ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО
Кафедра математического и программного обеспечения

УТВЕРЖДАЮ

Начальник 27 кафедры

полковник

С. Войцеховский

«___» _____ 20__ г.

Автор: старший преподаватель 27 кафедры
кандидат технических наук
подполковник С.Краснов

Лекция № 9

по учебной дисциплине
«Защита информации»
на тему

Тема: «МЕТОДЫ ЭТАЛОННЫХ ХАРАКТЕРИСТИК»

Рассмотрено и одобрено
на заседании кафедры № 27
« ___ » августа 202__ г.

протокол № __

Санкт-Петербург 2022

Содержание занятия и время

Введение – 5 мин.

Учебные вопросы (основная часть):

1. Идентификация и аутентификация пользователей – 30 мин.
2. Защита программ и дистрибутивов от копирования – 20 мин.
3. Методы обнаружения модификации данных Регистрация и анализ событий – 30 мин.

Заключение – 3-5 мин.

Литература:

Основная:

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.
2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.

Дополнительная:

1. Вихорев С.В. Классификация угроз информационной безопасности. - http://www2.cnews.ru/comments/security/elvis_class.shtml
2. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах. / Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.

Материально техническое обеспечение:

1. Технические средства обучения: ПЭВМ, мультимедиа проектор, экран, программное обеспечение.
2. Приложения (слайды).
3. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

Цель лекции: *Дать знания в области методов эталонных характеристик.*

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом произвести опрос курсантов по пройденному материалу.

Применяемым методическим приемом является рассказ.

В основной части сконцентрировать внимание курсантов на стеганографических методах ЗИ.

В заключительной части обобщить изложенный материал и осуществить контрольный опрос.

1. Перечислите основные методы эталонных характеристик?
2. В чем заключается суть методов эталонных характеристик?
3. Охарактеризуйте механизм защиты от копирования?
4. Охарактеризуйте механизм защиты от модификации?

Отвечаю на вопросы по теме занятия, даю задание на самостоятельную подготовку.

Лекция № 9

«Методы эталонных характеристик»

Суть метода ***эталонных характеристик*** заключается в анализе аппаратно-программной среды и формировании её уникального идентификатора. Только субъект, обладающий этим уникальным идентификатором, будет иметь (не иметь) право доступа к информации.

Под аппаратно-программной средой понимают: состав устройств, программ, носителей информации, установленный определённый порядок действий, правил и характеристики производительности компьютерных подсистем. *Подсистема* – набор устройств и программ АС выполняющих единую задачу. **Доступ к информации** – получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

В рамках двух подразделов защиты информации – защиты от НСД и поддержания целостности информации, *метод эталонных характеристик применяется* для решения следующих задач:

- разграничение (ограничение) доступа пользователей к ресурсам АС;
- защита программ и дистрибутивов от копирования;
- управление потоками информации;
- блокирование неиспользуемых сервисов;
- подтверждение подлинности информации;
- контроль целостности данных;
- мониторинг целостности аппаратно-программного обеспечения при передаче, обработке и хранении информации;
- регистрация и анализ событий, происходящих в АС.

В. 1. Разграничение (ограничение) доступа пользователей к ресурсам АС.

Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс первичного взаимодействия с компьютерной системой, который включает две стадии – *идентификацию и аутентификацию.*

Идентификация – это процедура распознавания пользователя по его идентификатору (имени).

Аутентификация – процедура проверки подлинности, позволяющая достоверно убедиться, что пользователь является именно тем, кем он себя объявляет.

Для подтверждения своей подлинности субъект может предъявлять системе разные сущности. В зависимости от предъявляемых субъектом сущностей процессы аутентификации могут быть разделены на следующие категории:

1. На основе знания чего-либо. Примером могут служить стандартные пароли, персональные идентификационные номера (Personal Identification Numbers – PIN), а также секретные и открытые ключи, знание которых демонстрируется в протоколах типа «запрос-ответ».
2. На основе обладания чем-либо. Обычно это магнитные карты, смарт-карты, сертификаты, устройства touch-memory и персональные генераторы, которые используются для создания одноразовых паролей.
3. На основе каких-либо неотъемлемых характеристик. Данная категория включает методы, базирующиеся на проверке биометрических характеристик пользователя (голос, сетчатка глаза, отпечатки пальцев). Аутентификация на основе биометрических характеристик применяется для контроля доступа в помещения или к какой-либо технике.

После идентификации и аутентификации пользователя система защиты должна

определить его полномочия для последующего контроля санкционированности доступа к компьютерным ресурсам. Полномочия пользователя считываются из базы эталонных данных системы защиты и заносятся в базу данных активных пользователей.

