## Угрозы безопасности программного обеспечения и примеры их реализации в современном компьютерном мире.

Угрозы безопасности информации и программного обеспечения КС возникают как в процессе их эксплуатации, так и при создании этих систем, что особенно характерно для процесса разработки ПО, баз данных и других информационных компонентов КС.

Наиболее уязвимы с точки зрения защищенности информационных ресурсов являются так называемые критические компьютерные системы. Под критическими компьютерными системами будем понимать сложные компьютеризированные организационно-технические и технические системы, блокировка или нарушение функционирования которых потенциально приводит к потере устойчивости организационных систем государственного управления и контроля, утрате обороноспособности государства, разрушению системы финансового обращения, дезорганизации систем энергетического и коммуникационно - транспортного обеспечения государства, глобальным экологическим и техногенным катастрофам.

При решении проблемы повышения уровня защищенности информационных ресурсов КС необходимо исходить из того, что наиболее вероятным информационным объектом воздействия будет выступать программное обеспечение, составляющее основу комплекса средств получения, семантической переработки, распределения и хранения данных, используемых при эксплуатации критических систем.

В настоящее время одним из наиболее опасных средств информационного воздействия на компьютерные системы являются программы - вирусы или компьютерные вирусы.

Наибольшее распространение компьютерные вирусы получили с развитием персональных ЭВМ (ПЭВМ) и появлением микропроцессоров фирмы Intel. Это обусловлено тем, что для ПЭВМ наиболее распространенными операционными системами (ОС) были и используются по настоящее время (в новых версиях) ОС MS-DOS и ОС Windows, которые по многим параметрам открыты и беззащитны к вирусной угрозе. В известных классификациях вирусов [[3,59]](http://citforum.ru/security/articles/kazarin/3.shtml#1) более 90% от их общего числа составляют именно вирусы для среды этих операционных систем. Для наиболее распространенных современных сетевых и многозадачных операционных систем ряда Windows, OS/2 и клона Unix по сравнению с этим вирусов обнаружено не столь много.

В последние 10-15 лет компьютерные вирусы нанесли значительный ущерб, как отдельным средствам вычислительной техники, так и сложным телекоммуникационным системам различного назначения. Интенсивные проявления вирусных заражений начались примерно в середине 80-х годов. Так, с 1986 по 1989 год было зарегистрировано 450 случаев проникновения через сеть INTERNET компьютерных вирусов в сеть Министерства обороны США DDN, из которых 220 были классифицированы как успешные. Только стоимость операций по выявлению источников вирусных атак в DDN превысила 100 тысяч долларов. Факты попыток проникновения с использованием компьютерных вирусов в информационные банки критических систем в первой половине 80-х были зарегистрированы в различных сетях США, Франции, Великобритании, ФРГ, Израиля, Пакистана и Японии. По мнению исследователей, после заражения одной ЭВМ в сети среднее время заражения следующего узла сети составляет от 10 до 20 минут. При такой интенсивности размножения некоторые вирусы способны за несколько часов вывести из строя всю сеть.

Классическим примером широкомасштабной вирусной угрозы является известный вирус Морриса, выведший 21 ноября 1988 на 24 часа из строя сеть ARPARNET. Промышленная ассоциация компьютерных вирусов (Computer Virus Industry Association - CVIA) выполнила детальный анализ расходов, связанных с действием этого вируса, заразившего 7,3% или 6200 из 85200 компьютеров сети. Пользователи потеряли свыше 8 млн. часов рабочего времени, а операторы и администраторы сети потратили около 1,13 млн. человеко-часов на то, чтобы привести сеть в рабочее состояние. Расходы от потерянной возможности доступа в сеть и средства, затраченные на ее восстановление, составили 98 млн. долларов. К декабрю 1988 г. в Ливерморской лаборатории США (Lawrence Livermore National Laboratories), которая занимается, в том числе, разработкой ядерного оружия 3-го поколения, было зафиксировано не менее 10 попыток проникновения в сеть лаборатории через каналы связи со Стэндфордским университетом, университетом штата Вашингтон и через сеть INTERNET. В результате было поражено 800 компьютеров. В том же году было зафиксировано 200 попыток заражения (из них 150 - успешных) глобальной компьютерной сети NASA. Причем 16 мая в течение 7 часов было заражено 70 ЭВМ, а после заражения в них была создана специальная программа для облегчения проникновения в сеть в будущем. Наиболее характерные исторические примеры проявления компьютерных вирусов и тенденции их роста в настоящее время можно найти в таблице 1.1 и на рис.1.1.

