70

Секретно 19
163

КОМИТЕТ
ГОСУДАРСТВЕННОЙ БЕЗОПАСНОСТИ СССР

УКАЗАНИЕ

28 июля 1989 года № 42с

Москва

Председателям КГБ союзных и автономных республик

Начальникам УКГБ по краям и областям

Начальникам управлений особых отделов, начальникам особых отделов КГБ СССР по группам войск, округам и флотам

Начальникам учебных заведений КГБ СССР

Начальникам главных управлений, самостоятельных управлений и отделов КГБ СССР

О порядке приобретения, эксплуатации и размножения зарубежных программных средств

Накопленный в мировой практике опыт создания программных средств для современной электронной вычислительной техники, в частности персональных электронных вычислительных машин, допускает возможность размещения в них различного рода посторонних программных включений ("компьютерных вирусов"), в том числе и диверсионного назначения.

В связи с этим все большее значение придается обеспечению безопасности данных, хранимых и обрабатываемых в автоматизированных системах информационного обеспечения и управления (АСИО и АСУ), построенных на базе персональных ЭВМ.

В целях обеспечения защиты информационных систем, использующих зарубежные программные средства для персональных ЭВМ (в том числе и адаптированных на русский язык) и функционирующих в

32
4 08 1989

системе КГБ СССР от возможного воздействия "компьютерных вирусов".

ПРЕДЛАГАЕТСЯ:

1. Использовать типовые программные средства, специально разрабатываемые в подразделениях центрального аппарата КГБ СССР, а также программные средства общего применения, распространяемые через Фонд алгоритмов и программ для персональных ЭВМ КГБ СССР, сформированный в ОТУ КГБ СССР, Государственный фонд алгоритмов и программ Государственного комитета СССР по вычислительной технике и информатике, его отраслевые фонды. Программные средства, приобретенные путем официальной закупки за рубежом через МВЭС СССР и другими путями, использовать в подразделениях центрального аппарата КГБ СССР, имеющих в своем составе специалистов по вычислительной технике, при условии проверки их на отсутствие "компьютерных вирусов" на основе методик и рекомендаций ОТУ КГБ СССР. Сведения о данных средствах направлять установленным порядком в Фонд алгоритмов и программ для персональных ЭВМ КГБ СССР.

2. Руководствоваться в практической работе с персональными ЭВМ и программными средствами к ним Ориентировкой о "компьютерных вирусах" и способах борьбы с ними (прилагается).

Первый заместитель Председателя Комитета
генерал армии

Н. Емохонов

Тематические индексы: 9-10; 20-13

Секретно

ПРИЛОЖЕНИЕ
к указанию КГБ СССР
от "28" июля 1989 г.

№ 420

ОРИЕНТИРОВКА
о "компьютерных вирусах" и способах борьбы с ними

В настоящее время все большее значение придается обеспечению безопасности данных, хранимых и обрабатываемых на ЭВМ, поскольку накопленный в мировой практике опыт программирования и специфика программного обеспечения современных компьютеров допускают возможность создания и размещения в программах различного рода включений, в том числе и диверсионного назначения.

Диапазон мотивов изготовления и внедрения этих программных включений очень широк - от нанесения экономического ущерба и защиты авторских прав изготовителей программных изделий до мелкого шантажа, сведения личных счетов и демонстрации интеллектуальных способностей отдельных программистов, недостаточно, по их мнению, оцененных руководством, без конкретной направленности наносимого вреда (например, случай, имевший место в 1982 году на вычислительном центре Волжского автозавода в городе Тольятти). По аналогии с техническими устройствами, скрытно внедряемыми в аппаратуру или другие конструкции, программные включения диверсионного назначения получили название программных закладок. Стремясь придать сенсационность публикациям о случаях проявления действия программных закладок, их авторы дают этим программам броские названия: "программные ловушки", "логические бомбы", "троянские кони", "черви", "компьютерные вирусы" и т.п.

Программные закладки типа "компьютерный вирус" (далее по тексту "компьютерный вирус" или просто "вирус") получили свое название в связи с наличием у них способности распространяться в программном обеспечении путем внедрения своей копии в тело других программ без нарушения до определенного момента времени их работоспособности. При бесконтрольном копировании программного обеспечения, имеющего в своем составе "компьютерный вирус", и его последующем использовании на других вычислительных установках может происходить многократное тиражирование этих программных закладок или, по выражению некоторых авторов, происходит "заражение" программ "вирусом". Наибольшее распространения программные закладки типа "компьютерный вирус" получили в персональных ЭВМ (ПЭВМ) из-за особенностей их архитектуры, общей структуры программного обеспечения и простоты обмена программами между пользователями.