Основными и наиболее часто применяемыми методами установления подлинности пользователей являются методы, основанные на использовании паролей. Под паролем при этом понимается некоторая последовательность символов, сохраняемая в секрете и предъявляемая при обращении к компьютерной системе. Ввод пароля, как правило, выполняют с клавиатуры после соответствующего запроса системы.

Эффективность парольных методов может быть значительно повышена путем записи в зашифрованном виде длинных и нетривиальных паролей на информационные носители, например, дискеты, магнитные карты, носители данных в микросхемах и т.д. В этом случае компьютерная система должна включать специальные устройства и обслуживающие их драйверы для считывания паролей с этих информационных носителей, а служба безопасности должна располагать средствами для формирования носителей с парольными данными.

Для особо надежного опознавания могут применяться и методы, основанные на использовании технических средств определения сугубо индивидуальных характеристик человека (голоса, отпечатков пальцев, структуры зрачка и т.д.). Однако такие средства требуют значительных затрат и поэтому используются редко.

Существующие парольные методы проверки подлинности пользователей при входе в ВС можно разделить на две группы [11, 19]:

- методы проверки подлинности на основе простого пароля;
- методы проверки подлинности на основе динамически изменяющегося пароля,

Пароль подтверждения подлинности пользователя при использовании простого пароля не изменяется от сеанса к сеансу в течении установленного администратором службы безопасности времени его существования (действительности).

При использовании динамически изменяющегося пароля пароль пользователя для каждого нового сеанса работы или нового периода действия одного пароля изменяется по правилам, зависящим от используемого метода.

1.1. Использование простого пароля

Процедура опознавания с использованием простого пароля может быть представлена в виде следующей последовательности действий [10, 12]:

1) пользователь посылает запрос на доступ к компьютерной системе и вводит свой идентификатор;
2) система запрашивает пароль;
3) пользователь вводит пароль;
4) система сравнивает полученный пароль с паролем пользователя. хранящимся в базе эталонных данных системы защиты, и разрешает доступ, если пароли совпадают; в противном случае пользователь к ресурсам компьютерной системы не допускается.

Поскольку пользователь может допустить ошибку при вводе пароля, то системой должно быть предусмотрено допустимое количество повторений для ввода пароля.

В базе эталонных данных системы защиты пароли, как и другую информацию, никогда не следует хранить в явной форме, а только зашифрованными. При этом можно использовать метод как обратимого, так и необратимого шифрования.

Согласно методу обратимого шифрования эталонный пароль при занесении в базу эталонных данных зашифровывается по ключу, совпадающему с этим эталонным паролем, а введенный после идентификации пароль пользователя для сравнения с эталонным также зашифровывается, но по ключу, совпадающему с этим введенным паролем. Таким образом, при сравнении эталонный и введенный пароли находятся в зашифрованном виде и будут совпадать только в том случае, если исходный введенный пароль совпадет с исходным эталонным При несовпадении исходного введенного пароля

с исходным эталонным исходный введенный пароль будет зашифрован по другому, так как ключ шифрования отличается от ключа, которым зашифрован эталонный пароль, и после зашифровывания не совпадет с зашифрованным эталонным паролем.

Для обеспечения возможности контроля правильности ввода пароля при использовании необратимого шифрования на винчестер записывается таблица преобразованных паролей. Для их преобразования используется односторонняя криптографическая функция y=F(x), обладающая следующим свойством: для данного аргумента x значение F(x) вычисляется легко, а по данному y вычислительно сложно найти значение аргумента x, соответствующего данному y. В таблице паролей хранятся значения односторонних функций, для которых пароли берутся в качестве аргументов При вводе пароля система защиты легко вычисляет значение функции от пароля текущего пользователя и сравнивает со значением. приведенным *а,* таблице для пользователя с выбранным идентификатором. Нарушитель, захвативший компьютер, может прочитать таблицу значений функций паролей, однако вычисление пароля практически не реализуемо.

При работе с паролями должна предусматриваться и такая мера. как недопустимость их распечатки или вывода на экраны мониторов. Поэтому система защиты должна обеспечивать ввод пользователями запрошенных у них паролей без отображения этих паролей на мониторах.

Можно выделить следующие основные способы повышения стойкости системы защиты на этапе аутентификации:

• повышение степени нетривиальности пароля:

• увеличение длины последовательности символов пароля;

• увеличение времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля;

• повышение ограничений на минимальное и максимальное время действительности пароля.

Чем нетривиальнее пароль, тем сложнее его запомнить. Плохо запоминаемый пароль может быть записан на листе бумаги, что повышает риск его раскрытия. Выходом Здесь является использование определенного числа не записываемых на бумаге пробелов или других символов в начале, внутри, а также в конце последовательности основных символов пароля. Кроме того, отдельные символы пароля могут набираться на другом регистре (например, вместо строчных быть прописными или наоборот), что также не должно отражаться на листе бумаги. В этом случае незаконно полученный лист бумаги с основными символами пароля не будет достаточным условием раскрытия пароля целиком,

Вероятность подбора пароля уменьшается также при увеличении его длины и времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля.