В качестве основных средств вредоносного (деструктивного) воздействия на КС необходимо, наряду с другими средствами информационного воздействия, рассматривать алгоритмические и программные закладки.

Под алгоритмической закладкой будем понимать преднамеренное завуалированное искажение какой-либо части алгоритма решения задачи, либо построение его таким образом, что в результате конечной программной реализации этого алгоритма в составе программного компонента или комплекса программ, последние будут иметь ограничения на выполнение требуемых функций, заданных спецификацией, или вовсе их не выполнять при определенных условиях протекания вычислительного процесса, задаваемого семантикой перерабатываемых программой данных. Кроме того, возможно появление у программного компонента функций, не предусмотренных прямо или косвенно спецификацией, и которые могут быть выполнены при строго определенных условиях протекания вычислительного процесса.

Под программной закладкой будем понимать совокупность операторов и (или) операндов, преднамеренно в завуалированной форме включаемую в состав выполняемого кода программного компонента на любом этапе его разработки. Программная закладка реализует определенный несанкционированный алгоритм с целью ограничения или блокирования выполнения программным компонентом требуемых функций при определенных условиях протекания вычислительного процесса, задаваемого семантикой перерабатываемых программным компонентом данных, либо с целью снабжения программного компонента не предусмотренными спецификацией функциями, которые могут быть выполнены при строго определенных условиях протекания вычислительного процесса.

Действия алгоритмических и программных закладок условно можно разделить на три класса: изменение функционирования вычислительной системы (сети), несанкционированное считывание информации и несанкционированная модификация информации, вплоть до ее уничтожения. В последнем случае под информацией понимаются как данные, так и коды программ. Следует отметить, что указанные классы воздействий могут пересекаться.

|  |  |
| --- | --- |
| **Год** | **События, цифры, факты** |
| 21.11. 1988 | Вирус Морриса на 24 часа вывел из строя сеть ARPANET. Ущерб составил 98 млн. долларов. |
| 1988 | Зафиксировано 200 попыток заражения вирусами (150 - успешных) глобальной компьютерной сети NASA. Причем 16 мая в течение 7 часов было заражено 70 ЭВМ. |
| с 20.03. по 9.09. 1988 | Промышленная ассоциация компьютерных вирусов (Computer Vi-rus Industry Association - CVIA) зарегистрировала 61795 случаев заражения вирусами различных информационных систем по всему миру. |
| 1986 - 1989 | Зарегистрировано 450 случаев попыток НСД и заражения вирусами (220 - успешные) сети МО США DDN. Длительность цикла проникновения и выборки информации не превышала 1 мин. |
| 1992 | В США было заражено чуть более одного из каждых десяти офисных компьютеров (данные для более, чем 60000 ПЭВМ фирм Mac, Atari, Amiga, PC) |
| 1994 | Национальная аудиторская служба Великобритании (National Audit Office - NAO) зарегистрировала 562 случая заражения вирусами компьютерных систем британских правительственных организаций, что в 3.5 раза превышает уровень 1993 г. |
| 1995 | В космическом центре Джонсона NASA зарегистрировано 52 случая заражения компьютеров Mac и PC вирусам. Время, затраченное на их устранение, составило более 350 часов |
| 1995 | Появление макровирусов. Изменение динамики процентного содержания макровирусов в общем числе компьютерных вирусов с 16% в январе 1995 г. до 44% в ноябре 1995 г. |
| 1995 | В сети Bitnet (международная академическая сеть) за 2 часа вирус, замаскированный под рождественское поздравление, заразил более 500 тысяч компьютеров по всему миру, при этом сеть IBM прекратила вообще работу на несколько часов. |
| Декабрь 1996 | Компьютерная атака на WebCom (крупнейшего провайдера услуг WWW в США) вывела из строя на 40 часов больше 3000 абонентских пунктов WWW. Атака представляла собой "синхронный поток", которая блокирует функционирование сервера и приводит к "отказу в обслуживании". Поиск маршрута атаки длился 10 часов. |

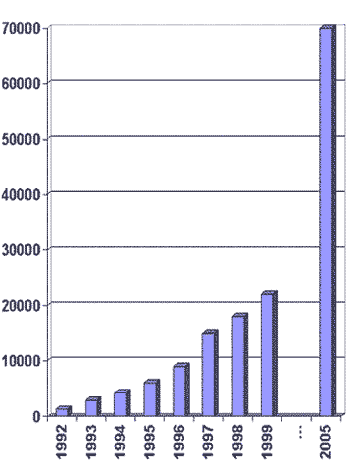


Рис. 1.1. График роста компьютерных вирусов

В первом классе воздействий выделим следующие:

* уменьшение скорости работы вычислительной системы (сети);
* частичное или полное блокирование работы системы (сети);
* имитация физических (аппаратурных) сбоев работы вычислительных средств и периферийных устройств;
* переадресация сообщений;
* обход программно-аппаратных средств криптографического преобразования информации;
* обеспечение доступа в систему с непредусмотренных периферийных устройств.