Уже в 1985 году стали появляться сообщения о фактах проявления "компьютерных вирусов" в ПЭВМ. Начиная с 1987 года количество таких сообщений резко увеличилось. Описание фактов "заражения" "компьютерными вирусами", в том числе и с достаточно серьезными последствиями, практически не сходят последние годы со страниц западной прессы.

В 1987-89 годах участились факты появления "компьютерных вирусов" на ПЭВМ и в нашей стране. Имеется информация об обнаружении "компьютерных вирусов" на объектах Минрадиопрома, Минсредмаша, АН СССР и других (всего около 20 вычислительных центров), а также в подразделениях КГБ СССР. Как правило, проникновение "вирусов" в ПЭВМ происходит при использовании программного обеспечения, которое приобреталось или бесконтрольно копировалось на основе личных неофициальных контактов между пользователями.

Простота создания "компьютерных вирусов" (может быть создан программистом средней квалификации), сложность обнаружения (обычно являются фрагментами программ без формальных признаков, позволяющих их обнаруживать), сложность, а в отдельных случаях невозможность определения автора "вируса" и источника "заражения", отсутствие в настоящее время эффективных универсальных средств борьбы с проникновением "вирусов", а также значительный ущерб, который может быть нанесен при проявлении "вирусом" агрессивных свойств, делают проблему борьбы с программными закладками типа "компьютерный вирус" актуальной.

Имеются данные, что спецслужбы противника проводят секретные разработки "компьютерных вирусов" в качестве эффективного диверсионного средства поражения вычислительных систем.

В соответствии с поручением Государственной комиссии Совета Министров СССР по военно-промышленным вопросам группа заинтересованных министерств и ведомств в 1984 году подготовила доклад в инстанции по проблеме программных закладок. Доклад был согласован с КГБ СССР и доложен правительству в порядке информации.

С целью оценки положения дел с защитой от "компьютерных вирусов" в системе КГБ СССР Научно-технический Совет КГБ СССР в конце 1988 года рассмотрел проблему "компьютерных вирусов" и методов борьбы с ними и принял по этому вопросу конкретные решения.

С технической точки зрения механизм действия "компьютерных вирусов" в общем случае заключается в следующем: "Вирус", являясь частью некоторой "зараженной" программы, при ее выполнении на ПЭВМ становится резидентным в оперативной памяти машины и остается там после завершения выполнения программы - носителя "вируса". Это возможно благодаря тому, что в современных ПЭВМ нет разделения памяти между системными и прикладными программами и выделения специального приоритетного режима выполнения системных программ. Таким образом любая прикладная программа пользователя может сделаться резидентной, перехватывать системные прерывания, обрабатывать их и выполнять другие функции операционной системы. Являясь резидентной программой и находясь по сути дела на уровне системных программ ПЭВМ, "вирус" имеет возможность контролировать работу машины и связанные с этим события. При вызове в память ПЭВМ каких-либо программ для их выполнения "вирус", находящийся в памяти, дописывает себя в эти программы. Некоторые вирусы могут просматривать директории на дисках, установленных на ПЭВМ во время присутствия "вируса" в памяти машины, и в момент обращения к дискам дописывать себя в программы без вызова их на выполнение. Программы модифицируются таким образом, чтобы при их выполнении сначала выполнялся бы "вирус", а затем уже сама программа. Это необходимо для обеспечения возможности дальнейшего распространения "вируса". Пользователь ПЭВМ до определенного момента видит только нормальное выполнение программ и не подозревает о содержащемся в них "вирусе".

Агрессивные действия "компьютерных вирусов", как правило, проявляются не сразу после "заражения" программного обеспечения ПЭВМ, а при наступлении определенных условий. Такими условиями могут быть соответствующие значения таймера, даты, дня недели, количество выполнений "зараженной" программы, количество копировании программы, количество "зараженных" "вирусом" программ и т.п. Определенные условия могут быть наложены и на способность "вируса" тиражироваться в программы.

Действия "компьютерных вирусов" могут быть самыми различными – от появления на экране монитора ПЭВМ посторонних изображений до разрушения данных и программ на дисках.

