Лекция №2

Распространение объектно-ориентированного подхода на информационную безопасность

Вопросы темы:

1. Основные понятия объектно-ориентированного подхода
2. Применение ООП к рассмотрению защищаемых систем
3. Недостатки традиционного подхода к ИБ с объектной точки зрения

1. Основные понятия объектно-ориентированного подхода

В настоящее время в ИБ пока не нашли отражения основные положения объектно-ориентированного подхода, ставшего основой при построении современных информационных систем. Не учитываются в ИБ и достижения в технологии программирования, основанные на накоплении и многократном использовании программистских знаний.

Это очень серьезная проблема, затрудняющая прогресс в области ИБ.

- Попытки создания больших систем еще в 60-х годах вскрыли многочисленные проблемы программирования, главной из которых является **сложность создаваемых и сопровождаемых систем**. Результатами исследований в области технологии программирования стали сначала **структурированное программирование**, затем **объектно-ориентированный подход.**
- **Объектно-ориентированный подход** является основой современной технологии программирования.

Структурный подход опирается на **алгоритмическую декомпозицию**, когда выделяются функциональные элементы системы. Основная проблема структурного подхода состоит в том, что он неприменим на ранних этапах анализа и моделирования предметной области, когда до алгоритмов и функций дело еще не дошло.

Объектно-ориентированный подход использует объектную декомпозицию, то есть поведение системы описывается в терминах взаимодействия объектов.

Основные понятия ООП

Класс - это абстракция множества сущностей реального мира, объединенных общностью структуры и поведения.

Объект - это элемент класса, то есть абстракция определенной сущности.

Объекты активны, у них есть не только внутренняя структура, но и поведение, которое описывается так называемыми **методами** объекта.

Важнейшими понятиями ООП являются **инкапсуляция**, **наследование** и **полиморфизм**.

Инкапсуляция - сокрытие реализации объектов (их внутренней структуры и деталей реализации методов) с предоставлением только строго определенных интерфейсов.

Полиморфизм - способность объекта принадлежать более чем одному классу.

Введение этого понятия отражает необходимость смотреть на объекты под разными углами зрения, выделять при построении абстракций разные аспекты сущностей моделируемой предметной области, не нарушая при этом целостности объекта.

Наследование означает построение новых классов на основе существующих с возможностью добавления или переопределения данных и методов.

Наследование является важным инструментом борьбы с размножением сущностей без необходимости.

Общая информация не дублируется, указывается только то, что меняется.

При этом класс-потомок помнит о своих "корнях".

Средства ИБ приходится постоянно модифицировать и обновлять.

Объекты реального мира обладают, как правило, несколькими относительно независимыми характеристиками.

Основные составляющие (характеристики) ИБ - доступность, целостность и конфиденциальность.

2. Применение ООП к рассмотрению защищаемых систем

Проблема обеспечения ИБ - комплексная, защищать приходится сложные системы, и сами защитные средства тоже сложны.

Применяя ООП к рассмотрению защищаемых систем, можно выделить основные уровни:

законодательные меры обеспечения информационной безопасности;

- административные меры (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);

- процедурные меры (меры безопасности, ориентированные на людей);
- программно-технические меры.

Законы и нормативные акты ориентированы на всех субъектов информационных отношений независимо от их организационной принадлежности (это могут быть как юридические, так и физические лица) в пределах страны (международные конвенции имеют даже более широкую область действия)

Административные меры - на всех субъектов в пределах организации.

Процедурные - на отдельных людей (или небольшие категории субъектов).

Программно-технические - на оборудование и программное обеспечение.

При такой трактовке в переходе с уровня на уровень можно увидеть применение наследования (каждый следующий уровень не отменяет, а дополняет предыдущий),

а также полиморфизма (субъекты выступают сразу в нескольких ролях - например, как инициаторы административных мер и как обычные пользователи, обязанные этим мерам подчиняться).

3. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения

Исходя из основных положений ООП, следует признать устаревшим традиционное деление на **активные и пассивные сущности** (субъекты и объекты в привычной для дообъектной ИБ терминологии).

Во-первых, в объектном подходе пассивных объектов нет.

Во-вторых, нельзя сказать, что какие-то программы (методы) выполняются от имени пользователя.

В дообъектной ИБ одним из важнейших требований является **безопасность повторного использования** пассивных сущностей (таких, например, как динамически выделяемые области памяти).

Подобное требование вступает в конфликт с таким фундаментальным принципом, как инкапсуляция. Объект нельзя очистить внешним образом (заполнить нулями или случайной последовательностью бит), если только он сам не предоставляет соответствующий метод.

При наличии такого метода надежность очистки зависит от корректности его реализации и вызова.

Одним из самых прочных стереотипов среди специалистов по ИБ является трактовка операционной системы как **доминирующего средства безопасности**.

В современных ИС, выстроенных в многоуровневой архитектуре клиент/сервер, ОС не контролирует объекты, с которыми работают пользователи, также как и действия самих пользователей, которые регистрируются и учитываются прикладными средствами.

Основной функцией безопасности ОС становится защита возможностей, предоставляемых привилегированным пользователям, от атак пользователей обычных.

Контрольные вопросы:

1. Почему традиционный подход неприемлем к современным средствам ИБ ?
2. Назовите важнейшие составляющие ООП.
3. С точки зрения ООП какие основные уровни можно выделить у ИБ?
4. Каковы недостатки традиционного подхода к ИБ?