Для исключения необходимости запоминания пользователями длинных и нетривиальных паролей в системе защиты может быть предусмотрена возможность записи паролей в зашифрованном виде на информационные носители, например, дискеты, магнитные карты, носители данных в микросхемах и т.д , а также считывания паролей с этих информационных носителей. Такая возможность позволяет повысить безопасность **за** счет значительного увеличения длины паролей, записываемых на носителе информации.

На степень информационной безопасности при использовании простого парольного метода проверки подлинности пользователей большое влияние оказывают ограничения на минимальное и максимальное время действительности каждого пароля. Чем чаще меняется пароль, тем обеспечивается большая безопасность.

Методы проверки подлинности на основе динамически изменяющегося пароля обеспечивают большую безопасность, так как частота смены паролей в них максимальна - пароль для каждого пользователя меняется ежедневно или через несколько дней. При

этом каждый следующий па роль по отношению к предыдущему изменяется по правилам, зависящим от используемого метода проверки подлинности.

Существуют следующие методы парольной защиты, основанные на использовании динамически изменяющегося пароля:

• методы модификации схемы простых паролей;
• метод «запрос-ответ»;
• функциональные методы.

Наиболее эффективными из данных методов являются функциональные методы.

В. 2. Защита программ и дистрибутивов от копирования

Защита программ и дистрибутивов от копирования реализуется привязкой программы инсталляции к дистрибутивным носителям, когда данная программа будет ориентирована на проведение инсталляции только при совпадении характеристик дистрибутивных носителей известным ей эталонным характеристикам.

Под инсталляцией понимается процесс специального копирования или разархивирования программы с дистрибутивных носителей на внешний носитель компьютера и ее настройки под требования пользователя для функционирования на данном компьютере. В качестве дистрибутивных носителей могут выступать как оптические или магнитные диски, так и магнитные ленты.

Инсталляция выполняется специальной программой, называемой **инсталлятором**.

Для защиты инсталлируемой программы от копирования инсталлятор должен выполнить следующие функции:

1) анализ аппаратно-программной среды компьютера, на котором должна будет выполняться инсталлируемая программа, и формирование на основе этого анализа эталонных характеристик среды выполнения программы;

2) запись зашифрованных эталонных характеристик аппаратно-программной среды компьютера на винчестер.

Основным требованием к свойствам дистрибутивных носителей, на основе которых формируются эталонные характеристики, является *требование по уникальности*. Согласно этому требованию контролируемыми свойствами не должны обладать другие носители информации и эти свойства не должны копироваться при копировании содержимого дистрибутивных носителей.

Зашифрованные эталонные характеристики аппаратно-программной среды компьютера могут быть занесены в следующие области жесткого диска:

- в любые свободные места области данных:
- в созданный для этой цели отдельный файл;
- в отдельные кластеры, которые должны помечаться затем в FAT как зарезервированные под операционную систему или дефектные;
- в зарезервированные сектора системной области винчестера;
- непосредственно в файлы размещения защищаемой программной системы, например, в файл настройки ее параметров функционирования

Инсталлированная программа для защиты от копирования при каждом запуске должна выполнять следующие действия;

1) анализ аппаратно-программной среды компьютера, на котором она запущена, и формирование на основе этого анализа текущих характеристик своей среды выполнения;

2) проверка подлинности среды выполнения путем сравнения ее текущих характеристик с эталонными, хранящимися на винчестере;

3) блокирование дальнейшей работы программы при несовпадении текущих характеристик с эталонными.

Рассмотрим метод привязки программы к уникальным характеристикам аппаратно-программной среды компьютера. Единственной трудностью при его реализации является определение тех характеристик аппаратно-программной среды компьютера, которые

однозначно бы идентифицировали данный компьютер. В случае, если такие характеристики отсутствуют или их определение значительно замедляет запуск программ или снижает удобство их использования, те для защиты программ от несанкционированного копирования может использоваться метод привязки программы к уникальному идентификатору формируемому инсталлятором. Суть данного метода заключается в том, что на винчестере при инсталляции защищаемой от копирования программы формируется уникальный идентификатор, наличие которого затем проверяется инсталлированной программой при каждом ее запуске. При отсутствии и несовпадении этого идентификатора программа блокирует свое дальнейшее выполнение.

Основным требованием к записанному на винчестер уникальному идентификатору является требование, согласно которому данный идентификатор не должен копироваться стандартным способом. Для этого идентификатор целесообразно записывать в следующие области жесткого диска:

- в отдельные кластеры области данных, которые должны помечаться затем в FAT как зарезервированные под операционную систему или дефектные;
- в зарезервированные сектора системной области винчестера.