Наиболее характерными проявлениями "компьютерных вирусов" в ПЭВМ на сегодняшний день можно считать следующие:

- появление на экране монитора посторонних изображений;
- "осыпание" символов на экране монитора в нижнюю свободную строку экрана;
- существенное снижение производительности ПЭВМ, не связанное с аппаратурными неисправностями;
- перезагрузка ПЭВМ при запуске на выполнение ранее работоспособных программ;
- увеличение длины программ на дисках (гибких и жестких);
- исчезновение программ с диска, если их никто не удалял умышленно;
- появление на ранее качественных дисках большого количества секторов, помеченных как дефектные, а также разрушение данных и программ (особенно большой длины), происшедшее на нескольких компьютерах примерно в одно и то же время.

Из имеющегося опыта известно, что наиболее вероятными носителями "компьютерных вирусов" являются служебные программы общего назначения, текстовые редакторы, а также игровые программы, поскольку бесконтрольный обмен этими видами программных средств происходит наиболее интенсивно.

В сообщениях за рубежом упоминается о существовании около 40 типов "компьютерных вирусов", однако, в настоящее время достоверно известно о проявлении в СССР только трех типов "вирусов", ориентированных на ПЭВМ IBM PC и им подобных.

Одним из наиболее часто встречающихся является "компьютерный вирус", имеющий длину 648 байт и известный под названием DOS-62, TIMEBOMB, VHS-648. Этот "вирус" внедряется в программы с расширением имени .COM (командные файлы). Агрессивные проявления этого "вируса" происходят при возникновении определенной комбинации младших разрядов таймера ПЭВМ в момент тиражирования "вируса" в очередную программу. Они заключаются в модификации программы таким образом, что ее запуск вызывает перезагрузку операционной системы ПЭВМ.

Другой известный тип "вируса" имеет длину 1701 байт или близкую к ней и внедряется в программы с расширением имени .COM. Агрессивные действия - "осыпание" символов на экране монитора в нижнюю свободную строку через некоторое время после запуска "пораженной" программы. По прошествии некоторого времени "вирус" вызывает перезагрузку операционной системы. Разрушение информации данный тип "вируса" не вызывает. Агрессивные проявления отмечаются с 20 октября 1988 года.

Еще один тип "вируса", обнаруженный в СССР, имеет длину 710 байт. Этот "вирус" способен внедряться в программы с расширением имени .COM и .EXE (выполняемые файлы). Агрессивные проявления - снижение производительности ПЭВМ, происходящее за счет собственной обработки "вирусом" прерываний по таймеру, а также разрушение программ на диске, которые пользователь пытается вызвать на выполнение 13 числа какого-либо месяца, пришедшегося на пятницу. Таким днем в 1989 году будет 13 октября.

В ОТУ КГБ СССР имеются программы обнаружения и удаления первых двух типов "вирусов".

Описанные "компьютерные вирусы" являются программами зарубежного производства. Однако не исключена возможность появления программных закладок этого типа, ориентированных на ПЭВМ отечественного производства, авторами которых будут являться отечественные программисты.

Борьба с "компьютерными вирусами" должна рассматриваться как составная часть мероприятий по обеспечению безопасности автоматизированных систем информационного обеспечения (АСИО) подразделений КГБ СССР. Она должна осуществляться в направлении уменьшения вероятности проникновения "вирусов" в программное обеспечение автоматизированных систем и проведения мероприятий по оперативной ликвидации последствий их агрессивного воздействия.

Возможными каналами проникновения "компьютерных вирусов" в программное обеспечение являются:

- нарушение пользователями, программистами - разработчиками или обслуживающим персоналом порядка установки и использования на ПЭВМ программных средств в действующих и разрабатываемых автоматизированных системах;
- установка на вычислительных средствах подразделений КГБ СССР программного обеспечения зарубежного или отечественного, созданного вне подразделений центрального аппарата КГБ СССР,

производства;

- подключение вычислительных средств подразделений КГБ СССР к широкодоступным сетям или использование своих сетей, в которых есть возможность доступа к устройствам ввода со стороны посторонних лиц или подключения чужих вычислительных средств.

