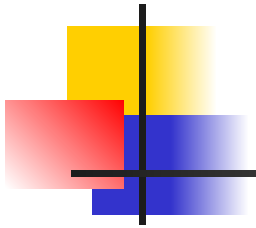
- разграничения доступа и мандатные модели;
- контроля целостности;
- отказа в обслуживании;
- анализа безопасности программного обеспечения (ПО);
- взаимодействия объектов вычислительной сети (ВС).

Противодействие разрушающим программным средствам (РПС)

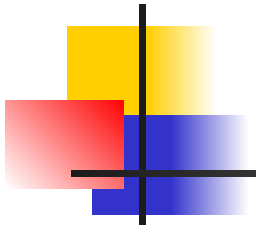
- создание специальных программных средств, предназначенных для поиска и ликвидации конкретных видов РПС;
- проектирование ВС, архитектура и МБ которых либо не допускает существование РПС, либо ограничивает область их активности и возможный ущерб;
- создание и применение методов и средств анализа ПО на предмет наличия в них угроз ИБ ВС и элементов РПС.

Анализ безопасности ПО

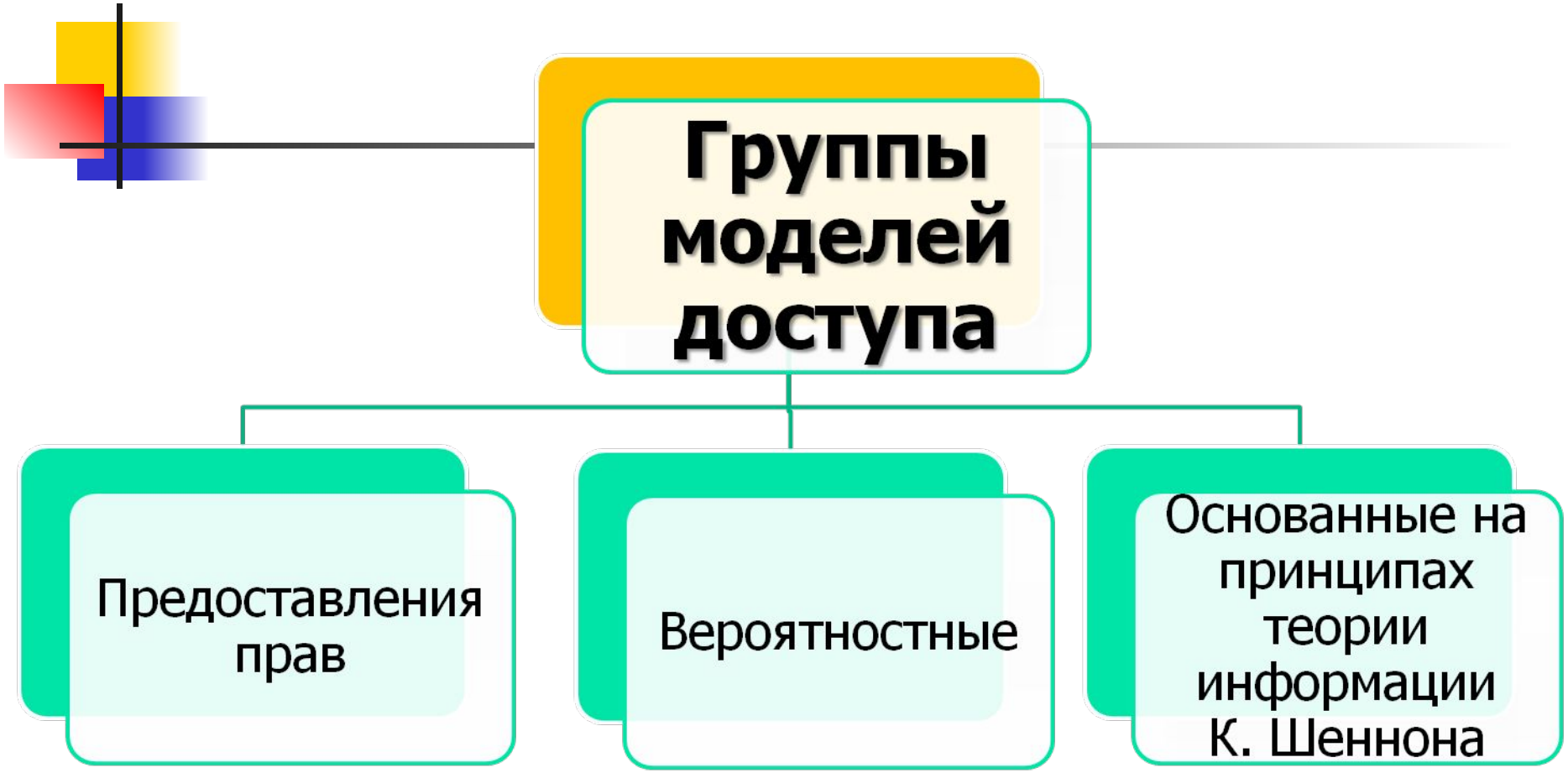
- Процедура анализа программного обеспечения на наличие в них угроз ИБ ВС.

