## 2.2. Преднамеренные угрозы безопасности АИС

### 2.2.1. Программные злоупотребления

Рассмотрим существующие к настоящему времени программные средства, используемые для осуществления несанкционированного доступа и нанесения ущерба АИС.

В качестве потенциальных программных злоупотреблений могут быть восприняты такие программные средства, которые позволяют или допускают возможность реализации следующих злоупотреблений [152, 130]:

- сокрытие признаков своего присутствия в программной среде ЭВМ;

- обладание способностью к самодублированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;

- разрушение (искажение произвольным образом) кодов программ в оперативной памяти;

- сохранение фрагментов информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

- искажение произвольным образом, блокирование и/или подмена выводимого во внешнюю память или в канал связи массива информации, образовавшегося в результате работы прикладных программ, или уже находящихся во внешней памяти массивов данных.

В соответствии с предложенной классификацией программные злоупотребления могут быть разделены по своему назначению на два больших класса: тактические и стратегические (рис.11) [111].

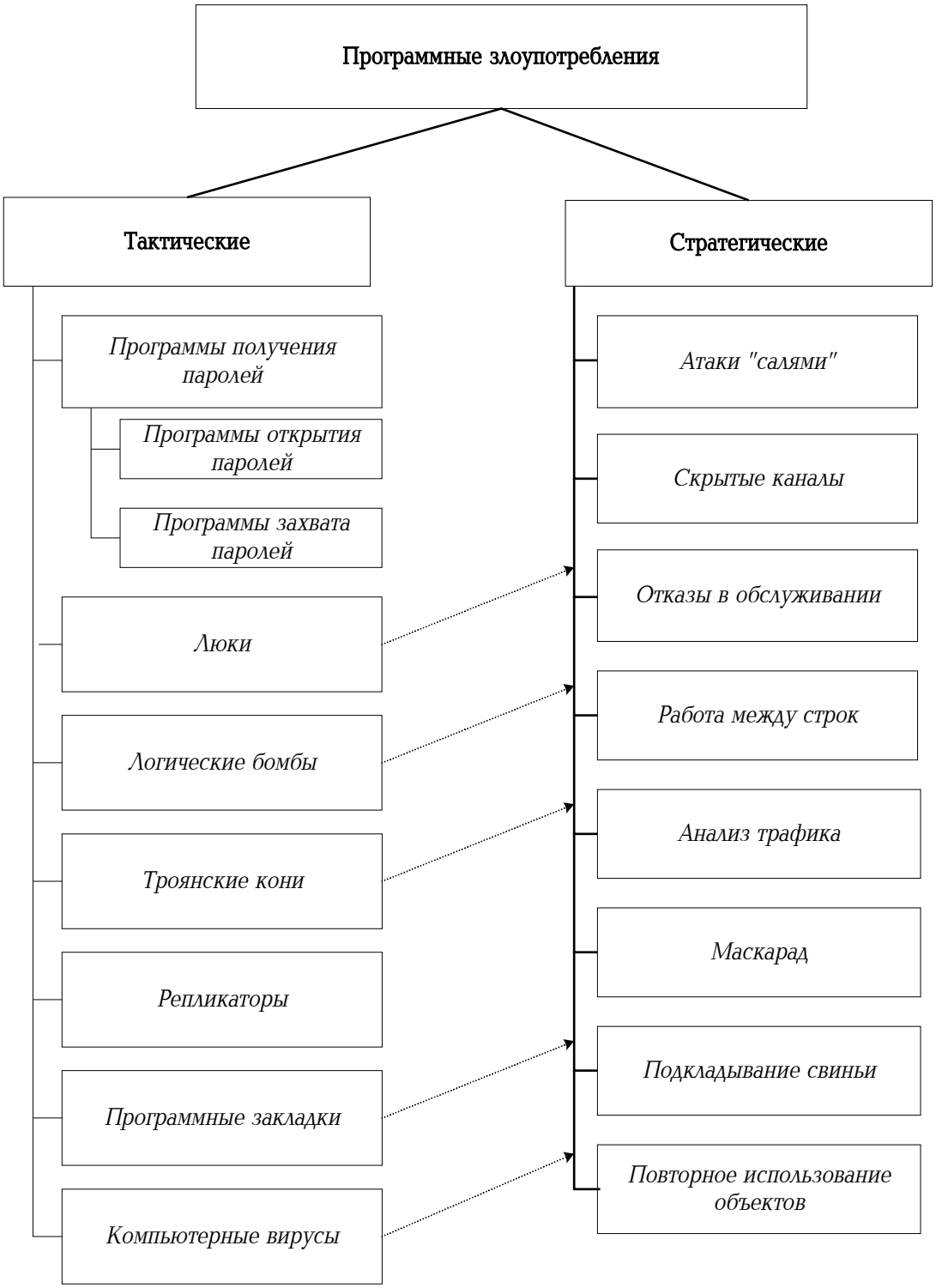


***Рис. 11.*** *Классификация программных злоупотреблений*

Тактические программные злоупотребления предназначаются для достижения ближайших целей: получение паролей,