Не копируемый стандартным образом идентификатор может помещаться и на дискету (диск), к которой должна будет обращаться при каждом своем запуске защищаемая от копирования программа. Такую дискету (диск) называют ключевой. Кроме того, защищаемая от копирования программа может быть привязана и к уникальным характеристикам ключевой дискеты (диска). Следует учитывать, что при использовании ключевой дискеты (диска) значительно увеличивается неудобство работы пользователя, так как он всегда должен вставлять эту дискету (диск) в дисковод перед запуском защищаемой от копирования программы.

Идентификация аппаратно-программной среды выполнения программ.

Можно выделить следующие способы привязки инсталлируемой программы к уникальным характеристикам аппаратно-программной среды компьютера:

1) привязка к характеристикам производительности отдельных компьютерных подсистем;

2) привязка к уникальным характеристикам жесткого диска, на который инсталлируется программа;

3) привязка к аппаратной конфигурации компьютера.

Наиболее высокий уровень защиты программ от копирования достигается при комбинировании различных способов привязки к уникальны» характеристикам аппаратно-программной среды компьютера.

При привязке к характеристикам производительности отдельных компьютерных подсистем в качестве эталонных характеристик выбираются показатели быстродействия жесткого диска и процессора. После запуска на выполнение инсталлируемая программа должна определить показа гели быстродействия компьютера и сравнить эти показатели с эталонными, блокируя свое дальнейшее выполнение в случае несоответствия текущих и эталонных показателей.

Способы привязки инсталлируемой программы к уникальным характеристикам жесткого диска и аппаратной конфигурации компьютера рас смотрим более подробно.

2.1. Привязка к уникальным характеристикам жесткого диска

Могут быть использованы следующие способы привязки *к* уникальным характеристикам жесткого диска:

1) привязка к физическому расположению или порядку физического размещения на жестком диске файлов инсталлированной программной системы (в этом случае должна исключаться дефрагментация дисковой памяти, приводящая к переразмещению файлов защищаемого от копирования комплекса программ);

2) привязка к содержимому неиспользуемых хвостовых частей последних кластеров файлов инсталлированной программной системы (нельзя допустить

уничтожение содержимого этих хвостовых частей специализированной программой уничтожения остаточных данных);

3) привязка к физическому расположению на жестком диске существующих или специально созданных дефектных кластеров (BAD кластеров) (эти кластеры могут быть преобразованы в рабочие при углубленном тестировании винчестера с помощью специализированных утилит);

4) + привязка к уникальной информации служебной дорожки или к нестандартному формату неиспользуемой дорожки винчестера;

5) + привязка к уникальному идентификатору, не копируемому стандартным образом.

Наиболее действенными и удобными **способами** привязки *к* винчестеру являются привязка к *уникальной информации служебной дорожки* или к нестандартному формату неиспользуемой дорожки винчестера, а также привязка *к уникальному идентификатору на жестком диске*, который невозможно скопировать стандартным образом. Нестандартное форматирование неиспользуемой дорожки винчестера, а также формирование уникального идентификатора на жестком диске должны выполняться инсталлятором. Уникальный для инсталляции идентификатор, как было рассмотрено ранее, целесообразно записывать в отдельные кластеры области данных, которые должны помечаться затем в FAT как зарезервированные под операционную систему или дефектные, либо в зарезервированные сектора системной области винчестера.

2.2. Привязка к аппаратной конфигурации компьютера

Различают следующие способы привязки к аппаратной конфигурации персонального iBM-сооместимого компьютера:

1) привязка к особенностям постоянного запоминающего устройства компьютера (ROM BIOS);

2) привязка к списку компьютерного оборудования.

В первом случае в качестве эталонных характеристик выступают контрольная сумма или дата изготовления BIOS. Дата изготовления BIOS хранится в восьми байтах внутренней памяти компьютера по адресу FOOO:FFF5$_{16}$.

При привязке к списку компьютерного оборудования в качестве эталонных характеристик выступает сам список оборудования, который можно получить путем использования соответствующей функции операционной системы.

Наиболее надежным способом привязки к аппаратной конфигурации компьютера является привязка к уникальному номеру процессора. Однако для персональных IBM-совместимых компьютеров этот способ нереализуем по причине невозможности программного доступа к этому уникальному номеру.

2.3. Привязка программы инсталляции к дистрибутивному носителю

Любые методы защиты от несанкционированного копирования исполняемых программ будут неэффективны, если не защищены от копирования дистрибутивные носители программного обеспечения, с которыми инсталлируются программы. Защита от копирования в этом случае реализуется привязкой программы инсталляции к дистрибутивным носителям, когда данная программа будет ориентирована на проведение инсталляции только при совпадении характеристик дистрибутивных носителей известными ей эталонными характеристиками.