Несанкционированное считывание информации, осуществляемое в автоматизированных системах, направлено на:

* считывание паролей и их отождествление с конкретными пользователями;
* получение секретной информации;
* идентификацию информации, запрашиваемой пользователями;
* подмену паролей с целью доступа к информации;
* контроль активности абонентов сети для получения косвенной информации о взаимодействии пользователей и характере информации, которой обмениваются абоненты сети.

Несанкционированная модификация информации является наиболее опасной разновидностью воздействий программных закладок, поскольку приводит к наиболее опасным последствиям. В этом классе воздействий можно выделить следующие:

* разрушение данных и кодов исполняемых программ внесение тонких, трудно обнаруживаемых изменений в информационные массивы;
* внедрение программных закладок в другие программы и подпрограммы (вирусный механизм воздействий);
* искажение или уничтожение собственной информации сервера и тем самым нарушение работы сети;
* модификация пакетов сообщений.

Из изложенного следует вывод о том, что алгоритмические и программные закладки имеют широкий спектр воздействий на информацию, обрабатываемую вычислительными средствами в КС. Следовательно, при контроле технологической безопасности программного обеспечения необходимо учитывать его назначение и состав аппаратных средств и общесистемного программного обеспечения (программно-аппаратную среду) КС.

С точки зрения времени внесения программных закладок в программы их можно разделить на две категории: априорные и апостериорные, то есть закладки, внесенные при разработке ПО (или "врожденные") и закладки, внесенные при испытаниях, эксплуатации или модернизации ПО (или "приобретенные") соответственно. Хотя последняя разновидность закладок и относятся больше к проблеме обеспечения эксплуатационной, а не технологической безопасности ПО, однако методы тестирования программных комплексов, вероятностные методы расчета наличия программных дефектов и методы оценивания уровня безопасности ПО могут в значительной мере пересекаться и дополнять друг друга. Тем более что действие программной закладки после того как она была внесена в ПО либо на этапе разработки, либо на последующих этапах жизненного цикла ПО, практически не будет ничем не отличаться.

Таким образом, рассмотренные программные средства деструктивного воздействия по своей природе носят, как правило, разрушительный, вредоносный характер, а последствия их активизации и применения могут привести к значительному или даже непоправимому ущербу в тех областях человеческой деятельности, где применение компьютерных систем является жизненно необходимым. В связи с этим такие вредоносные программы будем называть разрушающими программными средствами (РПС), а их обобщенная классификация может выглядеть следующим образом:

* компьютерные вирусы - программы, способные размножаться, прикрепляться к другим программам, передаваться по линиям связи и сетям передачи данных, проникать в электронные телефонные станции и системы управления и выводить их из строя;
* программные закладки - программные компоненты, заранее внедряемые в компьютерные системы, которые по сигналу или в установленное время приводятся в действие, уничтожая или искажая информацию, или дезорганизуя работу программно-технических средств;
* способы и средства, позволяющие внедрять компьютерные вирусы и программные закладки в компьютерные системы и управлять ими на расстоянии.

Угрозы безопасности информации в компьютерных системах

С позиции обеспечения безопасности информации в КС такие системы целесообразно

рассматривать в виде единства трех компонент, оказывающих взаимное влияние друг на друга:

• информация;

• технические и программные средства;

• обслуживающий персонал и пользователи.

В отношении приведенных компонент иногда используется и термин "информационные

ресурсы", который в этом случае трактуется значительно шире, чем в Федеральном законе "Об

информации, информатизации и защите информации".

Целью создания любой КС является удовлетворение потребностей пользователей в

своевременном получении достоверной информации и сохранении ее конфиденциальности.