несанкционированного доступа, разрушения информации и других действий. Тактические программные злоупотребления обычно используются для подготовки и реализации стратегических злоупотреблений. Стратегические программные злоупотребления направлены на реализацию далеко идуших целей и связаны с большими финансовыми потерями для АИС и объекта управления.

Рассмотрим структуру и организацию программных злоупотреблений, используя [152,58,119,30,16,107,174 и др.]. Блок-схемы реализации программных злоупотреблений представлены в приложении 1.

Среди самых распространенных программных злоупотреблений следует выделить: программы получения паролей, логические бомбы, троянские кони, репликаторы, компьютерные вирусы, программные закладки и др.

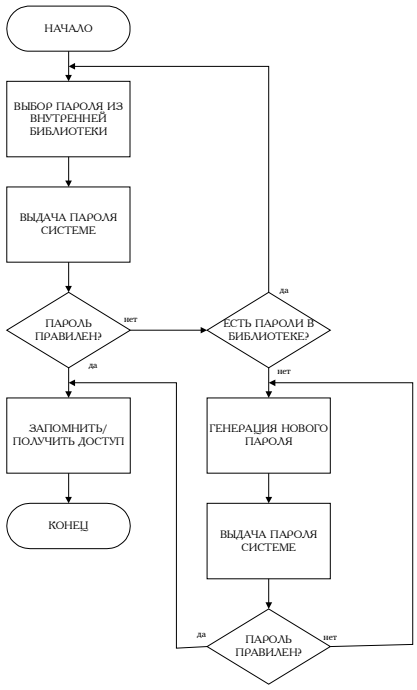


Рис. 12 Логическая схема реализации программ открыытия паролей.

1. *Программы получения паролей* - это две большие группы программ, которые предназначены для получения идентификаторов и паролей пользователей. В [30] с данным злоупотреблением связывается термин “взлом системы”.

*Программы открытия паролей* последовательно генерируют все возможные варианты пароля и выдают их системе до тех пор, пока не будет определен необходимый пароль [109]. Пароли являются основным

средством идентификации пользователей в многопользовательских компьютерных системах и открытие пароля и входного имени пользователя позволяет организовать доступ к конкретной информации. Логическая схема реализации данного злоупотребления представлена на рис. 12

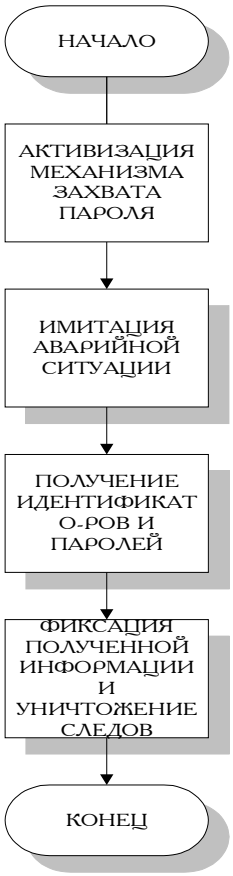


Рис. 13. Логическая схема реализации программ захвата паролей.

*Программы захвата паролей* имитируют системный сбой в работе компьютера (например, перезагрузку операционной системы, отключение сети и др.), и запрашивают у пользователя идентификатор и пароль, после чего передают управление рабочей программе, операционной системе или другим программам [36,30 и др.] (рис.13).

2. “Люки” или “trap door” - не описанные в документации возможности работы с программным продуктом [30,109 и др.]. В [109] автор приравнивает программы открытия паролей к так называемым “люкам”, которые на сегодняшний день формируются в самостоятельную группу злоупотреблений. Логическая схема механизма использования “люков” представлена на рис. 14.

Сущность использования люков состоит в том, что при реализации пользователем не описанных в документации действий, он получает доступ к ресурсам и данным, которые в обычных условиях для него закрыты (в частности, вход в привилегированный режим обслуживания).

“Люки” могут появиться в программном продукте следующими путями:

а) “люки” чаще всего являются результатом забывчивости разработчиков. В процессе разработки программы создаются временные

механизмы, облегчающие ведение отладки за счет прямого доступа к продукту.