Ранее для защиты дискет от копирования по секторам использовались достаточно простые способы нестандартного форматирования отдельных дорожек дискеты:

- создание большего, чем стандартное, числа секторов на дорожке;
- форматирование отдельных дорожек с размером секторов, отличным от стандартного, например 128 или 1024 байта;
- создание дорожек за пределами рабочей зоны диска, например создание 8-й дорожки для дискеты емкостью 1.44 Мбайта;
- форматирование отдельных дорожек с чередованием порядковых секторов.

Программа инсталляции в этом случае проводила инсталляцию только при наличии требуемого нестандартного формата дискеты, который невозможно было повторить при копировании дистрибутивных носителей стандартным способом (по секторам). Однако повторение формата дискеты возможно при ее побитовом копировании. Поэтому методы нестандартного форматирования дискет для защиты их от копирования в настоящее время потеряли свою актуальность.

Наиболее надежным способом формирования не копируемых эталонных свойств дистрибутивных дисков является искусственное **создание их не копируемых физических характеристик**. *К* таким физическим характеристикам можно отнести места расположения дефектов магнитного или оптического покрытия дистрибутивных дисков, а также степень синхронизации начала информационных дорожек.

В первом случае на дистрибутивных дисках искусственно ***создаются дефекты*** их магнитного (оптического) ***покрытия***, например - выжигание лазером небольших точек или нанесение незаметных царапин. Места расположения дефектов магнитного или оптического покрытия представляют собой эталонные характеристики дистрибутивных носителей информации. Запущенная инсталлирующая программа перед непосредственной инсталляцией должна будет проверить возможность считывания информации в эталонных местах расположения дефектов магнитного или оптического покрытия. Признаком подлинности дистрибутивного носителя будет возникновение ошибок при считывании данных из этих мест. В противном случае программа должна заблокировать свою дальнейшую работу, так как отсутствие ошибок является признаком копии дистрибутивного носителя. Ведь при любом виде копирования дистрибутива копируется только информация, а не его дефекты.

Во втором случае используются в качестве не копируемых физических характеристик дистрибутивных дисков – ***степени синхронизации начала информационных дорожек.*** Это возможно в связи с тем, что на стандартных дисках первые сектора дорожек никак не связаны друг с другом (Рис.1). При форматировании дискеты первый сектор на дорожке размещается в произвольном месте. Если же с помощью специально разработанной программы форматирования обеспечить синхронизацию первых секторов дорожек (Рис.1), то установленную степень синхронизации можно будет проверять программой инсталляции. Для проверки степени синхронизации между началами соседних дорожек необходимо будет выполнить следующую последовательность действий:

1) зафиксировать по времени прохождение первого сектора требуемой дорожки;

2) инициировать перемещение головки считывания на следующую дорожку;

3) зафиксировать по времени прохождение первого сектора следующей дорожки и определить интервал задержки между прохождениями первых секторов контролируемых дорожек;

4) сравнить полученное время задержки с эталонным.

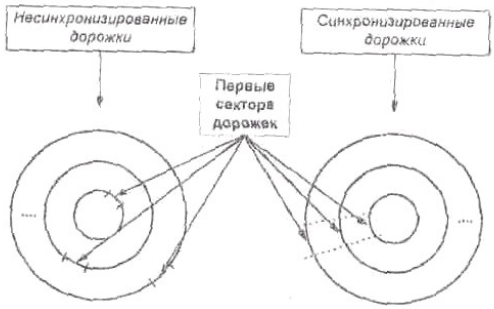

Рис. 1. Виды разметки дорожек дисковых носителей информации

Недостатком использования в качестве не копируемых физических характеристик дистрибутивных дисков степени синхронизации начала информационных дорожек является то, что при необходимости можно разработать побитовый копировщик, учитывающий степень синхронизации начала информационных дорожек копируемого

диска.

Управление потоками информации

Управление потоками информации входящих (выходящих) в АС осуществляется с помощью *фильтрации IP пакетов*. Суть данного метода, реализованного в межсетевых экранах (МЭ), заключается в том, что в правила пакетной фильтрации МЭ может вводиться информация о параметрах IP пакета, данные о протоколах, используемых сервисах (т.е. эталонные характеристики) проходящих через МЭ пакетов. МЭ пропускает через себя весь трафик, принимая относительно каждого проходящего пакета решение – пропускать его или отбросить. Более подробно о МЭ рассказывается в последующих лекциях.

