## Сакауова Мадина ИС 19-201-34

## Контрольные вопросы

## 1.Принципы классификации систем защиты программного обеспечения (по)

## Средства защиты(СЗ) ПО можно классифицировать по ряду признаков

## По используемому механизму защиты

## По методу установки

## По принципу функционирования

## 2. Классификация систем защиты по по методу установки

## Для производителей ПО удобней всего использовать защиту, устанавливаемую на скомпилированные модули. Но такая защита наименее стойка к атакам. Системы с внедрением СЗ в исходный код неудобны для производителей, так как им приходится обучать персонал работе с СЗ и ряд других неудобств. Лучшим решением является использование СЗ комбинированного типа.

## Системы защиты ПО по методу установки можно подразделить: - на системы, устанавливаемые на скомпилированные модули ПО; - системы, встраиваемые в исходный код ПО до компиляции; - комбинированные.

## Системы первого типа наиболее удобны для производителя ПО, так как легко можно защитить уже полностью готовое и оттестированное ПО (обычно процесс установки защиты максимально автоматизирован и сводится к указанию имени защищаемого файла и нажатию "Enter"), а потому и наиболее популярны. В то же время стойкость этих систем достаточно низка, так как для обхода защиты достаточно определить точку завершения работы "конверта" защиты и передачи управления защищенной программе, а затем принудительно ее сохранить в незащищенном виде.

## Системы второго типа неудобны для производителя ПО, так как возникает необходимость обучать персонал работе с программным интерфейсом (API) системы защиты с вытекающими отсюда денежными и временными затратами. Но такие системы являются более стойкими к атакам, потому что здесь исчезает четкая граница между системой защиты и как таковым ПО.

## +Наиболее живучими являются комбинированные системы защиты. Сохраняя достоинства и недостатки систем второго типа, они максимально затрудняют анализ и дезактивацию своих алгоритмов.

## 3. Классификация систем защиты по по используемым механизмам защиты

## Возможно два подхода решения проблемы защиты ПО. Один – это решение проблемы с помощью технических средств защиты. Включать СЗ в состав ПО. Другой – использование юридической защиты. ПО не содержит технические СЗ, а сопровождается информацией об управлении правами.

## По используемым механизмам защиты СЗ можно классифицировать на:

## системы, использующие сложные логические механизмы; - системы, использующие шифрование защищаемого ПО - комбинированные системы. Системы первого типа используют различные методы и приёмы, ориентированные на затруднение дизассемблирования, отладки и анализа алгоритма СЗ и защищаемого ПО. Этот тип СЗ наименее стоек к атакам, так как для преодоления защиты достаточно проанализировать логику процедур проверки и должным образом их модифицировать.

## +Более стойкими являются системы второго типа. Для дезактивации таких защит необходимо определение ключа дешифрации ПО. Самыми стойкими к атакам являются комбинированные системы.

## 4. Классификация систем защиты ПО по принципу функционирования.

## По принципу функционирования СЗ можно подразделить на: упаковщики/шифраторы;- СЗ от несанкционированного копирования СЗ от несанкционированного доступа (НСД).

## 5. Назначение упаковщиков-шифраторов

## Упаковщики/шифраторы. Их цель защита ПО от анализа его алгоритмов и несанкционированной модификации. Для достижения этого используются алгоритмы компрессии данных; шифрование данных, алгоритмы мутации, запутывание логики программы, приведение ОС в нестабильное состояние на время работы ПО и др.

## 6. Системы защиты от несанкционированного копирования

## СЗ от несанкционированного копирования осуществляют "привязку" ПО к дистрибутивному носителю (гибкий диск, CD ...). Данный тип защит основывается на изучении работы контроллеров накопителей, их физических показателей, нестандартных режимах разбивки, чтения/записи и т.п.

## Системы защиты от копирования можно разделить на следующие группы: привязка к дискете; привязка к компьютеру; привязка к ключу; опрос справочников ограничение использования ПО

## *7. Системы защиты от несанкционированного доступа*

## В защите информации ПК от НСД можно выделить три основных направления:

## пециальные технических средства опознавания пользователя; специальное программное обеспечение по защите информации; специальные средства защиты информации ПК от несанкционированного доступа.

## Системы защиты информации от НСД обеспечивают выполнение следующих функций:

## 1. идентификация, т.е. присвоение уникальных признаков - идентификаторов, по которым в дальнейшем система производит аутентификацию; 2. аутентификация, т.е. установление подлинности на основе сравнения с эталонными идентификаторами; 3. разграничение доступа пользователей к ПЭВМ; 4. разграничение доступа пользователей по операциям над ресурсами (программы, данные и т.д.); 5. администрирование: a. определение прав доступа к защищаемым ресурсам, b. обработка регистрационных журналов, c. установка системы защиты на ПЭВМ, d. снятие системы защиты с ПЭВМ; 6. регистрация событий: a. входа пользователя в систему, b. выхода пользователя из системы, c. нарушения прав доступа; 7. реакция на попытки НСД; 8. контроль целостности и работоспособности систем защиты; 9. обеспечение информационной безопасности при проведении ремонтно-профилактических работ; 10. обеспечение информационной безопасности в аварийных ситуациях. Права пользователей по доступу к программам и данным описывают таблицы, на основе которых и производится контроль и разграничение доступа к ресурсам. Доступ должен контролироваться программными средствами защиты. Если запрашиваемый доступ не соответствует имеющемуся в таблице прав доступа, то системы защиты регистрирует факт НСД и инициализирует соответствующую реакцию.