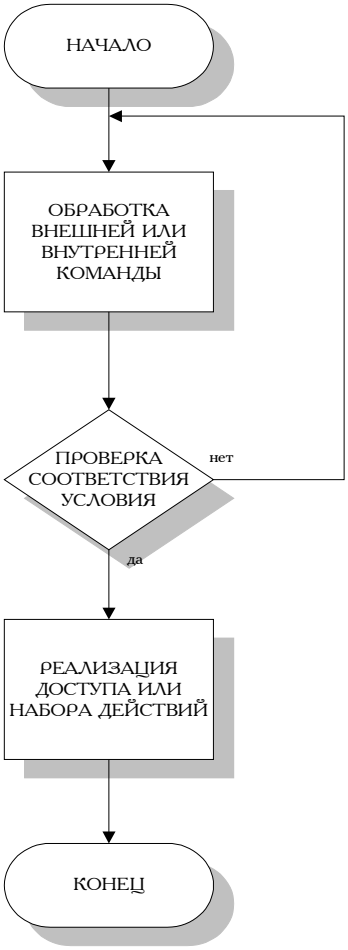


Рис. 14. Логическая схема использования “люков”

Одним из примеров использования забытых люков является инцидент с вирусом Морриса [104]. Одной из причин, обусловившей распространение этого вируса, являлась ошибка разработчика программы электронной почты, входящей в состав одной из версий ОС UNIX, приведшая к появлению малозаметного люка.

b) “люки” могут образоваться также в результате часто практикуемой технологии разработки программных продуктов "сверху-вниз". При этом программист приступает к написанию управляющей программы, заменяя предполагаемые в будущем подпрограммы так называемыми "заглушками" - группами команд, имитирующими или обозначающими место присоединения будущих подпрограмм. В процессе работы данные заглушки заменяются реальными подпрограммами.

На момент замены последней заглушки реальной подпрограммой программа считается законченной. Но на практике подобная замена выполнятся не всегда. Это имеет место из-за нарушения сроков разработки и сдачи в эксплуатацию и, невостребованностью данной подпрограммы, в связи с чем заглушка остается, представляя собой слабое место системы с точки зрения информационной безопасности.

**в)** программист пишет программу, которой можно управлять с помощью определенных команд, или например путем ввода "Y" ("Да") или "N" ("Нет"). А что произойдет, если в ответ на запрос будет вводится "A" или "B" и т.д.? Если программа написана правильно, то на экране должно появиться сообщение типа "Неправильный ввод" и повтор запроса. Однако может быть ситуация, когда программа не учитывает такое, предполагая, что пользователь будет действовать правильно. В таком случае реакция программы на неопределенный ввод может быть непредсказуемой. Такую ситуацию в программе можно специально создать для того, чтобы получить доступ к определенным ресурсам и данным.

Таким образом, “люк” может присутствовать в программном продукте вследствии умышленных или неумышленных действий со стороны программиста для обеспечения тестирования и отладки программного продукта; окончательной сборки конечной программы; скрытого средства доступа к программному продукту и данным.

В первом случае люк - это неумышленная, но серьезная брешь в безопасности системы, во втором - серьезная экспозиция безопасности системы и в третьем случае - первый шаг к атаке системы.

Такие виды нарушений называются trap doors или back doors (в литературе за данными программными злоупотрелениями закрепилось название "задние ворота"). Пример встроенного люка в операционную систему MS-DOS приводится в [78].

**3.** *Логические бомбы* (logic bomb) - программный код, который является безвредным до выполнения определенного условия, после которого реализуется логический механизм [109]. Общая схема механизма реализации логических бомб представлена на рис. 15.

Логические бомбы, в которых срабатывание скрытого модуля определяется временем (текущей датой), называют бомбами с часовым механизмом (time bomb). Подобные программы, реализующие свой механизм после конкретного числа исполнений, при наличии или,

наоборот, отсутствии определенного файла, а также соответствующей записи в файле, получили название логической бомбы (logic bomb).

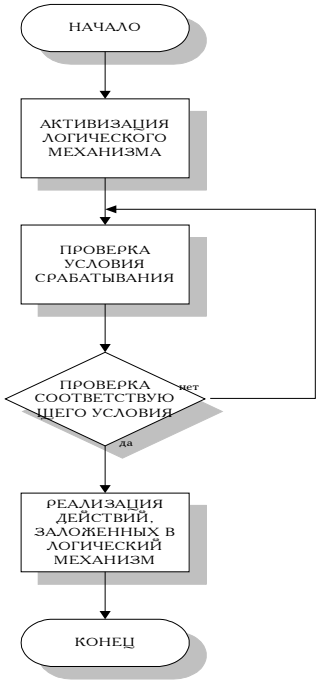


Рис. 15. Общая схема механизма реализации логических бомб

В связи с тем, что подобные программы имеют ограниченный доступ к ресурсам системы, то и разрушительный эффект остается достаточно низким. Опасность может значительно увеличиться, если логическая бомба будет встроена в системное программное обеспечение, что приведет к уничтожению файлов, переформатированию машинных носителей или к другим разрушающим последствиям. Основной целью функционирования программ типа логической бомбы следует считать нарушение нормальной работы компьютерной системы.