В. 3. Регистрации и анализа событий, происходящих в АС

Данная задача может решаться с помощью ***систем обнаружения атак.*** Широкое распространение получил *метод* **обнаружения злоупотреблений** [12], суть которого заключается в описании атаки в виде шаблона (pattern) или сигнатуры (signature) и поиска данного шаблона в контролируемом пространстве (сетевом трафике или журнале регистрации). В качестве сигнатуры атаки может выступать шаблон действий или строка символов, характеризующие аномальную деятельность. Этот метод очень похож на обнаружение вирусов (можно сказать, что антивирусные средства являются одной из составляющих систем обнаружения атак), т.е. система может обнаружить все известные атаки, но она мало приспособлена для обнаружения новых, еще неизвестных, атак.

Подход, реализованный в таких системах, очень прост и именно на нем основаны практически все предлагаемые сегодня на рынке системы обнаружения атак.

Метод **обнаружения аномального поведения** не получил пока широкого распространения. Суть его заключается в том, что аномальное поведение пользователя (т.е. атака или какое-нибудь враждебное действие) часто проявляется как отклонение от нормального поведения. Примером аномального поведения может служить большое число соединений за короткий промежуток времени, высокая загрузка центрального процессора или использование периферийных устройств, которые обычно не задействуются пользователем.

Если бы мы смогли описать профиль нормального поведения пользователя и определить граничные значения характеристик его поведения, то любое отклонение от него можно охарактеризовать как аномальное поведение. Однако этот метод трудно реализуем на практике.

Методы обнаружения компьютерных вирусов тоже можно отнести к методу эталонных характеристик. К ним относятся [6]:

- сканирование;
- обнаружение изменений;
- эвристический анализ;
- резидентные «сторожа»;
- вакцинирование программных средств.

Они позволяют решать следующие задачи:

- контроль целостности данных;
- мониторинг целостности аппаратно-программного обеспечения при обработке и хранении информации;
- анализ событий, происходящих в АС

Метод сканирования заключается в том, что специальная антивирусная программа, называемая сканером, последовательно просматривает проверяемые файлы в поиске так называемых «сигнатур» (эталонных характеристик) известных компьютерных вирусов (КВ). При этом под **сигнатурой** понимают уникальную последовательность байтов, принадлежащую конкретному известному КВ и не встречающуюся в других программах.

Метод обнаружения изменений заключается в том, что антивирусная программа предварительно запоминает характеристики всех областей диска, которые могут

подвергаться нападению КВ, а затем периодически проверяет их. Если изменение этих характеристик будет обнаружено, то такая программа сообщит пользователю, что, возможно, в компьютер попал КВ.

Антивирусные программы, основанные на обнаружении изменений программной среды, называются *ревизорами*.

Метод эвристического анализа реализуется с помощью антивирусных программ, которые проверяют остальные программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для КВ. Так, например, эвристический анализатор может обнаружить, что в проверяемой программе присутствует код, устанавливающий резидентный модуль в памяти.

В **методе резидентных сторожей** используются антивирусные программы, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. При этом перечень этих подозрительных действий заранее определён, например это может быть попытка изменить загрузочный сектор жесткого диска или дискеты, а также выполнимый файл.

Вакцинирование устанавливает способ защиты любой конкретной программы от КВ, при котором к этой программе присоединяется специальный модуль контроля, следящий за ее целостностью.

При этом проверяются контрольная сумма программы или какие-либо другие ее характеристики. Если КВ заражает вакцинированный файл, модуль контроля обнаруживает изменение контрольной суммы файла и сообщает об этом пользователю.

В. 4. Методы обнаружения модификации данных.

Своевременное обнаружение фактов несанкционированных действий пользователей основано на выполнении следующих функций:

- периодический контроль целостности информации;
- регистрация и сигнализация;
- контроль правильности функционирования системы защиты.

Периодический контроль целостности конфиденциальной информации позволяет своевременно обнаружить попытки подлога и потери данных, а системной - внедрение программных закладок и компьютерных вирусов.

Регистрация для своевременного обнаружения фактов несанкционированных действий пользователей предполагает фиксацию и накопление сведений о всех запросах, содержащих обращения к защищаемым компьютерным ресурсам, включая доступ в вычислительную систему и завершение сеанса работы пользователей. Сигнализация же в этом случае состоит в своевременном уведомлении соответствующих компонентов системы защиты и администрации об обнаруженных несанкционированных действиях.

Без эффективной реализации функции контроля правильности функционирования системы защиты невозможно достигнуть высокой эффективности функционирования не только подсистемы обнаружения не санкционированных действий пользователей, но и системы защиты в целом.

Общие сведения о контроле информационной целостности

Под контролем целостности данных, хранимых в вычислительной системе или передаваемых по каналам связи, понимается обнаружение их любых случайных или несанкционированных изменений.

Периодическому контролю на целостность должна подвергаться вся конфиденциальная и системная информация, хранящаяся в вычислительной системе. Периодический контроль целостности конфиденциальной информации позволяет своевременно обнаружить попытки подлога и потери данных, а системной - внедрение программных закладок и компьютерных вирусов.

