Лабораторная работа №9

Тема «Защита программ от несанкционированной эксплуатации и копирования»

ВЫПОЛНИЛ

Ганевич Андрей

Группа 25-ПО

Задание: исследовать методы защиты программ от несанкционированной эксплуатации и копирования.

Защита от копирования — система мер, направленных на противодействие несанкционированному копированию информации, как правило, представленной в электронном виде (данных или кода [проприетарного программного обеспечения](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BF%D1%80%D0%B8%D0%B5%D1%82%D0%B0%D1%80%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5)). При защите могут использоваться организационные, юридические и технические средства. Преимуществом [технических мер защиты](https://ru.wikipedia.org/wiki/%D0%A2%D0%A1%D0%97%D0%90%D0%9F) является возможность предотвращения несанкционированного копирования. В ряде случаев копирование разрешено законодательством (например, [резервное](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B7%D0%B5%D1%80%D0%B2%D0%BD%D0%BE%D0%B5_%D0%BA%D0%BE%D0%BF%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)).

Защита программного обеспечения – комплекс мер, направленных на защиту программного обеспечения от несанкционированного приобретения, использования, распространения, модифицирования, изучения и воссоздания аналогов.

Защита от несанкционированного использования программ – система мер, направленных на противодействие нелегальному использованию программного обеспечения. При защите могут применяться организационные, юридические, программные и программно-аппаратные средства.

Защита от копирования к программному обеспечению применяется редко, в связи с необходимостью его распространения и установки на компьютеры пользователей. Однако, от копирования может защищаться лицензия на приложение (при распространении на физическом носителе) или его отдельные алгоритмы.

Несанкционированный доступ (НСД) злоумышленника на компьютер опасен не только возможностью прочтения и/или модификации обрабатываемых электронных документов, но и возможностью внедрения злоумышленником управляемой программной закладки, которая позволит ему предпринимать следующие действия:

1. читать и/или модифицировать электронные документы, которые в дальнейшем будут храниться или редактироваться на компьютере;
2. осуществлять перехват различной ключевой информации, используемой для защиты электронных документов;
3. использовать захваченный компьютер в качестве плацдарма для захвата других компьютеров локальной сети;
4. уничтожить хранящуюся на компьютере информацию или вывести компьютер из строя путем запуска вредоносного программного обеспечения.

Программные системы защиты от несанкционированного копирования

Данные системы предотвращают нелицензионное использование программных продуктов и баз данных. Программа выполняется только при опознании некоторого уникального не копируемого ключевого элемента.

Таким ключевым элементом могут быть:

1. дискета, на которой записан не подлежащий копированию ключ;
2. определенные характеристики аппаратуры компьютера;
3. специальное устройство (электронный ключ), подключаемое к компьютеру и предна­значенное для выдачи опознавательного кода. Программные системы защиты от копирования программных продуктов:
4. идентифицируют среду, из которой будет запускаться программа;
5. устанавливают соответствие среды, из которой запущена программа, той, для которой разрешен санкционированный запуск;
6. вырабатывают реакцию на запуск из несанкционированной среды;

регистрируют санкционированное копирование.

Для идентификации запускающих дискет применяются следующие методы:

1. нанесение повреждений на поверхность дискеты ("лазерная дыра"), которая с тру­дом может быть воспроизведена в несанкционированной копии дискеты;
2. нестандартное форматирование запускающей дискеты.
3. Идентификация среды компьютера обеспечивается за счет:
4. закрепления месторасположения программ на жестком магнитном диске (так называемые неперемещаемые программы);
5. привязки к номеру BIOS (расчет и запоминание с последующей проверкой при за­пуске контрольной суммы системы);
6. привязки к аппаратному (электронному) ключу, вставляемому в порт ввода-вывода, и др.