4. *"Троянский конь"* - программа, которая кроме своей основной деятельности выполняет некоторые дополнительные (разрушительные), неописанные в документации функции, о чем пользователь не подозревает [30,109 и др.].

Реализация дополнительных функций выполняется скрытым от пользователя модулем, который может встраиваться в системное и прикладное программное обеспечение. При реализации пораженной программы троянский конь получает доступ к ресурсам вместе с пользователем (рис. 16).

Троянские кони значительно опаснее ПЗ, рассмотренных ранее, поскольку чаще всего они встраиваются в хорошо зарекомендовавшие

себя программные продукты - инструментальные средства, пакеты прикладных программ, текстовые редакторы, компьютерные игры и т.д., и выступают в качестве средства несанкционированного доступа к содержащейся в системе информации. В некоторых случаях термином "троянские программы" ошибочно называли программы, содержащие ошибки или плохо спроектированный интерфейс с пользователем.

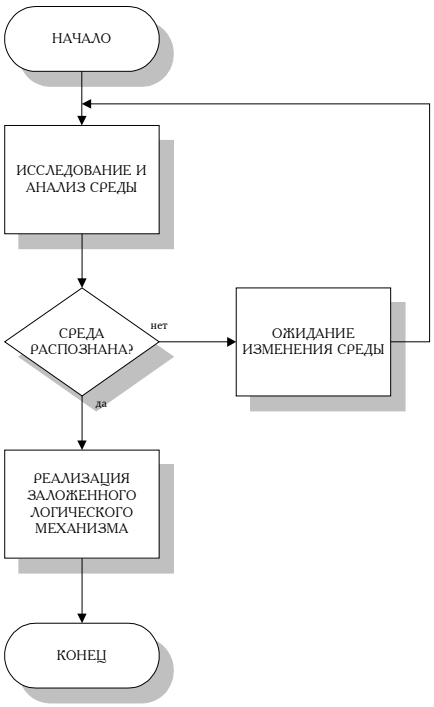


Рис. 17. Общая схема логического механизма реализации троянского коня.

Компьютерные системы, использующие дескрипторные методы управления доступом (в том числе такие,как полномочия, списки управления доступом и др.), становятся практически беззащитными против программ типа троянский конь.

5. *Репликаторы* - могут создавать одну или более своих копий в компьютерной системе. Это приводит к быстрому переполнению памяти компьютера, но данные действия могут быть обнаружены опытным пользователем и достаточно легко устранены. Устранение программы-репликатора усложняется в тех случаях, когда репликация выполняется с модификацией исходного текста программы, что затрудняет распознавание ее новых копий. Репликаторные программы становятся особенно опасными, когда к функции размножения будут добавлены другие разрушающие воздействия.

6. *Программные закладки* - программы, которые сохраняют вводимую с клавиатуры информацию (в т.ч. и пароли) в некоторой зарезервированной для этого области.

Данный тип программных злоупотреблений включает [30,154]:

* закладки, ассоциируемые с программно-аппаратной средой (BIOS);

* закладки, ассоциируемые с программами первичной загрузки находящимися в Master Boot Record или Root секторов активных разделов;

* закладки, ассоциируемые с загрузкой драйверов DOS, командного интерпретатора, сетевых драйверов;

* закладки, ассоциируемые с прикладным программным обеспечением общего назначения (встроенные в клавиатурные или экранные драйверы, программы тестирования, утилиты и оболочки типа Norton Commander);

* исполняемые модули, содержащие только код закладки (как правило, внедряемые в пакетные файлы типа .BAT);

* модули-имитаторы, совпадающие по внешнему виду с программами, требующими ввода конфиденциальной информации;

* закладки, маскируемые под ПС оптимизационного назначения (архиваторы, ускорители и т.д.);

* закладки, маскируемые под ПС игрового и развлекательного назначения (как правило, используются для первичного внедрения закладок типа "исследователь").