Информация является конечным "продуктом потребления" в КС и выступает в виде центральной

компоненты системы. Безопасность информации на уровне КС обеспечивают две другие

компоненты системы. Причем эта задача должна решаться путем защиты от внешних и

внутренних неразрешенных (несанкционированных) воздействий. Особенности взаимодействия

компонент заключаются в следующем. Внешние воздействия чаще всего оказывают

несанкционированное влияние на информацию путем воздействия на другие компоненты

системы. Следующей особенностью является возможность несанкционированных действий,

вызываемых внутренними причинами, в отношении информации со стороны технических,

программных средств, обслуживающего персонала и пользователей. В этом заключается основное

противоречие взаимодействия этих компонент с информацией. Причем, обслуживающий персонал

и пользователи могут сознательно осуществлять попытки несанкционированного воздействия на

информацию. Таким образом, обеспечение безопасности информации в КС должно

предусматривать защиту всех компонент от внешних и внутренних воздействий (угроз).

Под угрозой безопасности информации понимается потенциально возможное событие,

процесс или явление, которые могут привести к уничтожению, утрате целостности,

конфиденциальности или доступности информации. Все множество потенциальных угроз

безопасности информации в КС может быть разделено на два класса: случайные угрозы и

преднамеренные угрозы.

4.7.1.1. Случайные угрозы

Угрозы, которые не связаны с преднамеренными действиями злоумышленников и

реализуются в случайные моменты времени, называют случайными или непреднамеренными.

Реализация угроз этого класса приводит к наибольшим потерям информации (по

статистическим данным - до 80 % от ущерба, наносимого информационным ресурсам КС любыми угрозами). При этом могут происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию. К случайным можно отнести следующие виды угроз.

• Стихийные бедствия и аварии чреваты наиболее разрушительными последствиями для КС, т.к. последние подвергаются физическому разрушению, информация утрачивается или доступ к

ней становится невозможен.

• Сбои и отказы сложных систем неизбежны. В результате сбоев и отказов нарушается

работоспособность технических средств, уничтожаются и искажаются данные программы,

нарушается алгоритм работы устройств. Нарушения алгоритмов работы отдельных узлов и устройств могут также привести к нарушению конфиденциальности информации. Например,

сбои и отказы средств выдачи информации могут привести к несанкционированному доступу к информации путем несанкционированной ее выдачи в канал связи, на печатающее

устройство и т.п.

• Ошибки при разработке КС, алгоритмические и программные ошибки приводят к

последствиям, аналогичным последствиям сбоев и отказов технических средств. Кроме того, такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы КС.

Особую опасность представляют ошибки в операционных системах (ОС) и в программных средствах защиты информации.

• Согласно данным Национального Института Стандартов и Технологий США (NIST) 65 % случаев нарушения безопасности информации происходит в результате ошибок пользователей

и обслуживающего персонала. Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводит к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты.

Характеризуя угрозы информации в КС, не связанные с преднамеренными действиями, в целом, следует отметить, что механизм их реализации изучен достаточно хорошо, накоплен

значительный опыт противодействия этим угрозам. Современная технология разработки

технических и программных средств, эффективная система эксплуатации КС, включающая

обязательное резервирование информации, позволяют значительно снизить потери от реализации угроз этого класса.

4.7.1.2. Преднамеренные угрозы

Второй класс угроз безопасности информации в КС составляют преднамеренно

создаваемые угрозы. Данный класс угроз изучен недостаточно, очень динамичен и постоянно пополняется новыми угрозами. Угрозы этого класса в соответствии с их физической сущностью и механизмами реализации могут быть распределены по пяти группам:

• традиционный или универсальный шпионаж и диверсии;

• несанкционированный доступ к информации;

• электромагнитные излучения и наводки;

• модификация структур КС;

• вредительские программы.

Традиционный шпионаж и диверсии

В качестве источников нежелательного воздействия на информационные ресурсы по-

прежнему актуальны методы и средства шпионажа и диверсий, которые использовались и

используются для добывания или уничтожения информации на объектах, не имеющих КС. Эти методы также действенны и эффективны в условиях применения компьютерных систем. Чаще

всего они используются для получения сведений о системе защиты с целью проникновения в КС, а также для хищения и уничтожения информационных ресурсов.

К методам шпионажа и диверсий относятся:

• подслушивание;

• визуальное наблюдение;

• хищение документов и машинных носителей информации;

• хищение программ и атрибутов системы защиты;

• подкуп и шантаж сотрудников;

• сбор и анализ отходов машинных носителей информации;

• поджоги;

• взрывы.

