МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

ЛЕКЦИОННЫЕ МАТЕРИАЛЫ

Методы обеспечения целостности информации

(наименование дисциплины (модуля) в соответствии с учебным планом)

Уровень	бакалавриат
	(бакалавриат, магистратура, специалитет)
Форма обучения	очная
	(очная, очно-заочная, заочная)
Направление(-я) подготовки	09.03.02 «Информационные системы и технологии»
	(код(-ы) и наименование(-я))
Институт	кибербезопасности и цифровых технологий (ИКБ)
	(полное и краткое наименование)
Кафедра	Разработка программных решений и системное программирование
	(полное и краткое наименование кафедры, реализующей дисциплину (модуль))
Лектор	К.т.н. Ермакова Алла Юрьевна
	(сокращенно – ученая степень, ученое звание; полностью – ФИО)

Используются в данной редакции с учебного года 2023/24

(учебный год цифрами)

Проверено и согласовано «____» _____2023_г.

(подпись директора Института/Филиала с расшифровкой)

Москва 2023 г.

Содержание

Лекция 1. Защита целостности информации при хранении

Введение

Понятие целостности данных в научной литературе имеет несколько определений. В одной из наиболее распространенных трактовок под целостностью данных подразумевается отсутствие ненадлежащих изменений. Смысл понятия «ненадлежащее изменение» раскрывается Д. Кларком и Д. Вилсоном: ни одному пользователю АС, в том числе и авторизованному, не должны быть разрешены такие изменения данных, которые повлекут за собой их разрушение или потерю.

Нарушение целостности информации происходит либо при несанкционированном доступе к информации, либо без него.

Угроза целостности существует на всех этапах жизни информации:

• при хранении;

• при обработке;

• при транспортировке.

В ТКС основное место хранения информации – машинные носители, поэтому рассмотрим меры защиты применительно к этому классу носителей.

Определяя порядок хранения информации на МНИ, следует иметь в виду, что от состояния носителей зависит качество программ и защищаемых данных. МНИ являются электро-механическими утройствами, подвергаюшимися интенсивному износу. Кроме того, в МНИ могут быть внедрены аппаратные закладки, поэтому используемые методы записи, хранения и считывания нельзя считать защищенными.

Организационно-технологические меры защиты целостности информации на МНИ можно разделить на две основные группы:

• организационные меры по поддержке целостности информации, хранящейся на МНИ;

• технологические меры контроля целостности битовых последовательностей, хранящихся на МНИ.

Организационные меры

Организационные меры защиты направлены на предупреждение хищения или утраты носителей, а вместе с ними и информации. Организационные меры излагаются в документах, описывающих режим хранения конфиденциальной информации.

Организационные меры разделяются на две группы:

• создание резервных копий информации, хранимой на МНИ;

• обеспечение правильных условий хранения и эксплуатации МНИ.

Создание резервных копий

Создание резервных копий информации, хранимой на МНИ, должно быть обязательной регулярной процедурой, периодичность которой зависит от важности информации и технологии ее обработки, в частности от объема вводимых данных, возможности повторного ввода и т. д. Для создания резервных копий могут использоваться как стандартные утилиты, которые сохраняют выбранные файлы или каталоги, так и специализированные системы резервного копирования, адаптированные к конкретной ТКС. В последнем случае можно применять собственные методы архивирования, например, так называемое «разностное» архивирование, когда на вспомогательный носитель записывается не весь объем базы данных, а только та часть, которая была введена с момента последнего сохранения.

В качестве вспомогательных носителей для хранения архивных данных выбирают, как правило, те, которые при заданном объеме копируемой информации (в случае накопления информации и с учетом определенной

перспективы) и предполагаемом сроке хранения оптимальны по цене единицы хранимой информации. Так, в ряде случаев оптимальным устройством резервирования может быть дополнительный жесткий диск или CD-ROM. При ведении резервных копий необходимо регулярно проверять их сохранность и целостность находящейся в них информации.

Обеспечение правильных условий хранения и эксплуатации

Обеспечение правильных условий хранения и эксплуатации определяется конкретным типом машинного носителя.

Регистрация и учет МНИ производятся независимо от того, есть ли на них конфиденциальная информация или нет. Служебные МНИ должны иметь ясную, хорошо видимую этикетку, на которой проставлены гриф, номер, дата регистрации. Гриф секретности носителя может изменяться только в большую сторону, т. к. информация не может быть гарантированно удалена. Учет носителей по журналу ведется в течение всей «жизни» носителя. В помещении не должно быть личных носителей. Не допускается работа с непроверенными носителями. Должна проводиться систематическая комиссионная проверка наличия носителей и информации.

Хранение МНИ такое же, как обычных документов такого же уровня конфиденциальности. Основное требование при хранении – исключение НСД. Передача между подразделениями должна осуществляться под расписку и учитываться в журнале. Вынос за пределы помещения возможен только с разрешения уполномоченных лиц.

Жесткий диск регистрируется с грифом, соответствующим категории СВТ, независимо от целей его использования. На корпусе жесткого диска должна быть соответствующая этикетка. При передаче компьютера в ремонт необходимо изъять жесткий диск, либо гарантированно удалить с него информацию, либо присутствовать при ремонте.

Копирование файлов с зарегистрированных МНИ допускается только на компьютерах, категория которых не ниже грифа секретности носителя. Каждое копирование должно учитываться в журнале, обычном или электронном.

Необходимо уделять особое внимание удалению информации с носителей. Обычные способы удаления файлов не приводят к удалению области данных, происходит стирание только на логическом уровне. Кроме того, при удалении следует учесть, что в современных средствах обработки информация существует в нескольких экземплярах, под разными именами.

Технологические меры

Рассмотрим теперь технологические меры контроля целостности битовых последовательностей, хранящихся на МНИ. Целостность информации в областях данных на машинных носителях проверяется с помощью контрольного кода, контрольные числа которого записываются после соответствующих областей, причем в контролируемую область включаются соответствующие маркеры.

Для стандартного сектора диска размер контролируемой области составит 516 байт: 512 байт данных плюс 4 байта маркера данных. При чтении с диска данные проверяются на соответствие записанному коду и в случае несовпадения выставляется соответствующий флаг ошибки.

Для обеспечения контроля целостности информации чаще всего применяют циклический контрольный код. В основе данного подхода лежит понятие полинома. Как известно, полином – это формально заданный степенной ряд.

В общем случае любой блок информации x в памяти вычислительной машины представляет последовательность битов, которую можно считать двоичным полиномом $A(x)$. Для вычисления контрольного кода понадобится еще один полином, называемый порождающим полиномом. Этот полином

обозначим $G(x)$. Порождающий полином является в некотором роде ключом циклического кода.

Контрольный код, представляемый полиномом $R(x)$, вычисляется как остаток от деления полинома $A(x)$ на $G(x)$.

Из теории циклических кодов следует, что чем больше степень порождающего полинома, тем больше обнаруживающая способность контрольного кода.

Этот метод, дающий хорошие результаты при защите от воздействия случайных факторов (помех, сбоев и отказов), совсем не обладает имитостойкостью, т. е. не обеспечивает защиту от целенаправленных воздействий нарушителя, приводящих к навязыванию ложных данных.

Для контроля целостности можно использовать методы имитозащиты, основанные на криптографических преобразованиях. Они обеспечивают надежный контроль данных, хранящихся в системе, но в то же время реализуются в виде объемных программ и требуют значительных вычислительных ресурсов.