7. *Атака "салями"* - характерны для финансовых и банковских информационных систем, где ежедневно проводятся тысячи операций, связанных с безналичными расчетами, переводами сумм, начислениями и т.д. [36, 30, 105]. При реализации расчетов вычисляются различного рода доли, которые округляются в большую или меньшую сторону. Атака "салями" состоит в накоплении на отдельном счете этих долей денежной единицы. Практика показала, что эксплуатация такой программы обеспечивает накопление значительных сумм.

8. *Скрытые каналы* - это программы, передающие информацию лицам, которые в обычных условиях эту информацию получать не должны [30]. Злоумышленник не всегда имеет непосредственный доступ к компьютерной системе. Для скрытой передачи информации

используются различные элементы, форматы "безобидных" отчетов, например, разную длину строк, пропуски между строками, наличие или отсутствие служебных заголовков, управляемый вывод незначащих цифр в выводимых величинах, количество пробелов или других символов в определенных местах отчета и т.д.

При использовании скрытых каналов для получения относительно небольших объемов информации захватчик вынужден проделать достаточно большую работу. Поэтому скрытые каналы более приемлемы в ситуациях, когда нарушителя интересует не сама информация, а факт ее наличия.

Может возникнуть ситуация, когда скрытый канал сообщает о наличии в системе определенной информации, что в свою очередь служит признаком работы в системе определенного процесса, позволяющего провести атаку иного типа.

**9.** ***Компьютерные вирусы (КВ)*** - представляют собой программные разработки, способные проникать в среду компьютерных систем и наносить разного рода повреждения [4,16,30,107,174,141,109 и др.].

Вирусы представляют собой наиболее полно исследованный класс программных злоупотреблений, превосходящий по разрушающим возможностям все другие. Рассмотрим существующие определения КВ.

По определению [174] компьютерный вирус - это участки самовоспроизводящегося кода, который самостоятельно проникает в системное и прикладное программное обеспечение, осуществляет контроль за выполнением пользовательских программ.

В работе [107] приводится несколько отличное определение. Вирус представляет собой программу, которая может модифицировать другую программу, включать в нее свою точную или развитую копию.

Автор [141] определяет компьютерный вирус как специально написанную небольшую по объему программу, которая может "приписывать" себя к другим программам (т.е. "поражать" их), а также выполнять различные нежелательные действия.

В [16] компьютерные вирусы определяются как программы, которые могут создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, сети и т.д. При этом копии сохраняют способность дальнейшего распространения.

Интересным является определение компьютерного вируса в законодательстве штата Техас (США) [108], как посторонняя (нежелательная) компьютерная программа или другого набора инструкций, внесенных в память компьютера, операционную систему или программу, при разработке которых они были специально снабжены способностью к воспроизведению или к воздействию на другие программы и файлы, находящиеся в компьютере путем присоединения дубликата такой посторонней (нежелательной) программы к одной или более компьютерным программам или файлам.

По нашему мнению, компьютерные вирусы можно определить как самовоспроизводящуюся часть человеко-машинной системы, которая преднамеренно выполняет некоторые действия нежелательные для законных пользователей компьютерной системы.

Обобщая приведенные определения, следует отметить, что компьютерный вирус является программой, написанной программистом для достижения определенных целей. Конечной целью функционирования подобной программы не всегда являются только разрушительные действия (уничтожение директорий, секторов загрузки и пользовательских файлов). Они могут использоваться одновременно для выполнения полезной работы (например, для верификации, тестирования и т.д.), что является основой для создания "положительных" вирусов или антивирусов.

Компьютерные вирусы обладают разнообразными свойствами, характеризующими организацию логического механизма, деструктивный механизм и др. Представляется возможным расширить стандартную классификацию [107, 16, 17,174,109,4,117 и др.]. На рис. 12 представлена

классификация компьютерных вирусов, среди которых можно выделить следующие группы:


Рис.12 Классификация вирусов.

*- по среде распространения:*

а) *сетевые* - распространяются по каналам связи, через электронную почту, ввиду этого их называют еще и “червями”.

"Компьютерные черви" (worm) получили распространение исключительно в рамках компьютерных сетей. Типичными представителями данной группы являются Christmas tree в сети EARN (конец 1987 г.) и сетевой вирус Морриса в сети APRANET/INTERNET (ноябрь 1988 г.). Данные программы подобны репликаторным, но в отличие от них активно используют вычислительные ресурсы сетей. Подобные программы представляют собой совокупность сегментов, каждый из которых реализуется на отдельной ЭВМ. Сегменты программы поддерживают связь между собой даже в тех случаях, когда один из сегментов прекращает свое существование, оставшиеся сегменты обращаются к свободной в сети ЭВМ, инициализируют ее с передачей потерянного сегмента и она начинает исполнять данный сегмент.