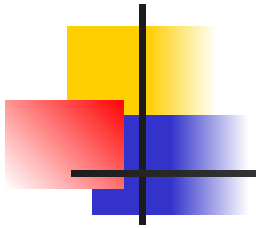


Модели безопасности по разграничению доступа в систему



- Наиболее важными являются характеристики множества субъектов и объектов системы, по которым доступа могут быть классифицированы модели разграничения.

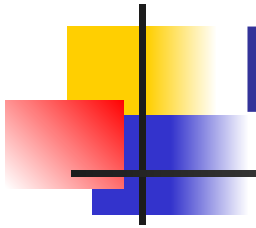

Группы моделей доступа
Предоставления прав
Вероятностные
Основанные на принципах теории информации К. Шеннона



Система передачи военных сообщений

Классификация

- Обозначение, накладываемое на информацию, которое отражает ущерб, причиненный неавторизованным доступом.



Решетка

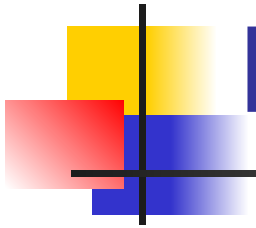
- Множество классификаций и отношение между ними.

Степень доверия пользователю

- Уровень благонадежности персоны.

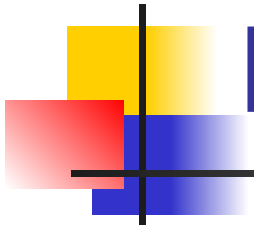
Пользовательский идентификатор (login)

- Строка символов, используемая для того, чтобы отметить пользователя системы.



Пользователь

- Персона, уполномоченная для использования системы.

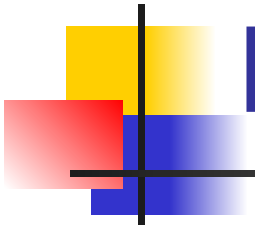


Роль

- Работа, исполняемая пользователем.

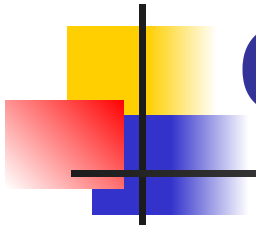
Объект

- Одноуровневый минимальный блок информации в системе, который имеет классификацию.



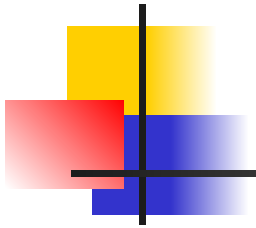
Контейнер

- Многоуровневая информационная структура, которая имеет классификацию и может содержать объекты и другие контейнеры.

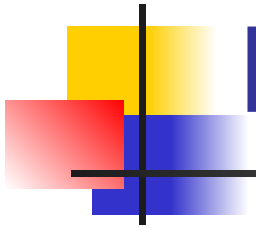


Сущность

- Объект или контейнер.

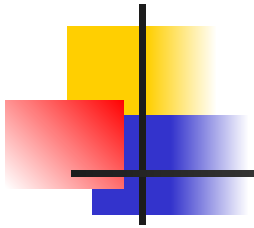


- Требование степени доверия — атрибут некоторых контейнеров.

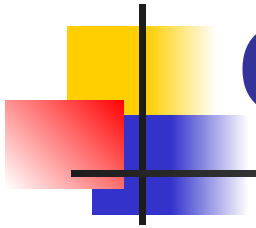


Идентификатор (ID)

- Имя сущности без ссылки на другие сущности.



- Ссылка на сущность прямая, если это идентификатор сущности.
- Ссылка на сущность косвенная, если это последовательность двух или более имен сущностей.

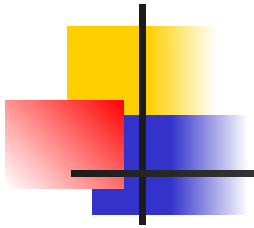


Операция

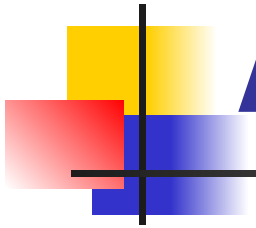
- Функция, которая может быть применена к сущности.