Периодичность контроля целостности хранящейся в вычислительной системе конфиденциальной и системной информации не должна быть реже ежедневной. Поэтому

программы контроля информационной целостности целесообразно активизировать в процессе загрузки операционной системы.

Передаваемая по каналам связи информация должна подвергаться контролю на целостность после каждого приема этой информации получателем.

Контроль информационной целостности реализуется на основе предварительного определения характеристики целостной (эталонной) информации, называемой эталонной характеристикой или эталонным кодом обнаружения модификаций. Для высокой эффективности использования эта эталонная характеристика должна быть по объему значительно меньше контролируемой информации и ее значение должно зависеть от содержимого и очередности всех двоичных блоков защищаемых от модификации данных. В зарубежной литературе эталонную характеристику обнаружения модификаций называют MAC-кодом (message authentfcation code) В процессе непосредственного контроля информационной целостности выполняются следующие действия:

1. для контролируемой информации определяется текущая характеристика обнаружения модификаций по тому же способу, по которому формировалась эталонная характеристика;
2. текущая и эталонная характеристики обнаружения модификаций сравниваются, и если они совпадают, то считается, что контролируемая на целостность информация не подвергалась изменению.

Для объективности заключения об информационной целостности по совпадению текущей и эталонной характеристик обнаружения модификаций необходимо, чтобы метод, используемый для формирования этих характеристик, обеспечивал чрезвычайно малую вероятность изменения данных, при которых их текущая и эталонная характеристики совпадают.

Эталонная характеристика обнаружения модификаций должна храниться или передаваться вместе с контролируемыми на целостность данными, для которых эта характеристика сформирована.

Способы определения модификаций информации

Определение случайных модификаций

Для определения случайных модификаций информации ее эталонная характеристика может быть открытой для доступа. В этом случае формирование характеристики обнаружения модификаций может осуществляться в соответствии со схемой последовательного контрольного суммирования по операции исключающего ИЛИ (XOR) двоичных блоков, составляющих контролируемую на целостность информацию.

Для определения не только случайных, но и преднамеренных модификаций информации ее эталонная характеристика должна защищаться криптографическими методами или формироваться на основе криптографических преобразований.

Практическая реализация контроля информационной целостности

Подсистема контроля информационной целостности является неотъемлемым компонентом любой специализированной системы защиты информации. Данная подсистема должна обеспечивать периодический контроль целостности не только конфиденциальных данных, но и всей системной информации, задающей требуемые режимы и параметры функционирования компьютера. Это позволит своевременно обнаружить как попытки подлога и потери конфиденциальной информации, так и внедрение несанкционированных программ (программных закладок и компьютерных вирусов).

Таким образом, функции по контролю информационной целостности наряду с проверкой целостности конфиденциальной информации обеспечивают своевременное обнаружение отклонений текущего состояния рабочей среды компьютера от эталонного. По этой причине подсистему контроля информационной целостности часто называют подсистемой обеспечения эталонного состояния рабочей среды вычислительной системы.

Наиболее надежные системы защиты, например, система «Кобра», обеспечивают не только своевременное обнаружение отклонений текущего состояния рабочей среды компьютера от эталонного, но и автоматическое восстановление ее основных компонентов (содержимого CMOS-памяти, главной загрузочной записи винчестера, включая его таблицу разделов, загрузчика DOS, CONFIG.SYS, AUTOEXEC.BAT и т.д.).

Для контроля информационной целостности также можно использовать антивирусные программы, называемые ревизорами. Однако перед выбором ревизора следует выяснить, обеспечивает ли он выполнение функций по контролю целостности файлов данных, так как основное назначение ревизоров контроль целостности программ.

Организация контроля

При установке и использовании программных средств контроля информационной целостности должны быть выдержаны следующие этапы.

1. Тщательный анализ всех файлов конфигурирования и настроим на отсутствие вызовов несанкционированных программ. При обнаружении такие вызовы следует удалить, а также установить и устранить причину их появления.

2. Тщательный анализ вычислительной системы на наличие вирусов и полное обезвреживание обнаруженных вирусных программ с помощью обновленной версии транзитного сканера. Для большей эффективности процессов поиска и обезвреживания вирусов целесообразно независимое применение нескольких различных сканеров.

3. Установка требуемых режимов и параметров рабочей среды компьютера,

4. Формирование с помощью специализированной программы, например, ревизора, следующих эталонных характеристик рабочей среды компьютера:

- содержимого загрузочных секторов жестких дисков;
- содержимого CMOS-памяти;
- контрольных сумм содержимого файлов конфигурирования и настройки, например, файлов AUTOEXEC.BAT, CONFIG.SYS, *INI для MS-DOS/Windows 3.11 (3.1), а также SYSTEM.DAT и USER.DAT для Windows 95-*;
- контрольных сумм или описания структуры содержимого оперативной памяти компьютера;
- информации о количестве и расположении сбойных кластеров жестких дисков (некоторые вирусы размещают свои тела в свободных кластерах, помечаемых затем этими вирусами как сбойные);
- контрольных сумм содержимого файлов с программами, а также их системных характеристик: пути, даты и времени создания, длины, значений атрибутов, а при необходимости, и адресов физического расположения;
- контрольных сумм и системных характеристик файлов с конфиденциальными данными.