Программы worm можно рассматривать также как специальный механизм поддержки отдельных сегментов и пользовательских программ. Механизм поддержки включает следующий набор программ: главную программу; программу инициализации первой и последующей ЭВМ; программу поиска свободной ЭВМ; программу, обеспечивающую связь и поддержку отдельных сегментов.

Рассмотрим общую структуру функционирования сетевого вируса. Он состоит из двух основных частей - стартового модуля и набора программ, во главе с главной. После проникновения в память, главная программа осуществляет сбор информации о доступных ЭВМ, входящих в сеть. Для этих целей используются системные функции и вспомогательные программы, а также общедоступные конфигурационные файлы. Затем главная программа осуществляет попытки внедрения стартового модуля в каждую доступную ЭВМ.

Прежде всего выполняется сбор доступной информации об именах и адресах других узлов сети, на основании которой строится список потенциальных пользователей. На данном этапе используются программы открытия паролей и, в случае успешного открытия, выполняется переход к следующему узлу.

б) *спутниковые вирусы.* Называются так по причине их распространения средствами спутниковой связи;

в) *файловые вирусы*- внедряются в выполняемых файлах;

"Истинные" компьютерные вирусы поражают исполняемые пользовательские файлы (обычно с расширениями .COM и .EXE).

В тоже время, в зависимости от реализуемых функций, вирусы могут быть объеденены в следующие три группы:

- загрузочные, поражающие секторы первоначальной загрузки дискет и жестких дисков;
- системные, поражающие системное программное обеспечение;
- пользовательские, поражающие прикладные программы пользователей.

К первой группе относят вирусы, способные поразить загрузочные сектора гибких и жестких дисков во время запуска операционной системы. При загрузке вирус попадает в нулевую дорожку дискеты и превращается в источник поражения для других гибких дисков. Использование пользователями пораженных вирусом дисков является единственным способом распространения данного типа вирусов [109].

Системные программы поражаются путем проникновения вируса в системный модуль или драйвер. Кроме того, вирусы данной группы в состоянии поражать интерпретаторы, системные программы ввода-вывода, программы управления работой периферийных устройств и т.д. При загрузке и инициализации операционной системы вирус совместно с пораженной системной программой получает доступ к системным ресурсам и поражает доступные системные программы, оставаясь при этом резидентным.

Третья группа вирусов (пользовательские) поражает прикладные программы пользователей во время их исполнения, осуществляет поиск новых объектов. Данная группа является наиболее представительной и именно вирусы данного типа наносят наибольший урон. Поражение выполняется путем присоединения к программе, либо проникновения в программу. В первом случае длина пользовательской программы увеличивается на длину вирусного механизма и при использовании контрольной суммы или последовательного просмотра появляется возможность обнаружения и идентификации вируса. Во втором случае вирус находит свободное внутреннее пространство в теле программы и размещает свою копию. Но таким свободным пространством обладают не все программы, поэтому наибольшее распространение получил первый способ. Во всех случаях выполняется замена инструкций пользовательских программ собственными инструкциями вирусного механизма и после реализации логического механизма первоначальные инструкции восстанавливаются и управление передается пользовательской программе.

В отдельную самостоятельную группу следует выделить вирусы, спроектированные по технологии "stealth". Применительно к вирусным механизмам данная технология обеспечивает "невидимость" и "прозрачность" при работе с антивирусными программными продуктами. Существует несколько подходов и точек зрения относительно состава данной группы и средств, затрудняющих их открытие и устранение. В частности, Н.Н.Безруковым в [16], предложены четыре категории таких средств, в зависимости от следующих видов затруднений:

- затруднения при открытии вируса в пораженных файлах. К данной категории относятся следующие средства: кодирование вируса или его составных частей; использование механизма мутации; запись тела вируса в неиспользованных областях пораженных файлов, что не приводит к увеличению длины последних; маскировка увеличения длины пораженных файлов с использованием перехвата соответствующих функций и др.;

- затруднения при открытии вируса в оперативной памяти, что обеспечивается использованием следующих средств: манипуляция контрольными блоками памяти; специальные методы перехвата векторов прерываний; динамическая корректировка объема свободной памяти; динамическое кодирование вируса в памяти и др.;

- маскировка процесса поражения программ с помощью следующих методов: сокрытие оригинальных программ; использование соответствующих прерываний и последующего прямого обращения к их адресам для обхода средств программной защиты;

- использование методов кодирования, которые затрудняют трассировку и дизассемблирование. Вирусы, использующие данные методы кодирования получили название "бронированных". К данным средствам относят: динамическое декодирование вирусом инструкций непосредственно перед исполнением и последующим кодированием; кодирование нескольких уровней с использованием нескольких методов и ключей; использованием вирусом стандартных прерываний, которые используются программами трассировки.