Дистанционная видеоразведка для получения информации в КС малопригодна и носит, как правило, вспомогательный характер. Видеоразведка организуется в основном для выявления

режимов работы и расположения механизмов защиты информации. Из КС информация реально может быть получена при использовании на объекте экранов, табло, плакатов, если имеются прозрачные окна и перечисленные выше средства размещены без учета необходимости

противодействовать такой угрозе. Видеоразведка может вестись с использованием технических средств, таких как оптические приборы, фото-, кино- и телеаппаратура. Многие из этих средств допускают консервацию (запоминание) видеоинформации, а также передачу ее на определенные расстояния.

В прессе появились сообщения о создании в США мобильного микроробота для ведения дистанционной разведки. Пьезокерамический робот размером около 7 см и массой 60 г способен самостоятельно передвигаться со скоростью 30 см/с в течение 45 мин. За это время

"микроразведчик" способен преодолеть расстояние в 810 м, осуществляя транспортировку 28 г полезного груза (для сравнения - коммерческая микровидеокамера весит 15 г).

Для вербовки сотрудников и физического уничтожения объектов КС также не обязательно иметь непосредственный доступ на объект. Злоумышленник, имеющий доступ на объект КС, может использовать любой из методов традиционного шпионажа. Злоумышленниками,

имеющими доступ на объект, могут использоваться миниатюрные средства фотографирования, видео- и аудиозаписи. Для аудио- и видеоконтроля помещений и при отсутствии в них злоумышленника могут использоваться закладные устройства или "жучки". Для объектов КС наиболее вероятными являются закладные устройства, обеспечивающие прослушивание помещений. Закладные устройства делятся на проводные и излучающие. Проводные закладные устройства требуют значительного времени на установку и имеют существенный демаскирующий признак - провода. Излучающие "закладки" ("радиозакладки") быстро устанавливаются, но также имеют демаскирующий признак - излучение в радио или оптическом диапазоне. "Радиозакладки" могут использовать в качестве источника электрические или акустические сигналы. Примером использования электрических сигналов в качестве источника является применение сигналов внутренней телефонной, громкоговорящей связи. Наибольшее распространение получили акустические "радиозакладки". Они воспринимают акустический сигнал, преобразуют его в электрический и передают в виде радиосигнала на дальность до 8 км. Из применяемых на практике "радиозакладок" подавляющее большинство (около 90 %) рассчитаны на работу в диапазоне расстояний 50 - 800 м.

Для некоторых объектов КС существует угроза вооруженного нападения

террористических или диверсионных групп. При этом могут быть применены средства огневого поражения.

Несанкционированный доступ к информации

Термин "несанкционированный доступ к информации" (НСДИ) определен как доступ к

информации, нарушающий правила разграничения доступа с использованием штатных средств вычислительной техники или автоматизированных систем. Под правилами разграничения доступа понимается совокупность положений, регламентирующих права доступа лиц или процессов (субъектов доступа) к единицам информации (объектам доступа).

Право доступа к ресурсам КС определяется руководством для каждого сотрудника в

соответствии с его функциональными обязанностями. Процессы инициируются в КС в интересах определенных лиц, поэтому и на них накладываются ограничения по доступу к ресурсам.

Выполнение установленных правил разграничения доступа в КС реализуется за счет создания системы разграничения доступа (СРД).

Несанкционированный доступ к информации возможен только с использованием штатных аппаратных и программных средств в следующих случаях:

• отсутствует система разграничения доступа;

• сбой или отказ в КС; ошибочные действия пользователей или обслуживающего персонала КС;

• ошибки в СРД;

• фальсификация полномочий.

Если СРД отсутствует, то злоумышленник, имеющий навыки работы в КС, может

получить без ограничений доступ к любой информации. В результате сбоев или отказов средств КС, а также ошибочных действий обслуживающего персонала и пользователей возможны

состояния системы, при которых упрощается НСДИ. Злоумышленник может выявить ошибки в СРД и использовать их для НСДИ. Фальсификация полномочий является одним из наиболее вероятных путей (каналов) НСДИ.

**Электромагнитные излучения и наводки**

Механизмы возникновения ПЭМИН, а также защита от утечки информации по

возникающим вследствие ПЭМИН каналам проанализированы в разделах 2.4, 2.5, 3.6.

Необходимо лишь отметить, что электромагнитные излучения используютс злоумышленниками не только для получения информации, но и для ее уничтожения. **Электромагнитные импульсы** способны уничтожить информацию на магнитных носителях. **Мощные электромагнитные** сверхвысокочастотные излучения могут вывести из строя электронные блоки КС. Причем для уничтожения информации на магнитных носителях с расстояния нескольких десятков метров может быть использовано устройство, помещающееся в портфель.