5. Периодическая проверка специализированной программой, на пример, ревизором, соответствия реальных характеристик элементов компьютерной системы их эталонным характеристикам, которые эти элементы имели при целостном (эталонном) состоянии. В зависимости от возможностей специализированной программы контроля могут использоваться следующие виды периодических проверок:

=>строго периодическая, например, ежедневная, при которой проверяются все элементы компьютера, для которых созданы эталонные характеристики;

=>в режиме реального времени, при которой осуществляется проверка контролируемых элементов только при попытке их использования, например, при попытке запуска программ и открытия документов.

При обновлении контролируемых на целостность информационных объектов, например, при изменении файлов конфигурирования и настройки, должны быть изменены и их эталонные характеристики.

Для файлов с конфиденциальными данными эталонные характеристики следует формировать после каждого обновления или создания этих файлов. Для высокой безопасности непосредственный контроль целостности файлов с информацией повышенного уровня секретности целесообразно выполнять не только ежедневно, но и перед доступом к этим файлам.

В случае обнаружения несоответствия реальных характеристик эталонным перед принятием мер необходимо выяснить причину этого несоответствия. Возможны следующие причины:

1) после обновления элементов, для которых формировались эталонные характеристики, не была обновлена эталонная информация;

2) повреждение контролируемых элементов данных по причине возникновения сбоев или отказов программно-аппаратных средств;

3) несанкционированная модификация информационных файлов;

4) заражение программ компьютерным вирусом.

Особенности использования программ непосредственного контроля

Программы, предназначенные для непосредственного контроля соответствия текущих характеристик элементов данных их эталонным характеристикам могут функционировать транзитно и резидентно.

Транзитные программы контроля загружаются в оперативную память только для выполнения проверок. Резидентные же после запуска остаются в оперативной памяти резидентно и проверяют контролируемые элементы компьютера при возникновении с ними определенных событий" (открытие документов, запуск и модификация программ, копирование, создание, переименование файлов и т.д.). Наибольшая результативность контроля информационной целостности достигается при совместном использовании транзитного и резидентного средства, когда осуществляется не только строго периодическая, например, ежедневная проверка, но и динамический контроль элементов данных на соответствие эталонным характеристикам. При этом следует учитывать, что использование резидентной программы контроля приводит к снижению быстродействия функционирования компьютера.

Для транзитной программы контроля должны быть предусмотрены следующие виды и периодичность использования:

- первый запуск для формирования эталонных характеристик подлежащих контролю информационных объектов компьютера после поиска и обезвреживания вирусов транзитным сканером и тщательной проверки файлов конфигурирования на отсутствие вызовов программных закладок;
- ежедневный запуск в процессе загрузки операционной системы для проверки всех контролируемых информационных объектов (в оперативной памяти, а также на всех логических дисках);
- по мере необходимости для формирования эталонных характеристик созданных или обновленных файлов с конфиденциальной и системной информацией;
- по мере необходимости для формирования эталонных характеристик программ, поступающих извне, после проверки их транзитным сканером.

Для активизации строго периодического запуска транзитной программы контроля может использоваться резидентная программа-планировщик.

Запуск резидентной программы контроля для ее постоянного нахождения в оперативной памяти должен осуществляться в процессе загрузки операционной системы.

Недостатком программ контроля информационной целостности является назойливость по отношению к пользователям, так как пользователями или администраторами не всегда вовремя обновляются эталонные данные. Но этот недостаток с лихвой компенсируется значительным повышением степени защищенности от подлога и потери данных, а также внедрения программных закладок и компьютерных вирусов.

Для повышения эффективности защиты программы от исследования кроме перечисленных мер необходимо внесение в секретную часть программы дополнительных функций безопасности, ориентированных на защиту от **модификации**. К ним относятся:

- периодический подсчет контрольной суммы области оперативной памяти, занимаемой защищаемым исходным кодом; сравнение текущей контрольной суммы с предварительно сформированной эталонной и принятие необходимых мер в случае несовпадения;
- проверка количества занимаемой защищаемой программой оперативной памяти; сравнение с объемом, *к* которому программа адаптирована, и принятие необходимых мер в случае несоответствия;
- контроль времени выполнения отдельных частей программы;
- блокировка клавиатуры на время отработки особо секретных алгоритмов.

Старший преподаватель 27 кафедры
подполковник
С.Краснов