Некоторые специалисты склоны относить к данной группе все вирусы, использующие две и более групп перечисленных средств. В частности, Ф.Скулассон, автор и разработчик наиболее мощного и мобильного антивирусного пакета F-PROT, в качестве критерия выделяет следующие два условия:

- если пораженный объект является файлом, то при просмотре его содержания и активном вирусе в оперативной памяти не отмечается увеличение длины файла;

- при просмотре пораженного файла и при активном вирусе в оперативной памяти объект остается визуально непораженным.

Подобные критерии, по нашему мнению, не всегда могут являться основанием для отнесения того или иного вируса к данной группе. Во-первых, если рассматриавть загрузочные вирусы, то они реализуют два приведенных условия, поскольку функционируют на уровне операционной системы и внимательно осуществляют контроль за поступающими заявками доступа к оригинальному сектору первоначальной загрузки. Во-вторых, большинство файловых вирусов реализуют именно первое условие.

*г) загрузочные (бутовые) вирусы* - внедряются в загрузочный сектор диска (boot sector) или в сектор Master Boot record винчестера. В литературе за данными вирусами закрепилось название “бактерии”.

Бактерии в качестве среды обитания и размножения используют компоненты операционной системы: сектор первоначальной загрузки, командный процессор и др.

- *по способу поражения* различают вирусы*:*

а. *резидентные* - после запуска остаются в оперативной памяти компьютера и заражают другие программы;

б. *нерезидентные* - поражают программы и выполняют другие несанкционированные действия только в момент их запуска.

- *по деструктивным возможностям* известны вирусы:

а. *очень опасные* - приводят к сбоям в системе, уничтожают данные и программы системы.

б. *опасные* - приводят к сбоям в компьютерной системе;

в. *безвредные* - не выполняют никакого иного действия, кроме некоторых видео или звуковых эффектов и самораспространения, тем самым, уменьшая свободную память компьютера;

г. *полезные* - реализуют различные полезные действия, например, архивирование, дефрагментацию файлов и т.д.

- *по способу организации* бывают*:*

а. *"вульгарные вирусы"* - программы подобных вирусов написаны едиными блоками и при поражении их можно обнаружить, локализовать и уничтожить в самом начале эпидемии;

б. *"раздробленные вирусы"* - программа данного вируса разделена на части, на первый взгляд не имеющие между собой связи. Эти части содержат инструкции, которые указывают, как собрать их воедино, чтобы воссоздать и размножить вирус. Таким образом вирус находится в "распределенном" состоянии, лишь на короткое время своей работы собираясь в единное целое.

### 2.2.2 Другие компьютерные злоупотребления

С развитием технологий обработки информации получили распространение и другие виды злоупотреблений. Самыми распространенными можно считать следующие:

1. "*Отказы в обслуживании"* - несанкционированное использование компьютерной системы в своих целях (например, для бесплатного решения своих задач), либо блокирование системы для отказа в обслуживании других пользователей. Для реализации такого злоупотребления используются так называемые "жадные программы" - программы, способные захватить монопольно определенный ресурс системы (причем необязательно центральный процессор). Следует отметить, что отказ в обслуживании пользователю, обладающего действительными правами доступа, может явиться одним из результатов функционирования таких программ, как "троянские кони", "люки " и другие.

2. “*Работа между строк (between lines)”.* Состоит в подключении к линиям связи и внедрение в компьютерную систему ПЗ с использованием промежутков в действиях законного пользователя [58 и др.]. При интерактивной работе пользователя образуются своеобразные “окна” (например, отклик системы опережает действия пользователя, которому необходимо время для обдумывания последующих действий). Эти "окна" вполне могут быть использованы нарушителем для работы с системой под маской пользователя.

3. “*Анализ трафика (trafic analysis)”* Заключается в том, что программа “захватчик" анализирует частоту и методы контактов пользователей в системе [58, и др.]. При этом можно выяснить правила вступления в связь, после чего производится попытка вступить в контакт под видом законного пользователя.

4. “*Маскарад (masquerade)”.* Программа “захватчик" использует для входа в систему ставшую ей известной идентификацию законного пользователя [58, и др.].

5. *"Подкладывание свиньи (piggback)”* - нарушитель подключается к линиям связи и имитирует работу системы с целью осуществления незаконных манипуляций. Например, он может имитировать сеанс связи и получить данные под видом легально пользователя. Пользователь, не подозревая об этом, передает информацию и/или получает ее. Таким образом может осуществляться не только шпионаж, но и дезинформация, что также отрицательно сказывается на работе АИС и объекта управления в целом.