Для уменьшения вероятности проникновения "компьютерных вирусов" по первому каналу и сокращения возможного ущерба при возможном появлении "вирусов", рекомендуются следующие профилактические меры:

- тщательный отбор контингента лиц, имеющих доступ к программному обеспечению, данным АСИО и контроль за их деятельностью;
- четкое разграничение боевого (переданного в боевую эксплуатацию, принятого на вооружение) и разрабатываемого программного обеспечения;
- строгий учет, регламентация и контроль доступа к носителям боевого программного обеспечения с целью исключения несанкционированного доступа к программам и данным;
- упорядочение и строгий учет при выполнении процедур внесения изменений в боевое программное обеспечение и в подготовленные к боевой эксплуатации программные средства на этапах их доработки и модификации, проводимые с целью исключения случаев несанкционированной коррекции;
- тщательное выявление и изучение специалистами всех нештатных ситуаций, подозрительных на наличие "компьютерного вируса", с целью оценки устойчивости программного обеспечения и своевременного выявления случаев проникновения или срабатывания возможных программных закладок.

Для обеспечения "противовирусной" защиты автоматизированных систем на канале поступления программных средств зарубежного и отечественного производства рекомендуется:

- опробование и проверку работоспособности новых программных средств проводить только на специально выделенной для этих целей вычислительной технике;
- преимущественно использовать программные средства, распространяемые через фонд алгоритмов и программ для персональных ЭВМ КГБ СССР, разрабатываемые в подразделениях центрального аппарата КГБ СССР и приобретаемые официальным путем у фирм-изготовителей;
- программные средства, приобретенные иным путем, проверять

их владельцам на отсутствие в них "вирусов" известных типов с использованием методик и рекомендаций ОТУ КГБ СССР. Первый выпуск методик разослан за № 16/10/10-420 от 29 июня 1989 г. О последующих выпусках будет сообщаться в информационных материалах Фонда алгоритмов и программ ПЭВМ КГБ СССР.

В настоящее время возможности проникновения "компьютерных вирусов" в АСИО подразделений КГБ СССР по третьему каналу сильно ограничены в связи с тем, что сетевые АСИО используются в системе КГБ СССР мало, причем только как сугубо локальные, несвязанные с сетями других организаций.

Для оперативной ликвидации последствий агрессивного действия "компьютерных вирусов" на автоматизированные системы, реализованные на технической базе ПЭВМ, при их эксплуатации должны использоваться меры и средства, позволяющие контролировать нештатные изменения программ и данных и восстанавливать их, после разрушения, с помощью копий.

При подозрении на проникновение в программное обеспечение ПЭВМ "компьютерного вируса" необходимо незамедлительное принятие мер по пресечению его возможного распространения и проявления агрессивных свойств. С этой целью следует временно прекратить проведение работ на ПЭВМ, в программном обеспечении которой предполагается наличие "вируса". Кроме того, необходимо прекратить работы на всех ПЭВМ, с которыми потенциально был возможен обмен информацией (например, через магнитные носители или через программно-технические средства сети). Далее следует выявить пораженные "вирусом" программы. Для этого необходимо загрузить эталонную копию операционной системы с дискеты, защищенной от записи и провести тестирование программного обеспечения с помощью имеющихся программ обнаружения и удаления известных типов "вирусов". Эти действия следует провести на каждой из остановленных ПЭВМ. Выявление зараженных программ может также осуществляться путем сравнения с эталонными копиями. Проводимое тестирование должно охватывать и программы операционной системы, функционировавшей в момент предполагаемого проникновения "вируса". Программы, в которых при тестировании обнаружены "вирусы" или отличия от эталонных копий, необходимо восстановить путем копирования эталонов. Использовать в работе копии программ, в которых "вирус" был обнаружен и удален, не рекомендуется.

Эффективная борьба с "компьютерными вирусами" возможна только при условии постоянного сбора и обобщения информации о

[illegible]

ПГУ.

В связи с этим необходимо оперативно информировать НИИАИ ОТУ КГБ СССР о случаях выявления "компьютерных вирусов", характеристиках "вирусов", способах их обнаружения, вероятных источниках распространения, способах локализации и устранения последствий проникновения "вирусов" в программное обеспечение, а также направлять материалы по новым типам "компьютерных вирусов".

Оперативно-техническое управление КГБ СССР

19. Последний абзац приложения к указанию КГБ СССР № 42с-1989 г. изложить в следующей редакции: "В связи с этим необходимо оперативно информировать НИИАИ-ОТУ КГБ СССР о случаях выявления "компьютерных вирусов" в персональных ЭВМ, эксплуатируемых в системе КГБ СССР, характеристиках "вирусов", способах их обнаружения, вероятных источниках распространения, способах локализации и устранения последствий проникновения "вирусов" в программное обеспечение и хранимую информацию".