**Несанкционированная модификация структур**

Большую угрозу безопасности информации в КС представляет несанкционированная

модификация алгоритмической, программной и технической структур системы.

Несанкционированная модификация структур может осуществляться на любом жизненном цикле КС. Несанкционированное изменение структуры КС на этапах разработки и модернизации

получило название "закладка". В процессе разработки КС "закладки" внедряются, как правило, в специализированные системы, предназначенные для эксплуатации в какой-либо фирме или государственных учреждениях. В универсальные КС "закладки" внедряются реже, в основном для дискредитации таких систем конкурентом или на государственном уровне, если предполагаются поставки КС во враждебное государство. "Закладки", внедренные на этапе разработки, сложно выявить ввиду высокой квалификации их авторов и сложности современных КС.

Алгоритмические, программные и аппаратные "закладки" используются либо для

непосредственного вредительского воздействия на КС, либо для обеспечения неконтролируемого входа в систему. Вредительские воздействия "закладок" на КС осуществляются при получении соответствующей команды извне (в основном, характерно для программных "закладок") и при наступлении определенных событий в системе. Такими событиями могут быть: переход на определенный режим работы (например, боевой режим системы управления оружием или режим устранения аварийной ситуации на атомной электростанции и т.п.), наступление установленной даты, достижение определенной наработки и т.д.

Программные и аппаратные "закладки" для осуществления неконтролируемого входа в

программы (например, режимов операционной системы), обхода средств защиты информации получили название "люки".

Вредительские программы

Одним из основных источников угроз безопасности информации в КС является

использование специальных программ, получивших общее название "вредительские программы".

В зависимости от механизма действия вредительские программы делятся на четыре класса:

• "логические бомбы";

• "черви";

• "троянские кони";

• "компьютернрые вирусы".

"Логические бомбы" - это программы или их части, постоянно находящиеся в ЭВМ или

вычислительных системах (ВС) и выполняемые только при соблюдении определенных условиях.

Примерами таких условий могут быть: наступление заданной даты, переход КС в определенный режим работы, наступление некоторых событий установленное число раз и т.п.

"Червями" называются программы, которые выполняются каждый раз при загрузке

системы, обладают способностью перемещаться в ВС или сети и самопроизводить копии.

Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и, в

конечном итоге, к блокировке системы.

"Троянские кони" - это программы, полученные путем явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.

"Компьютерные вирусы" - это небольшие программы, которые после внедрения в ЭВМ

самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на КС. Поскольку вирусам присущи свойства всех классов вредительских программ, то в последнее время любые вредительские программы часто называют вирусами.

**Классификация злоумышленников**

Возможности осуществления вредительских воздействий в большой степени зависят от

статуса злоумышленника по отношению к КС. Злоумышленником может быть:

• разработчик КС;

• сотрудник из числа обслуживающего персонала;

• пользователь;

• постороннее лицо.

Разработчик владеет наиболее полной информацией о программных и аппаратных

средствах КС и имеет возможность внедрения "закладок" на этапах создания и модернизации систем. Но он, как правило, не получает непосредственного доступа на эксплуатируемые объекты КС. Пользователь имеет общее представление о структурах КС, о работе механизмов защиты информации. Он может осуществлять сбор данных о системе защиты информации методами

традиционного шпионажа, а также предпринимать попытки несанкционированного доступа к информации. Возможности внедрения "закладок" пользователями очень ограничены. Постороннее лицо, не имеющее отношения к КС, находится в наименее выгодном положении по отношению к другим злоумышленникам. Если предположить, что он не имеет доступ на объект КС, то в его распоряжении имеются дистанционные методы традиционного шпионажа и возможность диверсионной деятельности. Он может осуществлять вредительские воздействия с

использованием электромагнитных излучений и наводок, а также каналов связи, если КС является распределенной.

Большие возможности оказания вредительских воздействий на информацию КС имеют

специалисты, обслуживающие эти системы. Причем, специалисты разных подразделений

обладают различными потенциальными возможностями злоумышленных действий. Наибольший вред могут нанести работники службы безопасности информации. Далее идут системные программисты, прикладные программисты и инженерно-технический персонал.

На практике опасность злоумышленника зависит также от финансовых, материально-

технических возможностей и квалификации злоумышленника.