6. “*Повторное использование объектов (object reutilization)”.* Состоит в восстановлении и повторном использовании удаленных объектов системы.

Примером реализации подобного злоупотребления служит удаление файлов операционной системой. Когда ОС выдает сообщение, что некоторый файл удален, то это не означает, что информация, содержащаяся в данном файле уничтожена в прямом смысле слова. Данное сообщение означает, что система пометила блоки памяти, ранее

составляющие содержимое файла, специальным флажком, говорящим о том, что данный блок не входит в состав какого-либо файла и может быть использован для размещения в нем другой информации. На самом деле информация, которая была в данном блоке никуда не исчезает до момента записи на это место другой информации. Таким образом, если прочесть содержание блока, можно получить доступ к "удаленной" информации (даже средствами ОС). Одним из разновидностей повторного использования объектов является работа с компьютерным ”мусором”. Компьютерным “мусором” являются данные, оставшиеся в памяти компьютера после завершения работы. Осуществляя сбор компьютерного “мусора” с помощью специальных программных средств, нарушитель имеет возможность проанализировать содержание информационной деятельности пользователей.

7. *Запуск “воздушного змея”.* Для реализации подобного программного злоупотребления используется следующая последовательность действий. В двух или более банках открываются счета. Денежные средства переводятся из одного банка в другой с повышающимися размерами. Суть злоупотребления заключается в том, чтобы замаскировать необеспеченный денежными средствами перевод. Данный цикл повторяется многократно, пока на конкретном счете не осядет значительная сумма [15]. После этого денежные средства снимаются и операции прекращаются. Следует отметить, что данное злоупотребление требует точного расчета и синхронизации последовательности действий нарушителей.

Несмотря на то, что данное злоупотребление не относится к “чисто” компьютерным, оно подготавливается и реализуется с помощью компьютера и программного обеспечения. В данном случае компоненты информационных и коммуникационных технологий используются в качестве средства подготовки и средства реализации преступления.

8. *“Раздеватели”.* С развитием рынка “персональных” технологий, широкое распространение получило такое злоупотребление, как

*нелегальное распространение, использование и/или изменение программных средств* [153].

Под *нелегальным распространением понимается продажа, обмен или бесплатное распространение программного продукта, авторские права на который принадлежат третьему лицу, без его согласия.*

*Нелегальное использование* - это использование программного продукта без согласия владельца авторских прав.

*Нелегальное изменение* - это внесение в код программы или внешний вид (интерфейс) изменений, не оговоренных с владельцем авторских прав, с тем, чтобы измененный продукт не попадал под действие авторских прав.

Следует отметить, что проблема нелегального копирования и распространения программного обеспечения является актуальной. Это вызвано влиянием ряда объективных и субъективных факторов (социальных, экономических и др.). В условиях зарождения рынка сформировались группы специалистов, выполняющих работы по вскрытию средств защиты программных продуктов и нелегальному их распространению. Кроме того, некоторая часть программного обеспечения не обладает средствами защиты или они настолько слабы, что их устранение требует минимальных знаний в области информационных технологий.

В целях защиты программных продуктов от несанкционированного копирования (НСК), начали развиваться методы и средства защиты, основные из которых рассмотрены в [120,121,55,130].

Одновременно с этим, на рынке появились специальные средства для реализации НСК и “взлома” систем защиты [153,152,154 и др.].

Группа специальных средств, которые предназначены для реализации НСК и снятия защиты в [120] названа “раздевателем”. “*Раздеватель”* - комплекс специально разработанных программных средств, ориентированных на исследование защитного механизма программного продукта от НСК и его преодоление. В данную группу

входят следующие программные разработки, используемые для “вскрытия” защиты [121]:

* эмуляторы среды, предназначенные для подделки среды, в которой работает защищаемая программа;

* симулятор микропроцессора 8088;

* специальные отладчики для работы в защищенном режиме для 386-го микропроцессора.

**9.** В связи с развитием средств связи и электронной почты выделено злоупотребление, которое относится к классу “компьютерного хулиганства” и в литературе получило название “*пинание*” (pinging). Суть данного злоупотребления заключается в том, что используя стандартные или специально разработанные программные средства злоумышленник может вывести из строя электронный адрес, бомбардируя его многочисленными почтовыми сообщениями. Следствием “пинания” могут стать осложнения и возможность непреднамереннного игнорирования полученной электронной почты.

Необходимо отметить, что при планировании и разработке злоупотреблений нарушителями могут создаваться новые, не приведенные в данной классификации, а также применяться любые сочетания описанных злоупотреблений.