Множество доступа

- Множество троек (пользовательский идентификатор или роль, операция, индекс операнда), которое связано с сущностью.



Ограничения безопасности

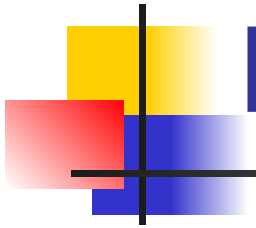


Авторизация

- Пользователь может запрашивать операции над сущностями, только если пользовательский идентификатор или текущая роль присутствуют в множестве доступа сущности вместе с этой операцией и со значением индекса, соответствующим позиции операнда, в которой сущность относят к требуемой операции.

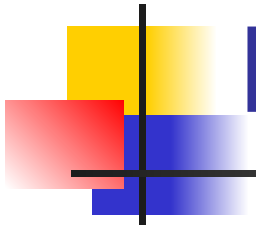
Классификационная иерархия

- Классификация контейнера всегда больше или равна классификации сущностей, которые он содержит.



Изменения в объектах

- Информация, переносимая из объекта, всегда наследует классификацию данного объекта.



Просмотр

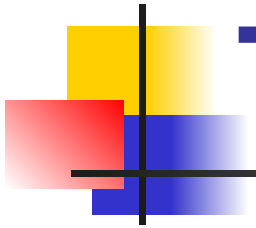
- Пользователь может просматривать только сущности с классификацией меньше, чем классификация устройства вывода и степень доверия к пользователю.

Доступ к объектам, требующим степени доверия

- Пользователь может получить доступ к косвенно адресованной сущности внутри объекта, требующего степени доверия, только если его степень доверия не ниже классификации контейнера.

Преобразование косвенных ссылок

- Пользовательский идентификатор признается законным для сущности, к которой он обратился косвенно, только если он авторизован для просмотра этой сущности через ссылку.



Требование меток

- Сущности, просмотренные пользователем, должны быть помечены его степенью доверия.

Установка степеней доверия, ролей, классификации устройств

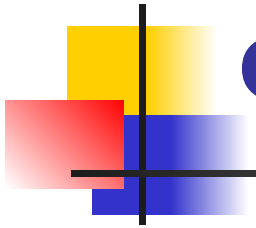
- Только пользователь с ролью офицера безопасности системы может устанавливать данные значения.

Понижение классификации информации

- Никакая классифицированная информация не может быть понижена в уровне своей классификации, за исключением случая, когда эту операцию выполняет пользователь с ролью «пользователь, уменьшающий классификацию информации».

Уничтожение информации

- Операция уничтожения информации проводится только пользователем с ролью «пользователь, уничтожающий информацию».



Формальная модель

- Является базисом для спецификации и реализации системы.

Модель защищенности сети

- Дает описание требования безопасности для построения защищенной сети.

Предположения безопасности модели сети

- На хостах сети существует надежная схема пользовательской аутентификации.
- Каждый пользователь и процесс в сети имеет уникальный идентификатор.
- Только пользователь с ролью «офицер безопасности сети» может присваивать классы безопасности субъектам и компонентам сети и роли пользователям.

Предположения безопасности модели сети

- Все сущности сети имеют сравнимые классы безопасности.
- Имеет место надежная передача данных по сети.
- В сети реализована надежная криптозащита.

Вероятностные модели

- Исследуют вероятность преодоления системы защиты за определенное время.

Вероятностные модели

Достоинства

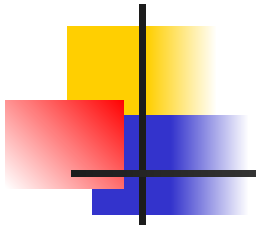
- числовая оценка стойкости системы защиты.

Недостатки

- изначальное допущение того, что система защиты может быть вскрыта.

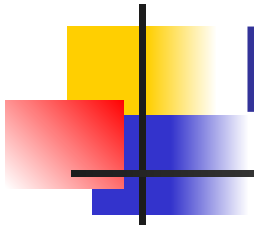
Задача вероятностных моделей

- Минимизация вероятности преодоления системы защиты.



Вероятностные модели

- Игровая модель
- Модель системы безопасности с полным перекрытием



Игровая модель

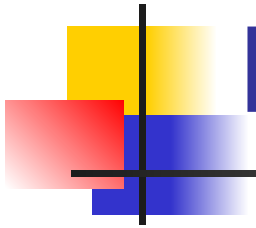
- Описывает процесс эволюции системы защиты в течение времени.

