Тема . Безопасность

Цель защиты обеспечить безопасность программных средств.

Система защиты должна быть многоуровневой, адаптируемой к новым условиям функционирования, и включать в себя совокупность средств, методов и мероприятий.

Для построения системы защиты необходимо:

- выявить уязвимые элементы вычислительной системы;
- выявить угрозы для выделенных элементов;
- сформировать требования к системе защиты;
- выбрать методы и средства, удовлетворяющий предъявляемым требованиям.

Основные виды угроз в ВС:

- несанкционированное использование ресурсов ВС;
- некорректное использование ресурсов ВС;
- проявление ошибок в аппаратных и программных средствах;
- перехват данных в линиях связи;
- несанкционированная регистрация электромагнитного излучения;
- хищение устройств ВС, носителей информации и документов;
- несанкционированное изменение состава компонентов ВС или их выход из строя.

Возможные последствия нарушения защиты:

- получение секретных сведений;
- снижение производительности или остановка системы;
- невозможность загрузки системы с жесткого диска;
- материальный ущерб;
- катастрофические последствия.

Три основные задачи защиты:

- защита информации от хищения;
- защита информации от потери;
- защиты ВС от сбоев и отказов.

Надежность ПО – способность точно и своевременно выполнять возложенные на него функции.

Степень надежности ПО определяется качеством и уровнем автоматизации процесса разработки и организацией сопровождения.

4 уровня комплексной защиты информации в ВС:

- **высший уровень, охватывающий всю территорию расположения ВС;**
- **уровень отдельных сооружений и помещений, где расположены устройства ВС, и линии связи и ними;**
- **уровень компонентов ВС и внешних носителей информации;**
- **уровень технологических процессов хранения, обработки и передачи информации.**

Методы защиты делятся на 4 класса:

- физические;
- аппаратные;
- программные;
- организационные.

Физическая защита применяется в основном на верхнем уровне.

Аппаратная защита входит в состав самой ЭВМ или реализуется с помощью специализированных устройств.

Программная защита реализуется с помощью различных программ.

Организационная защита – совокупность организационно-технических мероприятий, разработка и принятие законодательных актов по вопросам защиты информации, морально-этические нормы использования информации.

Программно-аппаратные методы защиты

- защита от несанкционированного доступа к ресурсам пользователей и программ;
- защита от несанкционированного использования ресурсов при наличии доступа;
- защита от некорректного использования ресурсов;
- внесение структурной, функциональной и информационной избыточности;
- высокое качество разработки программно-аппаратных средств.

Защита от несанкционированного доступа к ресурсам со стороны пользователей и программ реализуется в основном двумя способами:

- **парольная защита;**
- **аутентификация.**

Идентификация **позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя).**

Посредством *аутентификации* вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "*аутентификация*" иногда используют словосочетание "проверка подлинности".

Защита от несанкционированного использования ресурсов при наличии доступа предусматривает следующие варианты:

- **от копирования;**
- **от исследования (программ);**
- **от просмотра (данных);**
- **от модификации;**
- **от удаления.**

Защиту от некорректного использования ресурса выполняют программы ОС, которые должны предусмотреть следующие средства:

- **изолирование друг от друга участков памяти, выделенных различным программам;**
- **защита системных областей внешней памяти;**
- **контроль допустимости команд ЦП.**

Структурная избыточность – резервирование аппаратных компонентов ВС на различных уровнях.

Функциональное резервирование – организация вычислительного процесса так, чтобы функции управления, хранения и обработки информации реализуются несколькими элементами системы.

Информационное резервирование – одноразовое или периодическое копирование наиболее ценной информации.

Многие причины потери информации в процессе работы системы, а также сбоев и отказов связаны с ошибками и неточностями, заложенными на этапах проектирования ВС.