Модель системы безопасности с полным перекрытием

- Система, в которой имеются средства защиты на каждый возможный путь проникновения.

Модели, основанные на принципах теории информации К.Шеннона

- Определяют ограничения на отношение ввода/вывода системы.

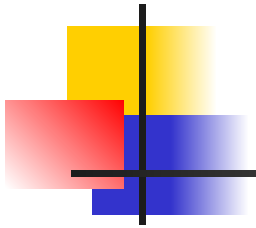


Модель невмешательства

- Ввод высокоуровневого пользователя не может смешиваться с выводом низкоуровневого.

Модель невыводимости

- Требует, чтобы низкоуровневые пользователи не были способны использовать доступную им информацию для получения высокоуровневой информации.



Модели контроля целостности информации в системе

Основные правила мандатной модели целостности

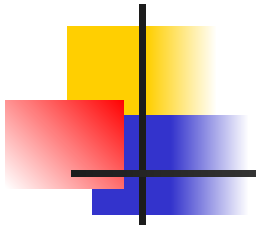
- Правило «нет чтения снизу» определяется как запрет субъектам на чтение информации из объекта с более низким уровнем целостности.
- Правило «нет записи наверх» определяется как запрет субъектам на запись информации в объект с более высоким уровнем целостности.

Модель понижения уровня субъекта

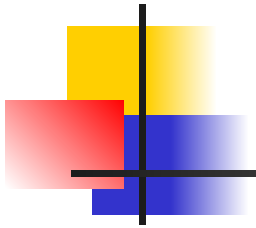
- Разрешает осуществлять чтение снизу, но в результате такого чтения уровень целостности субъекта понижается до уровня целостности объекта.

Модель понижения уровня объекта

- Разрешает запись наверх, но снижает уровень целостности объекта до уровня целостности субъекта, осуществлявшего запись.



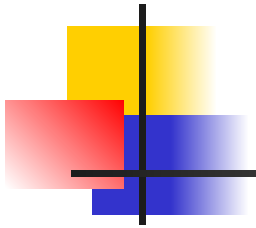
Модели защиты при отказе в обслуживании



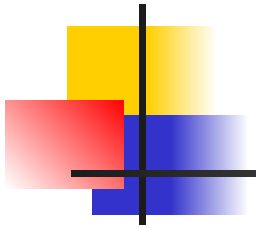
- Монитор пересылок безопасных вычислительных систем служит промежуточным звеном при запросе услуг пользователями.

Модель детального распределения ресурсов (модель Миллена)

- Предполагает, что для выполнения нужного задания субъектам необходимы определенные пространственные и временные требования к ресурсам.



Модели анализа безопасности ПО и безопасности взаимодействия объектов ВС



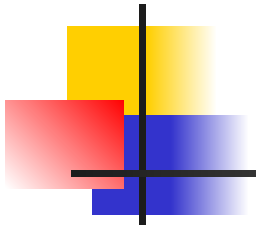
- Наиболее перспективным с точки зрения анализа безопасности представляется объектно-ориентированный подход, рассматривающий РПС как сущности, обладающие определенной структурой и свойствами, вступающие во взаимодействие с другими элементами ВС, такими как программы и данные.

Легитимные действия

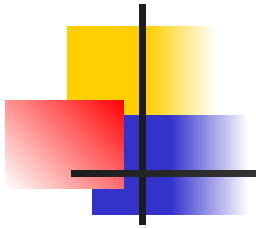
- Действия программы или пользователя, не приводящие к ущербу безопасности и целостности системы.

Нелегитимные действия

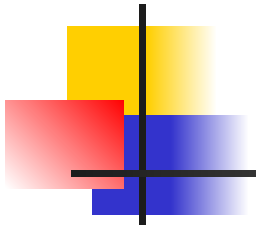
- Действия программы или пользователя, наносящие ущерб безопасности или целостности системы.



- Отличие понятия легитимности отношений от СБ состоит в том, что СБ служит упрощенной моделью реального распределения ролей пользователей и функций программ в системе.



Модель безопасности взаимодействия объектов ВС



- Сетевая ОС Novell Netware является модной и распространенной операционной системой для локальных сетей.

Нарушения безопасности

- выбор модели безопасности, несоответствующей назначению или архитектуре ВС;
- неправильное внедрение МБ;
- отсутствие идентификации и (или) аутентификации субъектов и объектов;
- отсутствие контроля целостности средств обеспечения безопасности;

Нарушения безопасности

- ошибки, допущенные в ходе программной реализации систем обеспечения безопасности;
- наличие средств отладки и тестирования в конечных продуктах;
- ошибки администрирования.